WHITEPAPER:

NIS 2 MAGYARORSZÁGON

Tapasztalatok és javaslatok
az elmúlt másfél év gyakorlata alapján

PUBLIKÁLVA: 2026. JÚLIUS 30.

VERZIÓ 2.0

Impresszum

Kiadó: Dr. Váczi Dániel

Szerkesztették: Dr. Váczi Dániel, Orbók Ákos

Az első verziót írták: Ács Bálint, dr. Albert Ágota, Apró William Z., Arató György, Barbul Gergő, Biró Gabriella, Borbély Zsuzsa,BódisPéter,CsarnaiGergő,CsehPatrik,CserhátiVencel,EnyediAlexandra,FreyKrisztián, Gedra János, dr. Jeney Andrea, Kálmán Kinga, Dr. Kiss Judit, Kovács György Attila, Lóth Tamás, Maczkó Péter, Major Róbert, Mandrik Edina, Máté Márk, Mészáros Csaba, Mészáros Etele, Molnár Bálint, Molnár Ferenc, Nagy Imre, dr. Novák Anett, Pataki Norbert, Robotka Árpád, dr. Simon Ádám, Sipos Zoltán, Solymos Ákos, dr. Szabó László, Szabó Mária Etelka, dr. Szilágyi Emese, Szűcs Krisztina, Dr. Tiszolczi Balázs Gergely, Dr. Váczi Dániel, Végh András

A második verziót írták: dr. Albert Ágota, Dr. Bederna Zsolt, Biró Gabriella, Jakobetz András, dr. Jeney Andrea, Kalmár István, Koppány Géza, Lendák Imre, Major Róbert, Molnár Bálint, Nagy Ágnes Beáta, Nagy Imre Gábor, Sipos Zoltán, Szabó Mária Etelka, Dr. Tiszolczi Balázs Gergely, Dr. Váczi Dániel

Az első verziót lektorálták: Arató György, Dr. Berzsenyi Dániel, Dr. Bonnyai Tünde, Bor Olivér, Dr. Kiss Judit, Miklós Márton, dr. Szilágyi Enikő

A második verziót lektorálták: Arató György, Dr. Szilágyi Enikő, Dr. Váczi Dániel,

Projektvezető: Forgács Éden

Design: Elek Zsófia, Csengery Csenge

Felhasznált fotók: Solymos Ákos EFIAP/A-MAFOSZ/s

ISBN 978-615-83074-0-6

A két kiadásban résztvevő szervezetek:

Tartalom

Impresszum **2**

1. Bevezető **9**

2. Jogszabályi háttér **13**

2.1. A NIS2 célja 13

2.2 Kapcsolódó EU szabályozások és tanúsítási keretrendszerek a NIS2 kontextusában 19

2.3. A NIS2 magyarországi jogszabályi háttere 21

Példaként említhetők: 23

A finomhangolás folyamata 25

2.4. NIS 2-megfelelés értelmezése a Whitepaperben 26

3. Érintett szervezetek azonosítása **28**

3.1. Önazonosítás 28

3.2. Segítő szereplők 31

3.3 Nemzetközi szolgáltatásnyújtás kérdései 33

4.Szerepkörök és felelősségek **38**

4.1 Információbiztonsági szerepkörök 38

4.2. Szükséges IBF készségek és tanúsítványok 42

5. Kockázatkezelési keretrendszer kialakítása **45**

5.1. A kockázatkezelési keretrendszer 45

5.2. Mit kell tartalmaznia a kockázatkezelési keretrendszernek? 45

5.3. Kockázatkezelés: a meglévő keretrendszer része legyen, vagy különálló rendszerként működjön? 46

5.4. Rendelkezésre állási követelmények 48

5.5. Adatvagyon és BIA (üzleti hatáselemzés) szerepe 49

5.5.1. BIA folyamata 49

5.5.2. Várható eredmények 53

5.6. Üzleti folyamatok feltérképezése 53

5.7. A kockázatelemzés, figyelembe véve az ellátási lánc kockázatait 55

5.8 Compliance scoring és a folyamatos megfelelés mérése 57

5.8.1 A compliance scoring szerepe a NIS2 megfelelési modellben 57

5.8.2 Jogszabályi háttér és megfelelőségi elvárások 57
5.8.3 A compliance scoring céljai és alapelvei 58
5.8.4 A compliance scoring dimenziói 58
5.8.5 Pontozási modell és súlyozás 58
5.8.6 Compliance Scoring mintatáblázat (alkalmazási példa) 59
5.8.6 Riportolás és vezetői dashboard 60
6. Azonosított EIR-ek és rendszerelemek 62
6.1. Mit tekintünk EIR-nek? 62
6.2. Biztonsági osztályba sorolás irányelvei 66
6.3 OT rendszerek sajátosságai 69
6.4. EIR kiválasztása SEVESO és kritikus infrastruktúrájú üzemeknél 71
6.4.1. SEVESO környezet specifikus követelményei 72
6.4.2. EIR kiválasztási folyamat és kritériumok 72
6.4.3. Gyakorlati implementáció 73
7. Nemzetközi kitettség és harmonizáció 75
7.1. Más EU tagállamok hozzáállása 75
7.1.1. Az EU követelményrendszere 75
7.1.2. Belgium 75
7.1.3. Franciaország 76
7.1.4. Szlovákia 76
7.1.5. Ausztria 76
7.1.6. Németország 76
7.1.7. Olaszország 78
7.1.8. Lettország 78
7.1.9. Dánia 78
7.1.10. Bulgária 79
7.2. Csoportosítási elvek: lehetőségek és buktatók 79
8. A hazai követelmények gyakorlati értelmezése és alkalmazása 81
8.1. 7/2024 vs 1/2025 rendelet összevetése 81

8.1.1. 7/2024. (VI. 24.) MK rendelet 81
8.1.2. 1/2025 (I.31.) SZTFH rendelet 82
8.2. Gyakorlati megvalósítási tippek magas erőforrásigény mellett 88
8.3. Szerződések kiegészítési javaslatai 89
8.4. Meg kell-e felelni minden pontnak? 92
8.5. A megfelelés túl- vagy alulteljesítésének kockázatai 92
8.6. Helyettesítő védelmi intézkedések lehetőségei 93
8.7. Eltérési lehetőségek kezelése 94
9. Előkészítendő dokumentumok és nyilvántartások 97
9.1. Az EIR-ek biztonsági és kockázatmenedzsment dokumentációi 97
9.2. Információbiztonsági szabályzat (IBSZ) 100
9.3. Egyéb belső szabályozások 102
9.4. Eljárásrendek és protokollok 104
9.5. Személyi biztonsággal kapcsolatos dokumentumok 105
9.6. Nyilvántartások és azok vezetése 108
9.6.1. Hogyan lehet ennyiféle nyilvántartást vezetni, karbantartani? 109
9.7. A rendszerbiztonsági terv 110
10. Auditálási folyamat 115
10.1. Evidenciák előkészítése, összegyűjtése 115
10.2. Auditálásba bevont személyek felkészítése 115
10.3. Pontozási rendszer értelmezése és bemutatása gyakorlati példán keresztül 116
10.4. Szubjektív tényezők szerepe az auditban 121
10.5. Módszertani eltérések auditorok között 122
10.6. Behatolás tesztelés (Pentesztekre) való felkészülés 123
10.7. Összeférhetetlenség 124
10.8. Audit riport értelmezése (JSON) 127
10.9. Eddigi audittapasztalatok 131
11. Ellátási lánc biztonsága 136
11.1. Meglévő szerződések felülvizsgálata 136
11.2. Új szerződéskötések szempontjai 138

11.3. Kockázatelemzés az ellátási lánc mentén 142
11.4. Milyen információkat kérjünk be a beszállítóktól? 143
11.5. Mit adjunk át beszállítóként? 146
12. Használható eszközök és automatizálási lehetőségek 149
12.1. Excel-alapú megoldások 149
12.2. GRC és menedzsment eszközök 150
12.3. AI alkalmazási lehetőségei 151
12.4. Evidenciafeldolgozás nyelvi modellekkel: lehetőségek és korlátok 154
13. Incidenskezelés és válság- kommunikáció 158
13.1. Általános keretek 158
13.1.1 Gyakorlati forgatókönyvek 159
13.1.2. Incidenskezelés forgatókönyv 159
13.1.3. Válságkommunikációs forgatókönyv 161
13.1.3. Gyakorlati szimulációk 163
13.1.4. Eddigi tanulságok 166
13.2. CSIRT jelentési kötelezettségek 166
13.3. Média, partnerek, felügyeletek, NAIH – mit, mikor, kinek? 168
13.4. Vezetői, PR és jogi szereplők bevonása 170
13.5 Digital Omnibus Package 173
14. Fizikai biztonsági intézkedések 175
14.1 A fizikai biztonság szintjei 175
14.2 Biztonsági intézkedések 176
15. Folyamatos fenntartás és megfelelőség- menedzsment 184
15.1. Mit kell tennünk a következő 2 évben? 184
15.2. Intézkedési tervek kialakítása 184
15.3. PPT érettségi szint követése 185
15.4. IT, biztonság és üzlet súlyozása 186
15.5. SZTFH és/vagy NKI szerepe 187
16. Kapcsolódó feladatok és megfelelések 192
16.1. NAIH kötelezettségek 192

16.2. DORA megfelelés 195
16.3. ISO 27001 196
16.4. TISAX 198
16.5. A NIS 2 és a GDPR kapcsolata 202
17. Információbiztonsági architektúra a NIS2 megfelelési programban 210
17.1 Az információbiztonsági architektúra szerepe és fogalma 210
17.2 Architektúra keretrendszerek 210
17.3 Az információbiztonsági kontrollok architektúrája 213
17.4 Az információbiztonsági architektúra technológiai elemei 214
17.5 Információbiztonsági architektúra a NIS2 megfelelésben 215
17.6. Esettanulmány – mikro és KKV szolgáltatók architektúrája 216
17.7 NIS2 audit tapasztalatok 219
17.8 Ajánlások mikro és KKV szervezetek számára 221
18. Kommunikáció a menedzsmenttel 224
18.1. Hogyan és mit mondjunk a vezetőségnek? 224
18.2. Riportolási lehetőségek 225
18.3. Legfontosabb költségtételek 225
18.4. Nem választás, hanem kötelesség – A vezetőség feladatai és a várható kihívások 225
19. Megérteni és megértetni 228
19.1. Belső munkacsoportok, felhasználók bevonása 228
19.2. Szervezeten belüli együttműködés, szervezeti egységek bevonása 230
19.3. Felhasználók szerepe, tájékoztatása és bevonása 231
20. „Quick Win” lista 234
21. Szankciók és következmények 237
21.1. Jogkövetkezmények a szervezettel és annak vezetőjével szemben 237
21.2. Jogkövetkezmények az auditorral szemben 238
21.3. A jogkövetkez-mények alkalmazása 238
21.4. Jogorvoslat 239

22. Biztonsági kultúra és tudatosság **241**

23. Rövidítés- jegyzék **246**

Mi változott a 2.0 verzióban? **251**

Záradék **253**

1. Bevezető

Írta: Dr. Váczi Dániel

A whitepaper első verziójának elkészítését a 2025 tavaszán zajló szakmai beszélgetések és a NIS 2 podcast felvételei inspirálták. Ezekből a párbeszédekből világosan kirajzolódott, hogy az érintett szervezetek részéről valós igény mutatkozik egy olyan gyakorlati iránymutatásra, amely segíti őket a magyarországi jogi implementáció kérdéses pontjaiban. Az első változat ebből az igényből született meg, azzal a szándékkal, hogy a jogszabályi megfelelésről szóló általános diskurzust közelebb hozza a mindennapi megvalósításhoz.

A megjelenést követően számos pozitív szakmai visszajelzést kaptunk. Sokan elismerésüket és köszönetüket fejezték ki azért, hogy egy olyan anyag készült, amely nem pusztán elméleti síkon beszél a NIS 2-ről, hanem gyakorlati kapaszkodókat is igyekszik adni. Ugyanakkor több konstruktív észrevétel és fejlesztési javaslat is érkezett. Ezek, kiegészülve az elmúlt bő fél év audit tapasztalataival, egyértelművé tették, hogy a dokumentum frissítése indokolt. A jelen verzió ezért nem egyszerű újrakiadás, hanem egy továbbgondolt, tapasztalatokkal bővített változat, amely jobban reflektál a megfelelési és auditálási folyamatok során felmerülő gyakorlati kérdésekre.

Az elmúlt időszakban a megfelelési folyamatok érezhetően előrehaladtak. Egyre több szervezet jutott el az önazonosítástól a gyakorlati felkészülésig, majd onnan az audit közeli vagy audit alatti állapotig. Ezzel párhuzamosan jelentősen nőtt a rendelkezésre álló tapasztalat mennyisége is. Világossá vált, hogy a szervezeteknek nemcsak jogértelmezési segítségre van szükségük, hanem olyan útmutatásra is, amely a gyakorlati megvalósításban támogatja őket. A kérdés ma már sokszor nem az, hogy mit ír elő a szabályozás, hanem az, hogy az előírásokat miként lehet egy adott szervezet működésébe-, folyamataiba-, felelősségi rendszerébe és erőforrásai közé reálisan beilleszteni.

A dokumentum megszületésében fontos szerepet játszott az a szemlélet is, amelyet az általam képviselt startup képvisel. Ennek lényege, hogy hídként kapcsolja össze a hazai és az uniós kiberbiztonsági szereplőket a NIS 2 kapcsán. Ebből szinte természetesen következett az a gondolat, hogy egy ilyen whitepaper közösségi alapon jöjjön létre. Személyes motivációm is az volt, hogy ne csak arról beszéljünk, miért fontos a NIS 2-nek való megfelelés, hanem arról is, hogyan lehet ezt a gyakorlatban, lépésről lépésre megvalósítani. Az első verzió megírása előtt a közösségi média szakmai fórumain közzétett felhívásunkra több mint ötven, a témában jártas szakember és szervezet jelentkezett. Volt, aki a fejezetek írásában, más projektvezetésben, a szerkesztésben vagy szakmai véleményezésben vállalt szerepet. Külön öröm és büszkeség számomra, hogy ennyien szántak időt és energiát a közös munkára a napi feladataik mellett. A közösségi együttműködés ebben az esetben is megmutatta az erejét, hiszen különböző nézőpontok, szakterületek és tapasztalatok tudtak egy közös cél érdekében találkozni.

Jelen, második verzió ugyanígy készült. Csatlakoztak az írók közé új szakemberek és szervezetek is. Mely további megerősítést ad nekünk abban, hogy ez egy jó irány és szükség van a munkára. Véleményem szerint, a jelenleg hatályos 2026. június 30-ai audit határidőt követően viszont már egy egységes irányalkotásra van szükség, miután a szakma és a jogalkotó levonta a következtetést az elmúlt évek tapasztalata alapján és esetleg módosításokat eszközöl a jelenlegi elvárásokon, jogszabályi környezetben.

Mindez azért is különösen fontos, mert a mindennapi gyakorlat azt mutatja, hogy a jelenleg akkreditált auditor cégek, az őket támogató alvállalkozók, az érintett szervezetek és az őket

felkészítő tanácsadók eltérő hozzáállása, érettsége és szakmai felkészültsége egy rendkívül összetett szakmai közeget hozott létre. Ebben a közegben sokszor nem könnyű eligazodni. A szervezetek gyakran azt tapasztalják, hogy ugyanarra a kérdésre többféle megközelítés, eltérő hangsúly vagy akár különböző gyakorlati elvárás is megjelenhet. Ez önmagában nem feltétlenül probléma, hiszen a megfeleléshez vezető út valóban nem minden esetben egyforma. Ugyanakkor ez a sokféleség bizonytalanságot is okozhat, különösen azok számára, akik most szembesülnek először a NIS 2 gyakorlati végrehajtásával.

Ezért ezzel a whitepaperrel nem az a célunk, hogy minden létező módszertant bemutassunk, vagy egyetlen helyes megközelítést hirdessünk. Nem szeretnénk sem kizárólagos értelmezési keretet adni, sem egységes szakmai receptet előírni. Sokkal inkább az a szándékunk, hogy az írók és közreműködők által a gyakorlatban szerzett tapasztalatokat visszacsatornázzuk a szakma felé, és ezzel érdemi segítséget nyújtsunk a megfelelési és auditálási folyamatok során. A dokumentum célja tehát nem a lezárás, hanem a tájékozódás támogatása. Egy olyan gyakorlati kapaszkodó kíván lenni, amely segíthet abban, hogy a szervezetek a saját működésükhöz illeszkedő módon tudják kialakítani a megfelelési lépéseiket.

A szöveg kialakítása során ezért kiemelten figyeltünk arra, hogy megőrizzük a szakmai hitelességet, miközben közérthetően és lényegre törően fogalmazunk. Fontos volt számunkra, hogy az anyag ne csak azok számára legyen hasznos, akik mély szaktudással rendelkeznek a kiberbiztonság, a compliance vagy az audit területén, hanem azok számára is, akik most találkoznak először ezzel a témával, mégis kulcsszerepet töltenek be a szervezeti megfelelés biztosításában. Úgy gondoljuk, hogy a NIS 2 hazai implementálásának sikeres gyakorlati alkalmazásához nemcsak szakmai pontosságra, hanem érthetőségre és alkalmazhatóságra is szükség van.

Nem állítjuk, hogy nálunk van a legjobb megoldás, ha egyáltalán létezik ilyen. A NIS 2 szabályozás összetettsége miatt bizonyosan vannak olyan témák, amelyeket ebben a dokumentumban nem tudtunk teljes mélységükben bemutatni. Igyekeztünk ugyan többféle nézőpontot és megközelítést párhuzamosan is érzékeltetni, de vannak olyan részterületek, amelyek önmagukban is külön dokumentumot érdemelnének. Mindezek ellenére törekedtünk arra, hogy egy olyan gyakorlati esszenciát adjunk át, amelyből a szervezetek saját működésükre, érettségi szintjükre és belső folyamataikra szabott következtetéseket tudnak levonni.

Fontos tehát hangsúlyozni, hogy ez a dokumentum nem hivatalos útmutató. Nem garantáljuk, hogy kizárólag ennek alkalmazásával egy szervezet automatikusan megfelel az elvárásoknak vagy sikeresen teljesít egy auditot. Abban azonban hiszünk, hogy a gyakorlati megvalósításról közérthetően beszélni már önmagában is érték. Ha ez az anyag segít abban, hogy egy szervezet jobb kérdéseket tegyen fel, tudatosabban készüljön, és jobban értse a saját helyzetét, akkor már betölti a szerepét.

Végül fontosnak tartjuk felhívni minden olvasó figyelmét arra, hogy a legjobb eredményt akkor lehet elérni, ha a szervezet saját közvetlen szakmai környezetével konstruktív együttműködésre törekszik. Ennek alapja a jóhiszeműség, amely az elmúlt időszakban nem minden esetben valósult meg kellő mértékben. Meggyőződésünk, hogy a megfelelési és auditálási folyamatok minőségét jelentősen javítja, ha egymásban nem ellenérdekű másik felet, hanem partnert látunk. A nyílt, folyamatos és tisztességes kommunikáció nem pusztán udvariassági kérdés, hanem a szakmai előrehaladás egyik legfontosabb feltétele. Ennek a whitepapernek is az a célja, hogy ezt a szemléletet erősítse, és hozzájáruljon egy együttműködőbb, érettebb szakmai kultúra kialakulásához.

Ha az Olvasó úgy érzi, hogy fontos szempont vagy téma maradt ki, örömmel vesszük, ha csatlakozik az esetleges jövőbeli felülvizsgálati munkához. Ráadásul létrehoztunk egy tárhelyet, ahol olyan anyagokat tettünk közzé, melyet mindenki használhat tesztelési, gyakorlási célokra. Külön öröm lenne, ha ezek az idő előrehaladtával fejlődnének az Olvasók és a szakma által, és egy kicsit tudnánk folyamatosan segíteni egymást még a nagy felkészülési és auditálási munkák mellett is.

A NIS 2 hatálybalépése új fejlődési, tanulási folyamatot indított el az európai és benne a magyarországi szakemberek számára. Ennek mi is aktív formálói kívánunk lenni ezzel a dokumentummal. Bátorítunk mindenkit, hogy kapcsolódjon be ebbe a közös munkába akár közvetlenül ehhez a projekthez, akár más módokon. Mert minél többen osztjuk meg tudásunkat, tapasztalatainkat, annál jobban tudunk alkalmazkodni a kihívásokhoz. Így járulhatunk hozzá a NIS 2 eredeti céljához: a kiber-ellenállóbb és biztonságosabb jövőhöz Európában és így Magyarországon.

02

Jogszabályi háttér

Az európai és hazai kiberbiztonsági szabályozások folyamatos fejlődésének célja, hogy a digitális infrastruktúrák és szolgáltatások biztonságát egységes, hatékony keretek között garantálják. E folyamat legújabb mérföldköve az EU NIS2 irányelve, amely jelentősen bővíti a korábbi szabályozási kört, szigorúbb követelményeket ír elő, és közvetlen hatással van a tagállamok nemzeti szabályozására is. Ez a fejezet áttekinti az NIS2 irányelv alapvető céljait, majd bemutatja a magyarországi implementáció jogszabályi kereteit, különös tekintettel az érintett szervezetek kötelezettségeire és a hazai jogrendszerbe.

2. Jogszabályi háttér

Írták: dr. Szabó László, dr. Szilágyi Emese, Dr. Bederna Zsolt, Dr. Váczi Dániel

2.1. A NIS2 célja

A digitalizáció gyors fejlődése és az egységes belső piac működésének biztosítása már a 2000-es évek elején szükségessé tette a kiberbiztonság közösségi szintű szabályozását. Az uniós tagállamok felismerték, hogy a kibertérből érkező fenyegetések nemcsak gazdasági, hanem alapvető jogokat is érintő biztonsági kockázatokat jelentenek. a harmonizált szabályozás célja ezért az volt, hogy közös alapokra helyezze a védekezést, különösen a kritikus infrastruktúrák védelme érdekében, amelyek működése alapvető a társadalom és a gazdaság szempontjából egyaránt.

> A 2004. évi madridi terrortámadás, amely a kritikus infrastruktúrák átfogó szabályozásához vezetett; a 2007. évben Észtországot, 2008. évben Grúziát ért kibertámadások világossá tették, hogy a kibertérben véghez vitt cselekmények kockázata az államok szemszögéből nem merül ki a gazdasági károkban vagy korlátozott hozzáférésű adatok illetéktelen kézbe kerülésében, hanem egy-egy nagyobb volumenű támadás akár az állam – és közösségeik – működését is veszélyezteti.

Az uniós kiberbiztonsági stratégia megfogalmazása és az első NIS irányelv kodifikációs folyamata 2013-ban indult meg; stratégia alcíme egy nyílt, biztonságos és megbízható kibertér volt.

A folyamat részeként az európai biztonság kiterjesztésének két pillére: az adatvédelem körében a GDPR[1], és a hálózatbiztonság körében a NIS 1[2] irányelv, két különböző aspektusból és két különböző cél érdekében (adatilletve hálózatvédelem) támasztott eléggé hasonló elvárásokat, ideértve biztonsági előírásokat és incidens bejelentési kötelezettséget. Míg a NIS 1 irányelv geopolitikai alapon harmonizációra törekedve írt elő minimumszabályokat és kötelező együttműködési mechanizmusokat a tagállamoknak, addig a GDPR rendeletként továbbra is közvetlenül alkalmazandó.

E helyütt tartjuk szükségesnek megemlíteni, hogy az IKT termékek ellenállóképességének kialakítását, valamint robosztusabbá tételét célzó Uniós jogforrások, miként a fent említett irányelv és az adatvédelmi rendelet adatbiztonságra vonatkozó rendelkezései által képviselt ex ante szabályozás nem kizárólagos jellegű. a kibertér biztonságát érintő váratlan események, amelyek alááshatják a felhasználóknak a technológiába, a hálózatokba és a szolgáltatásokba vetett bizalmát, az EU a büntetőjog eszközeivel is védeni kívánja, amelyek szankciós, épp ezért ex post típusú megközelítése kevéssé tűnik hatékonynak, mert az elkövetett cselekmények globális háttere nehezíti a felderítést, továbbá az esetlegesen kiszabott büntetés nem feltétlenül tartja vissza a további, potenciális elkövetőt. Ennek ellenére az említett felhasználói bizalom megtartása a jogalkotó szerint szükségessé teszi az ilyen jellegű szabályozást, amelynek gyökerei az 1986-os

1 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg)

2 Az Európai Parlament és a Tanács (EU)2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (nincs hatályban)

OECD[3] jelentésig vezethetőek vissza. a jelentés elsődleges célja a számítógépes környezetben elkövetett bűncselekmények megismerése és a kodifikáció elősegítése volt. E tárgykörben az Unió által kibocsájtott első ilyen jellegű dokumentum a Tagállamok Tanácsának No. R (89) 9-sz számú, számítógépes bűncselekményekről szóló ajánlása[4] volt, amely tartalmazta azon bűncselekmények minimumlistáját, amelyeket a tagállamoknak a kibertérben elkövetett cselekmények körében büntetendővé kellett nyilvánítaniuk. E szabályozási folyamat, amelynek nemzetközi közjogi állomása az Európa Tanács Számítástechnikai bűnözésről szóló 2001. évi Budapesti Egyezménye volt, a 2013/40/EU irányelvben konkludált, amely esetében a jogalkotó azt tűzte ki célul, hogy ugyanaz a – kiberteret érintő – bűncselekmény valamennyi tagállamban büntetendő legyen.

E tárgykörhöz tartozik továbbá az Európai Unió Kiberbiztonsági Ügynökségének (European Union Agency for Cybersecurity, ENISA) létrehozásának kérdése, ugyanis a NIS 2 irányelv és az ENISA kapcsolata kulcsfontosságú az EU kiberbiztonsági stratégiájában. a 2023-ban hatályba lépett NIS 2 irányelv jelentősen kibővítette az egyébként az Európai Tanács 2004/97/EK határozattal létrehozott, jelenleg a Cybersecurity Act (EU) 2019/881[5] által szabályozott ENISA szerepét és feladatait az uniós kiberbiztonság megerősítése érdekében. a NIS 2 a rendelethez képest tovább bővítette az ügynökség feladatkörét a tárgyalt irányelv végrehajtásának tekintetében is, úgy mint technikai támogatás nyújtása a tagállamoknak a NIS 2 nemzeti jogba való átültetése során, valamint a CSIRT-ek hálózatát (Computer Security Incident Response Team) és a Koordinációs Csoport munkájának segítését. a 2016-ban elfogadott NIS 1 irányelv választ kívánt adni a növekvő és súlyosbodó biztonsági eseményekre. a minimum harmonizációt az események gazdasági tevékenységek folytatását nehezítő, pénzügyi veszteségeket okozó hatása indokolta (pl.: egy hackertámadás okozta leállás és helyreállítás idő- erőforrás vesztesége), transznacionális jellege és az egyes tagállamok eltérő felkészültségi szintje. a NIS 1 megteremtette a kiberbiztonsági együttműködés és (incidenskezelés és -elemzés szintű) reagáló képesség alapjait, szabályozta a közösségi szintű feladatokat, előírta a nemzeti stratégiák, a szakosított szervezetek és a tagállami CSIRT-ek hálózata létrehozását. a NIS 1 kiemelt célterületei a hatékonyság jegyében a rendszerek elleni fenyegetések mérséklése és az események során a szolgáltatások folyamatosságának biztosítása.

A NIS 1 irányelv tagállami átültetése és a nemzeti jogszabályok harmonizációja 2016 és 2018 között valósult meg, a nemzeti szabályokat 2018. május 10-től kellett alkalmazni.

Amint a NIS 2 irányelv preambulumából is kitűnik, a NIS 1 célkitűzései és rendszere előremutatónak bizonyultak, azonban a tagállamok eltérő módon hajtották végre azt. Ezek a jelentős eltérések a belső piac széttöredezettségét eredményezték, ami károsan befolyásolta annak működését, ezért elkerülhetetlenné vált a NIS 1 felülvizsgálata. a szabályok felülvizsgálata szükségessé vált a digitális átalakulás és a hálózati rendszerek széles körű használata miatt is. Az alapszolgáltatások, mint a közlekedés, vízellátás, hulladékkezelés, világítás fejlesztése és digitalizációja, valamint az innovatív technológiák (például a mesterséges intelligencia) megjelenése tovább bővítette a biztonságos működés

3 OECD (1986). Computer-related criminality: Analysis of legal politics in the OECD area. Paris: OECD.

4 Európa Tanács Miniszteri Bizottsága R (89) 9. számú ajánlása (Recommendation No. R (89) 9 of the Committee of Ministers to Member States on computer-related crime, 1989. szeptember 13.)

5 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg)

védendő kereteit. Emellett a COVID-19 világjárvány[6] is rávilágított a digitális megoldások gazdasági jelentőségére és az ellátási láncok sérülékenységére.

Az Európai Bizottság 2020 decemberében terjesztette elő a NIS 2 irányelvre vonatkozó javaslatát, amelyet az uniós jogalkotók 2022 novemberében fogadtak el.

A NIS 2 célja a tagállamok közötti eltérések kiküszöbölése, a hatóságok együttműködése és a védendő ágazatok listájának aktualizálása. a NIS 2-vel az egységes magas szintű kiberbiztonság Unión belüli elérése céljából az eddig ágazatokon alapuló alkalmazási kört kiterjesztette a gazdaság nagyobb részére, továbbá a jogbiztonság érdekében egységes kritérium rendszert, méretküszöb-szabályt alkalmazott, mellyel az érintettek körébe bevonta az irányelv hatálya alá tartozó ágazatban működő középvállalkozásokat, illetve egyes ágazatok esetén a mérettől független szereplőket is (pl.: bizalmi szolgáltatók).

Kiemelendő, hogy a NIS 2 Preambulumában deklaráltan a reaktív reagálás helyett az aktív kiberbiztonságot helyezi előtérbe, melynek sajátja a megfelelő eszközök megléte az észleléshez, riasztások és válaszintézkedések gyors és automatikus megosztásához és megértéséhez.

Hangsúlyossá vált a technikai és szervezeti képességek kialakítása, az események és kockázatok megelőzése, észlelése és azokra reagálás. a NIS 1-hez képest erőteljesebb mértékben került előtérbe a CSIRT-ek eseménykezelés feladata. Emellett kiemelt tagállami feladat lett a nemzeti stratégiák keretében a KKV-k sajátos kiberbiztonsági igényeinek kezelése, a kibertudatosság növelése és erősítése, ideértve a beszállítóként megjelenő vállalkozásokkal kapcsolatos kérdéseket is.

A NIS 2 céljait akként látta megvalósíthatónak, ha az eddig ágazatokon alapuló alkalmazási kört kiterjeszti a gazdaság nagyobb részére,

A NIS 2 fő céljai közé tartozik:

- az ellenállóképesség növelése a hálózati és információsrendszerekben,
- a kiberfenyegetések elleni hatékony védekezés,
- a belső piac zavartalan működésének biztosítása,
- valamint a tagállamok közötti együttműködés javítása.

továbbá a jogbiztonság érdekében egységes kritérium rendszert, méretküszöb-szabályt alkalmaz, mellyel az érintettek körébe bevonta az irányelv hatálya alá tartozó ágazatban működő középvállalkozásokat, illetve egyes ágazatok esetén a mérettől független szereplőket is (pl.: bizalmi szolgáltatók).

Egységes uniós követelmény ként írja elő a magas szintű kiberbiztonsági védettségi szint elérését a gazdaság működése szempontjából fontos szervezetek számára, korszerű védelmi intézkedések és technológia bevezetésével, alkalmazásával, valamint az incidensek bejelentési kötelezettségének szigorításával. Az irányelv egyértelmű célja a kibertámadások és más fenyegetések megelőzése, a már bekövetkezett támadások negatív hatásainak csökkentése, valamint a tagállamok összehangolt együttműködésével egy egységes „védelmi háló” felépítése.

A NIS 2 szabályozás közösen értelmezendő az EU adatstratégiájával, kiberstratégiájával, valamint az EU Digitális Nyilatkozattal. Az EU adatstratégiája központi szerepet játszik a digitális gazdaság fejlődésében, mivel célja egy egységes európai adatpiac létrehozása, ahol az adatok biztonságosan és jogszerűen áramolhatnak a tagállamok között. a kiberstratégia ezzel összhangban megerősíti az Unió ellenállóképességét a kibertámadásokkal szemben, és meghatározza

6 Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs

azokat a védelmi kereteket, amelyek elengedhetetlenek a digitális szolgáltatások megbízható működéséhez. Az EU Digitális Nyilatkozat[7] pedig rögzíti a polgárok és vállalkozások digitális jogait és elvárásait, biztosítva, hogy a digitális átmenet emberközpontú, biztonságos és fenntartható módon történjen. Ezek a kezdeményezések szorosan kapcsolódnak a NIS 2 irányelvhez, mivel annak célja, hogy az uniós szinten meghatározott elvek mentén egységes, magas szintű kiberbiztonságot teremtsen. a gazdaság- és társadalom mindennapi működésében, az új technológiák kifejlesztése és bevezetése során is referenciapontként kell szolgáljanak.

A NIS 2 irányelv azon törekvése, hogy – elődjével összevetve – célzottan szűkítse a tagállamok mozgásterét a hatálya alá tartozó ágazatok kiberbiztonsági szabályozásának tekintetében, nem jár együtt azzal, hogy hatályát tekintve, kizárólagos jogforrásként kívánjon funkcionálni. a kizárólagosságra törekvés hiányában sem beszélhetünk azonban, az egyes, specifikus szabályozások esetében az irányelvtől független regulációról, hiszen az irányelv 4. cikke maga ad lehetőséget ágazatspecifikus uniós jogi aktusok megalkotására és ezt meghaladóan kapocsként működik az egyes – mint az eIDAS[8] rendelet módosítása esetén később látni fogjuk – már hatályos, illetve a későbbiekben hatályba lépő, a NIS 2-ben meghatározottaknál specifikusabb előírásokat igénylő gazdasági ágazatok vonatkozásában.

Ahhoz azonban, hogy el tudjuk dönteni, vonatkozik-e ágazatspecifikus jogforrás az általunk vezetett, vagy felelősségi körünkbe tartozó szervezet tekintetében, valamint, hogy az általános-különös szabályozás mely ágazatok esetében és azon belül milyen hatállyal valósul meg, a következőkben felsoroltakat kell figyelembe vennünk.

Az irányelv említett 4. cikke, valamint az ezzel kapcsolatban a Bizottság által kiadott, 2023/C 328/02 számú közlemény is megállapítja, hogy speciális szabályozás kizárólag csak az irányelv szerinti alapvető vagy fontos szervezetek esetében állhat fenn, azaz a NIS 2 és egy ágazatspecifikus uniós jogi aktus vonatkozásában mintegy „moduláris", egymást kiegészítő szabályozási formát láthatunk. Ez a megállapítás nyilvánvalóan nem bír revelatív jelleggel, hiszen egy speciális szabályozás megléte eleve feltételezi a hozzá képest valamilyen tekintetben generális szabályozás létezését. Azonban a fenti észrevétel egyértelműségét árnyalja, hogy úgy az irányelv, mint az említett bizottsági közlemény is kimondja, hogy amennyiben az ágazatspecifikus uniós jogi aktusok hatálya nem terjed ki az irányelv hatálya alá tartozó, adott ágazatban működő valamennyi szervezetre, az említett irányelv (azaz a NIS 2) vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus uniós jogi aktusok hatálya alá. Röviden: amely speciális szabály adott ágazatban (pl.: „gyártás") nem fed le minden alágazatot, csak a „villamos berendezések gyártását", a „gyártás" ágazat „villamos berendezések" alágazatára vonatkozó szabályozás hatályán kívül eső alágazatokra a NIS 2 rendelkezései – további szabályozás hiányában – kizárólagosan alkalmazandóak.

Az ágazati szabályozás hatályának tekintetében utolsóként figyelembe veendő elem, hogy a főszabálytól, azaz az irányelvtől való eltérést a NIS 2 azokban az esetekben engedi, ha az (a) kiberbiztonsági kockázatkezelési intézkedésekre, vagy (b) jelentős biztonsági események bejelentésével függ össze. E követelményeknek – a 4. cikk alapján – hatásukban legalább egyenértékűek kell lenniük a NIS 2 irányelvben meghatározott kötelezettségekkel. Ebben az esetben az (EU) 2022/2555 irányelv vonatkozó

7 EURLEX

8 AZ EURÓPAI PARLAMENT ÉS a TANÁCS 910/2014/EU RENDELETE

rendelkezései – beleértve az említett irányelv VII. fejezetében meghatározott, a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket – nem alkalmazandók az említett, specifikus szabályozással érintett szervezetekre.

A fenti, ágazatspecifikus uniós aktusok tipizálásával összefüggésben három példát szeretnék felhozni, amelyek a speciális kiberbiztonsági rendelkezések és a komplementer szabályozás által végpontokként kijelölt skálán helyezkednek el.

A sokszor ismételt ágazatspecifikus uniós aktusok ideáltipikus reprezentánsa a EU 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, amely tervezetten a NIS 2 irányelv I. Mellékletében felsorolt banki szolgáltatások és pénzügyi piaci infrastruktúrák ágazataira vonatkozó, közvetlenül alkalmazandó és hatályos Európai Uniós jogforrás. a mai napig ez az egyetlen olyan ágazatspecifikus uniós jogi aktus, amelyet a Bizottság vonatkozó 2023/C 328/02 közleményének melléklete tartalmaz.

E körben értelmezhető az Európai Parlament és a Tanács 910/2014/EU számú rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS rendelet), amely a Digitális infrastruktúra ágazatán belül a bizalmi szolgáltatókra, mint alapvető szervezetekre vonatkozóan tartalmaz, méretüktől függetlenül, előírásokat.

Utolsó példánk az (EU) 2022/2557 irányelve[9] a kritikus szervezetek rezilienciájáról, amely – bizonyos kritikus infrastruktúrák tekintetében – azok ellenállóképességének kialakításával, kockázatelemzésével és válságkezelési tervének elkészítésével kapcsolatos kötelezettségeket telepít az ilyen infrastruktúrát működtető szervezetekre. Lényeges különbség a két tárgyalt irányelv között, hogy míg a NIS 2 a hálózati és információs rendszerek védelme, addig a kiberreziliencia irányelv a fizikai és általános működési ellenállóképességére fókuszál, így a két jogforrás egymás komplementereként funkcionál. Ezt erősíti a kritikus szervezetek rezilienciájáról szóló irányelv azon rendelkezése is, amely előírja, hogy az irányelv nem alkalmazandó az (EU) 2022/2555 irányelv, azaz a NIS 2 hatálya alá tartozó kérdésekre.

Ezen túlmenően a Bizottság 2024. október 17-i (EU) 20024/2690 végrehajtási rendelete tartalmamz további többlet rendelkezéseket. Ezek elsősorban technikai és módszertani szabályok a DNS szolgáltatók, a legfelső szintű domain-név nyilvántartók, a felhőszolgáltatók, az adatközpontok, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok, vagy közösségi média szolgáltatási platformok tekintetében, a jelentősnek minősülő biztonsági események pontosítása tekintetében történő alklamazásra vovnatkozó követelményeket fogalmaz meg. Lényege, hogy a NIS2 hatálya alá tartozó fenti speciális szervezetek tekintetében meghatározott technikai és módszertani követelmények alapja európai és nemzeteközi szabványok, úgy mint, a ISO/IEC 27001, ISO/IEC27002, ETSI EN 319401 szabvány, valamint a hálózati és információs rendszerek biztonsága szempontjából releváns műszaki előírások, pl: CEN/TS 18026:2024.

A NIS2 irányelv implementációja az egyes tagállamokban az elmúlt év során eltérő ütemben zajlott. 2024. novemberében a Bizottság mintegy 23 tagállam ellen indított kötelezettségszegési eljárást az átültetés késedelme miatt. (www. Gyakorlati tapasztalatként elmondható, hogy az országonként elétrő részletszabályok, valamint a

9 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)

tagállami hatóságok párhuzamos hatáskörei miatti ellentmondások az egységes jogalkalmazási gyakorlat ellen hatottak. A leggyakoribb átültetési problémák az alábbiak voltak:

- illetékes hatóság (minisztérium vagy külön kibervédelmi hatóság)
- a NIS2 hatálya alá tartozó szervezetek defeiniálása nem volt egyyértelmű
- szakértelem hiánya (szervezeti és auditori oldalon)
- regisztrációs rendszerek hiánya vagy nem megfelelő volta
- más jogszabályokkal történő átfedés, párhuzamos szabályozás (DORA, CRA)
- kiépítetlen auditor rendszere, illetve audit struktúra.

Az utóbbi időszakban egyre erősödik az a felfogás, hogy a NIS2 kötelezettségek nem csupán egy joganyagnak történő megfelelés, hanem egy komplex EU Cyber szabályozási csomag része, ennélfogva egy komplex, compliance alapú keretrendszer kialakítása szükséges. Ennek részeként a szabályozás hatálya alá eső szervezetek pontosabb, körülhatároltabb meghatározása indokolt. Mindezek okán egyes tagállamok további bővítik az irányelv alkalmazási területét (pl.: Olaszország). A nemzeti implementációban olyan új iprarágak is kezdenek megjelenni, mint pl: védelmi, nukleáris ipar, egyes gyártóipari ágazatok.

Összességében az elmúlt egy év jelentős jogi diverzitást eredményezett az egyes tagállamok között. Ez a változás nem kedvez az EU szintű egységes jogalkalmazásnak, amely az NIS2 irányelv eredeti célkitűzése is volt.

NIS 2 főbb újításai a NIS 1-hez képest:

- **Tágabb hatály:** több ágazat (digitális infrastruktúra, közigazgatás, IKT-szolgáltatók, online piacterek, közösségi média, világűr stb.) kerül a szabályozás alá
- **Szerepkategorizálás:** megszűnik az alapvető szolgáltatók vs. digitális szolgáltatók elkülönítése; helyettük az alapvető és fontos szervezetek egyértelmű besorolása történik
- **Kockázatalapú követelmények:** szigorúbb, részletes szabályok kockázatelemzésre, ncidenskezelésre, ellátási lánc biztonságára, kriptográfiára és többtényezős hitelesítésre.
- **Beszállítói lánc felelősség:** a biztonsági megfelelés kiterjed a beszállítókra is, különösen az IKT rendszerek terén.
- **Szankciók szigorítása:** jelentős bírságok – alapvető szervezeteknél minimum 10 millió EUR vagy 2% árbevétel, fontos szervezeteknél 7 millió EUR vagy 1,4% árbevétel.
- **Tagállami kötelezettségek:** kötelező kiberbiztonsági stratégia, CSIRT-ek, válságkezelési keret, együttműködési hálózatok (pl.: EU-CyCLONe)
- **ENISA szerepvállalás:** európai sebezhetőségi adatbázis kezelése, rendszeres jelentések, kritikus szereplők nyilvántartása

A Bizottság 2024. október 17-i (EU) 20024/2690 végrehajtási rendelete tartalmaz további rendelkezéseket, melyek elsősorban technikai és módszertani szabályok a DNS szolgáltatók, a legfelső szintű domain-név nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, az irányított biztonsági szolgáltatók, az

online piacterek, online keresőprogramok, vagy közösségi média szolgáltatási platformok tekintetében, a jelentősnek minősülő biztonsági események pontosítása tekintetében történő alkalmazásra vonatkozó követelményeket fogalmaz meg. Lényege, hogy a NIS2 hatálya alá tartozó fenti speciális szervezetek tekintetében meghatározott technikai és módszertani követelmények alapja európai és nemzetközi szabványok, úgy mint, a ISO/IEC 27001, ISO/IEC27002, ETSI EN 319401 szabvány, valamint a hálózati és információs rendszerek biztonsága szempontjából releváns műszaki előírások, pl: CEN/TS 18026:2024.

A NIS2 irányelv implementációja az egyes tagállamokban az elmúlt év során eltérő ütemben zajlott. 2024. novemberében a Bizottság mintegy 23 tagállam ellen indított kötelezettségszegési eljárást az átültetés késedelme miatt. Gyakorlati tapasztalatként elmondható, hogy az országonként eltérő részletszabályok, valamint a tagállami hatóságok párhuzamos hatáskörei miatti ellentmondások az egységes jogalkalmazási gyakorlat ellen hatottak. A leggyakoribb átültetési kihívások az alábbiak voltak:

- illetékes hatóság (minisztérium vagy külön kibervédelmi hatóság) kijelölése, valamint feladatköreinek meghatározása
- a NIS2 hatálya alá tartozó szervezetek nem egyértelmű meghatározása
- szakértelem hiánya (szervezeti és auditori oldalon egyaránt)
- regisztrációs rendszerek hiánya vagy nem megfelelő működése
- más jogszabályokkal való átfedések, párhuzamos szabályozás (DORA, CRA)
- kiépítetlen auditor rendszer, illetve audit struktúra.

Az utóbbi időszakban egyre erősödik az a felfogás, hogy a NIS2 kötelezettségek teljesítése nem csupán egy jogszabálynak történő megfelelés kell, hogy legyen, hanem az uniós kiberbiztonsági szabályozási csomag részeként egy komplex, compliance- alapú keretrendszer kialakítása szükséges. Ennek következtében indokolttá vált a szabályozás hatálya alá eső szervezetek pontosabb, körülhatárolt meghatározása. Mindezekre tekintettel egyes tagállamok az irányelv alkalmazási körét tovább bővítik (pl.: Olaszország). A nemzeti implementáció során olyan új iparágak is megjelennek a szabályozás hatálya alatt, mint pl: védelmi, nukleáris ipar, egyes gyártóipari ágazatok.

Összességében az elmúlt egy év jelentős jogi diverzitást eredményezett az egyes tagállamok között. Ez a változás nem kedvez az EU szintű egységes jogalkalmazásnak, amely az NIS2 irányelv egyik eredeti célkitűzése is volt.

Magyarország a fenti implementációs kötelezettségeinek a 2024. LXIX. törvény elfogadásával eleget tett.

2.2 Kapcsolódó EU szabályozások és tanúsítási keretrendszerek a NIS2 kontextusában

A NIS2 irányelv az Európai Unió kiberbiztonsági szabályozási architektúrájának központi eleme, amely a kritikus és fontos szervezetek számára kockázatalapú kiberbiztonsági irányítási- és incidenskezelési kötelezettségeket ír elő. Ugyanakkor a megfelelési követelmények értelmezése és gyakorlati megvalósítása szorosan összefügg más uniós jogszabályokkal és kiberbiztonsági keretrendszerekkel, különösen az EU AI Act-tel, a Cybersecurity Act-tel, valamint a Cyber Solidarity Act-tel.

Az AI Act (Regulation (EU) 2024/1689)[10] az első átfogó európai szabályozás a mesterséges intelligencia rendszerekre, amely a technológiát kockázati kategóriák szerint szabályozza. A magas kockázatú AI-rendszerek esetében a rendelet kötelező követelményeket határoz meg többek között a robosztusság, a biztonság és a kiberbiztonság területén.

E követelmények közvetlenül kapcsolódnak a NIS2 irányelvben meghatározott szervezeti kiberbiztonsági kötelezettségekhez. A NIS2 a kritikus és fontos szervezetek számára előírja többek között:

- a kiberbiztonsági kockázatkezelési intézkedések bevezetését,
- az ellátási lánc biztonságának biztosítását,
- valamint a jelentős incidensek bejelentését az illetékes hatóságok felé.

Amennyiben egy szervezet AI-alapú rendszereket használ kritikus szolgáltatások nyújtásához, a két szabályozás együttesen alkalmazandó: az AI Act a technológia biztonságos tervezésére és működésére vonatkozó követelményeket határozza meg, míg a NIS2 az adott szervezet kiberbiztonsági irányítási és működési felelősségét szabályozza.

A Cybersecurity Act (Regulation (EU) 2019/881)[11] létrehozta az EU kiberbiztonsági tanúsítási keretrendszerét, amely harmonizált módszert biztosít az informatikai termékek, szolgáltatások és folyamatok biztonsági szintjének igazolására.

A tanúsítási keretrendszer egyik első konkrét megvalósítása az EU Common Criteria (EUCC) tanúsítási séma, amely az ICT-termékek – például hardverek, szoftverek és hálózati eszközök – biztonsági értékelését teszi lehetővé európai szinten. Az EUCC célja, hogy egységes és kölcsönösen elismert tanúsítási rendszert biztosítson az EU digitális piacán.

A Cybersecurity Act alapján további tanúsítási sémák is fejlesztés alatt állnak, például az EU Multi-Stakeholder Scheme (EUMSS, European Union Managed Security Services) jellegű megközelítések vagy az EU-szintű felhőbiztonsági tanúsítási rendszerek, amelyek célja a digitális szolgáltatások és infrastruktúrák biztonságának egységes igazolása.

A NIS2 irányelv szempontjából ezek a tanúsítási mechanizmusok különösen relevánsak, mivel a jogszabály előírja, hogy a szervezeteknek megfelelő és arányos technikai, működési és szervezeti intézkedéseket kell bevezetniük a kiberbiztonsági kockázatok kezelésére. Az EU-szintű tanúsítási sémák alkalmazása segítheti a szervezeteket abban, hogy objektív módon igazolják informatikai rendszereik és beszállítóik biztonsági szintjét, különösen az ellátási lánc biztonsága és a kritikus infrastruktúrák védelme területén.

A Cyber Solidarity Act[12] az EU kibervédelmi együttműködésének új eleme, amely a nagyléptékű kibertámadások elleni közös európai reagálási képességet erősíti. A rendelet többek között létrehozza az European Cybersecurity Alert Systemet (Európai Kiberbiztonsági Riasztási Rendszer), amely összekapcsolja a tagállami és határokon átnyúló kiberbiztonsági műveleti központokat a fenyegetések korai felismerése érdekében.

10 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1689 RENDELETE (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról,

11 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

12 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2025/38 RENDELETE (2024. december 19.) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról

A rendszer szoros kapcsolatban áll a NIS2 által létrehozott incidensjelentési- és információmegosztási mechanizmusokkal, amelyek célja a kritikus infrastruktúrákat érintő kibertámadások gyors és koordinált kezelése az Európai Unió egész területén. A Cyber Solidarity Act emellett létrehozza az EU Cybersecurity Reserve mechanizmust, amely technikai és operatív támogatást biztosíthat a tagállamok számára súlyos kiberbiztonsági incidensek esetén.

2.3. A NIS2 magyarországi jogszabályi háttere

Magyarország már a NIS 1 irányelv átvétele előtt rendelkezett nemzeti kiberbiztonsági stratégiával10 és szabályozással, valamint bizonyos intézményi kerettel a kritikus infrastruktúrák tekintetében. Minderre alapozva a teljesen új szabályozás helyett a meglévő szabályozási- és intézményi keretrendszerbe illesztette az uniós elvárásokat.

> A NIS 1 irányelvnek megfelelő nemzeti szabályokat 2018. május 9-ig kellett elfogadni és 2018. május 10. naptól alkalmazni, míg az irányelvben meghatározott alapvető szolgáltatásokat nyújtó szereplők (II. melléklet szerinti valamennyi alágazat vonatkozásában az adott tagállam területén letelepedettek) tagállam általi azonosítása 2018. november 9-ig kellett megvalósuljon.

A 2013-as kiberbiztonsági stratégia kiegészítésével és az ágazati stratégiák elfogadásával az ország az uniós megfelelést szolgálta. Az alapvető szolgáltatásokat nyújtó szereplők (energia, közlekedés, pénzügy, egészségügy, ivóvíz, digitális infrastruktúra) nagyrészben azonosítható voltak, így a kritikus infrastruktúrák esetén a meglévő szabályozás NIS 1 szerinti kiegészítésével, míg a digitális szolgáltatók új szabályozással kerültek be a rendszerbe11. A NIS 1 incidensbejelentésre vonatkozó szabályaival (jelentős hatás fogalmának bevezetése, illetve indokolatlan késedelem nélküli bejelentési kötelezettség) kiegészítették az eseménykezelő központok feladatairól szóló Kormányrendeletet, míg az érintett szektorok szabályozása Kormányrendeletekkel12 ágazatonként történt. A digitális szolgáltatókra vonatkozó szabályok az elektronikus kereskedelemhez és az információs társadalommal kapcsolatos szolgáltatásokhoz-kapcsolódvakerültekszabályozásra.[13]

> A kormány szektorális stratégiaként 2018 decemberében fogadta el a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozatot. Ebben megfogalmazta „az új kiberbiztonsági kihívásokat és fejlesztésekre való célkitűzéseket, a kibertér biztonságos használatát célzó gyakorlati tudást elősegítő, tudatosító tevékenységek szakosított intézmények általi támogatását, illetve a kutatás fejlesztés kiemelését is a digitális állam megvalósítása körében”.

Az intézményi rendszert tekintve, a létfontosságú létesítmények, rendszerek biztonsága esetén a felügyeletet a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) látta el, míg eseménykezelőként a Nemzetbiztonsági Szakszolgálat (NBSZ) -azon belül a kormányzati eseménykezelő központ (GovCERT)- járt el. Az új szabályozás eredményeként a bejelentés-köteles szolgáltatók felügyeletét és eseménykezelését az NBSZ Nemzeti Kiberbiztonsági Intézet vette át 2019-től.

13 Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm.határozat

A NIS 2 irányelvnek megfelelő hazai jogszabályi környezetet[14] az első uniós tagállamok között a 2023. évi XXIII. törvény (Kibertan.tv.) elfogadásával alakították ki, amely 2024. október 18-ig több lépcsőben lépett hatályba.

Az új törvény az érintett szervezeteket kritikussági szint szerint sorolta be – a Kiemelten kockázatos ágazatokat (alapvető szervezetek), valamint a Kockázatos ágazatokat (fontos szervezetek) külön jelölve, és önazonosítás keretében került sor olyan szektorok bevonására is, amelyek eddig nem foglalkoztak információbiztonsággal. Az érintettek meghatározása a NIS 2 szerinti méretkorlát (középvállalatok – 50 főnél több foglalkoztatott vagy 10 millió EUR feletti éves árbevétel) és a méretkorláttól függetlenül a hatálya alá tartozó egyes ágazatokra figyelemmel történt. A Kibertan.tv. célja egy jól működő, kockázatokkal arányos információbiztonsági irányítási keretrendszer létrehozása és működtetése volt.

A NIS 2 szerint előírt nemzeti kiberbiztonsági tanúsító hatóságként általános jelleggel a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH) jelölték ki, míg a hadiipari K+F, gyártás esetén külön hatóság jár el. A Kibertantv-ben foglalt követelmények tekintetében az érintett szervezetek, valamint azok EIR kiberbiztonsági felügyeletét szintén az SZTFH látja el. Az SZTFH elnöke rendeleti szinten szabályozza a tanúsító hatósági tevékenység eljárásrendjét, a nyilvántartási feladatokat, a tanúsított IKT termékek, auditorok nyilvántartásba vételi rendjét és velük szembeni követelményeket, kiberbiztonsági felügyeleti díjat, az audit eljárásrendjét stb.

Emellett, a Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) szól a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. A jogalkotó a megfelelőségi keretrendszert tovább pontosította az 1/2025. (I. 31.) SZTFH rendelettel (a továbbiakban: SZTFH rendelet), amely meghatározza a kiberbiztonsági audit alapvető szabályait és a díjszabás kereteit. E két rendelet együttesen teremti meg a törvényi szintű előírások gyakorlati alkalmazásának alapját. A részletek a későbbi fejezetekben kerülnek kifejtésre (lásd: 8.1.1 és 8.1.2).

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) még a 1838/2018- as Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló Kormányhatározat égisze alatt született meg, amely egységesítette, kiegészítette és újradefiniálta a korábban a terület két alapvető jogszabályában, az állami és önkormányzati szervek elektronikus információ-biztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) és a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényben (a továbbiakban: Kibertan. tv.) szabályozott területet. A jogalkotás fő célja a 2022-es NIS 2 irányelv hazai jogrendbe való átültetése volt, amely az Európai Unió tagállamai számára egységes és szigorúbb kiberbiztonsági követelményeket ír elő. E törvény végrehajtási szabályait a 418/2024. (X. 30.) Korm. rendelet (a továbbiakban: Kormányrendelet) részletezi, amely meghatározza többek között az érintett szervezetek azonosításának, kötelezettségeinek, valamint a hatósági felügyeleti és ellenőrzési eljárásoknak a kereteit.

Ez a szigorúbb szövetségi követelményrendszer tükröződik vissza Magyarország 2025-ben elfogadott, új Kiberbiztonsági Stratégiájáról szóló 1089/2025. (III. 31.) Korm. határozatban.

14 Létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.), az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény törvény (Ibtv) és végrehajtási rendeleteik

A dokumentum megállapítja, hogy az állami és nem állami szereplők fokozott online jelenléte növeli az ebből a jelenlétből eredő kockázatokat. Az így potenciálisan fennálló, a kibertérből érkező fenyegetések megakadályozása, hatékony elhárítása és kezelése érdekében a jogalkotó célja a magyar IKT hálózatok (és ennek részeként a termékek és szolgáltatások), a gazdaság és társadalom szempontjából alapvető és fontos feladatokat ellátó ágazatok ellenállóképességének növelése és az operatív kapacitásépítés[15].

A tárgyalt törvény 2025. január 1-jén lépett hatályba, ezzel egyidejűleg hatályon kívül helyezve az Ibtv.-t és a Kibertan. tv.-t, mely utóbbi már szintén a NIS 2 irányelv hazai jogba való implementálásának céljával született. Az új jogszabály nem csupán az eddigi szabályokat konszolidálta, hanem számos új intézkedést és kötelezettséget is bevezetett, amelyek közül az egyik legszembetűnőbb újítás az „alapvető" és „fontos" szervezetek kategóriáinak bevezetése, amelyek meghatározása a szolgáltatások kritikussága és a szervezeti méret alapján történik. A két szervezettípus közötti különbségtétel a NIS 2 irányelv logikáját követi.

A kiberbiztonság egységesebb követelményrendszerének Kiberbiztonsági tv. általi bevezetése azonban továbbra sem nem jelenti az egyes, szektorspecifikus jogszabályok megszűnését az olyan ágazatok tekintetében, amelyek nagyobb társadalmi, nemzetgazdasági vagy honvédelmi, illetve nemzetbiztonsági jelentőségüknél fogva részben, vagy egészben eltérő szabályozást igényelnek. Így a kritikus szervezetek ellenálló képességéről szóló törvény (a továbbiakban: Kszetv.) alapján kijelölt kritikus szervezetek és kritikus infrastruktúrák (a továbbiakban együtt: kritikus szervezet), valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) alapján kijelölt, az ország védelme és biztonsága szempontjából jelentős szervezetekétől. A DORA rendelet[16] hatálya alá tartozó kritikus szervezetekre, illetve az ország védelme és biztonsága szempontjából jelentős szervezetekre a törvény kiberbiztonsági felügyeleti rendelkezései nem alkalmazandóak, az incidenskezelési tevékenységre vonatkozó rendelkezések pedig csak a törvényben meghatározott eltérésekkel[17].

A többszintű magyar szabályozás tehát akként épül fel, hogy a törvényi szinten az alap elvárások, míg rendeleti szinten a részletszabályok kerülnek meghatározásra. A megfelelést ugyanakkor egyéb, nem jogszabályi szintű jogforrások is segítik, ideértve különösen szabványokat is, melyek bár nem bírnak kötelező erővel, de a jelentőségük nem elhanyagolható. Felügyeleti hatóságként az SZTFH tájékoztató anyagokkal, míg az NKI útmutatókkal segíti a szervezeteket a jogszabályi előírások értelmezésében.

Példaként említhetők:

- Az audit módszertan a NIST Special Publication 800-53A Revision 5 dokumentum alapján került kialakításra.
- A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete közzétett több útmutatót[18], mely egyrészt megkönnyíti a szervezeteknek az egyes védelmi intézkedések alkalmazását, másrészt, amennyiben a szervezet a korábban hatályos 41/2015. (VII. 15.) BM rendelet szerint alakította ki az információbiztonsági

15 Energetika: 374/2020. Korm.r.; Egészségügy: 246/2015. Korm.r., Pénzügy: 330/2015. Korm.r., Vízgazdálkodás: 541/2013. Korm.r., Közlekedés: 161/2019. Korm.r., Infokommunikációs technológiák: 249/2017. Korm.r., emellett szabályozott: Agrárgazdaság, Társadalombiztosítás, Honvédelem, Közbiztonság-védelem (rendőrség).

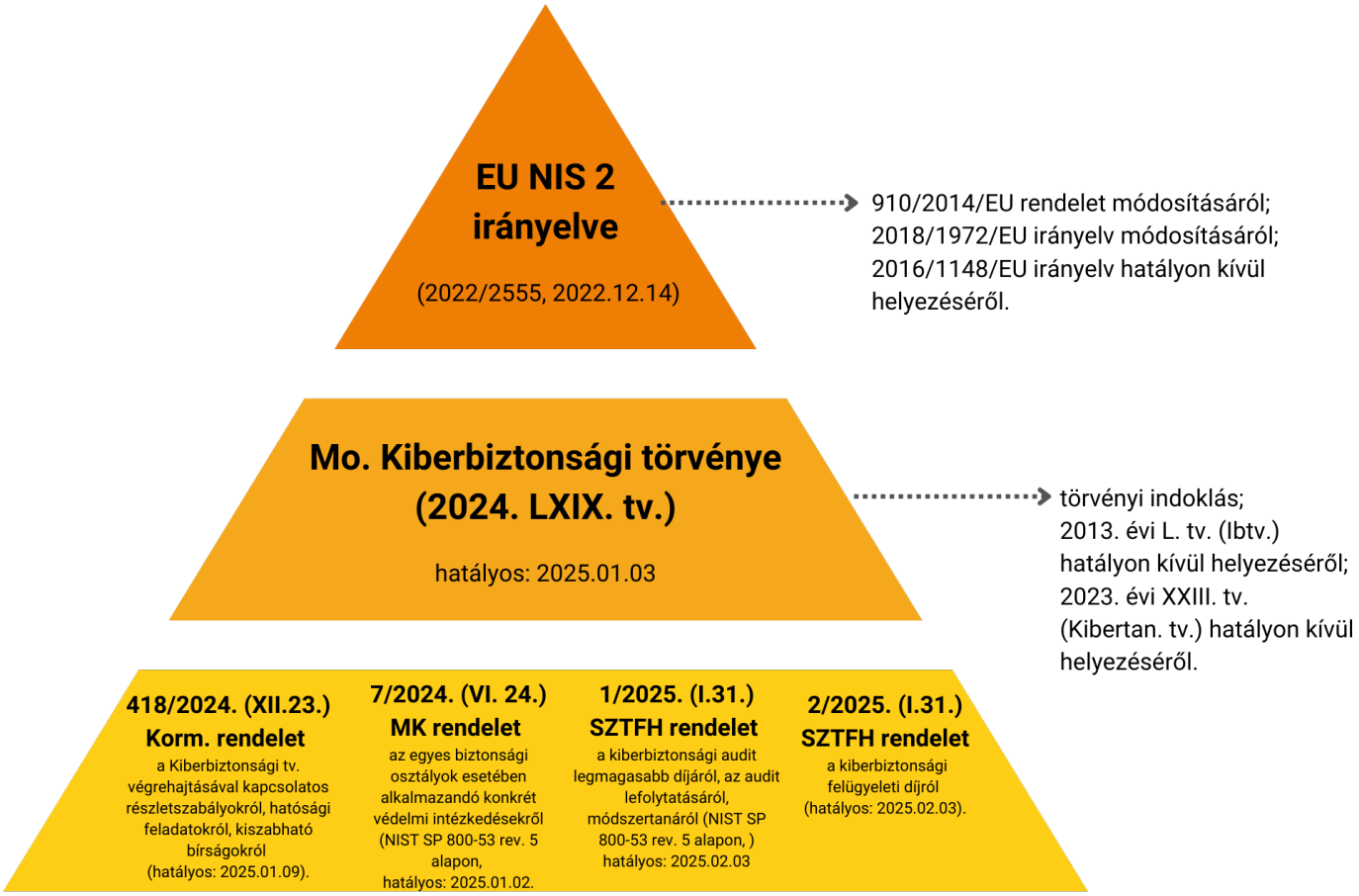
16 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvénybe (Ekertv.)

17 A NIS 2 irányelv tagállami átültetésre 2024. október 17-ig, alkalmazására 2024. október 18-tól kellett sor kerüljön.

18 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiája

szervezetek és infrastruktúrák (a továbbiakban együtt: az ország védelme és biztonsága szempontjából jelentős szervezet) vonatkozásában a hatósági felügyeleti tevékenység elhatárolásra kerül a Kiberbiztonsági tv-ben meghatározott irányítási keretrendszerét, esetleg ISO/IEC 27001:2022 (vagy elődje, az ISO/IEC 27001:2013) alapon tette mindezt, úgy meg tudja feleltetni az egyes kontrollokat az új normában rögzítettekkel.

Megjegyzendő továbbá, hogy a kiberbiztonsági követelményrendszerhez kapcsolódóan több, az érintett szervezetek szempontjából kevésbé közvetlen, de a jogszabályi háttér teljességéhez fontos rendelet is hatályba lépett. A 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díj mértékét és megfizetésének szabályait rögzíti, a 3/2025. (IV. 17.) SZTFH rendelet a felügyeleti és ellenőrzési eljárások részleteit, valamint az információbiztonsági felügyelő szerepét szabályozza, míg az 5/2025. (VI. 20.) SZTFH rendelet a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és természetes személyek nyilvántartására, valamint a velük szemben támasztott követelményekre vonatkozó szabályokat állapítja meg. Bár ezek a rendeletek nem minden esetben érintik közvetlenül a jogszabály hatálya alá tartozó szervezeteket, mégis fontosak a kiberbiztonsági ökoszisztéma egységes működése és a piaci szereplők hitelesítése szempontjából.



1. ábra (Forrás: MOORE Hungary – ACPM IT Tanácsadó Zrt)

A finomhangolás folyamata

A 2026-ban a kiberbiztonsági felügyeleti hatóságok várhatóan tovább folytatják a finomhangolást a jogszabályi megfelelőséggel kapcsolatos jogalkalmazási gyakorlat fejlesztésében.

Általánosságban elmondható, hogy ez az időszak a végrehajtásról és a megfelelések ellenőrzéséről, valamint a szankciók alkalmazásáról fog szólni. Egyelőre a szervezetek együttműködési hajlandósága okán, valamint a kialakulóban lévő joggyakorlat miatt jelentősebb szankciós hullámról nem lehet beszámolni. Ehhez az a körülmény is hozzájárul, hogy az auditok nem léptek a hatósági döntés szakaszába, vagyis a jogorvoslati igény eddig nem nyílt meg a felek számára.

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 2026. január 1-től hatályos legfontosabb változásai az alábbiak:

1) Hatály és érintett szervezetek: Az éves nettó árbevétel számításának szabályait pontosításra került, különösen vállalatcsoportok esetén, hogy jogalkalmazás szempontjából egyértelmű legyen, mely szervezetek esnek a törvény hatálya alá. Új feltétel a szervezet azonosításánál, hogy az alapvető vagy fontos besorolás esetén akkor is hatály alá kerülhet, ha legalább 5 más, a törvény hatálya alá tartozó szervezetnek nyújt szolgáltatást. A törvény hatálya alá kerülés és a hatály alóli kikerülés időpontját részletesebben került rögzítésre.

2) Vezetői kötelezettségek: A szervezet vezetője köteles együttműködni a kiberbiztonsági hatósággal, és a szervezetet érintő változásokat 15 napon belül átvezetni a nyilvántartásban.

3) Biztonsági osztályba sorolás: Ha a biztonsági osztály a szervezet hátrányára változik, a magasabb osztályhoz tartozó kontrollintézkedéseket 2 éven belül kell megvalósítani.

4) Audit és auditori nyilvántartás: Az első kiberbiztonsági auditot a nyilvántartásba vételt követő 2 éven belül kell elvégezni és az auditori nyilvántartásban bekövetkező változások 5 év elteltével kerülnek törlésre.

5) Hatósági eljárások és határidők: Az SZTFH számára a hatósági ellenőrzés lefolytatására 120 nap áll rendelkezésre, egyéb eljárásoknál az eljárási határidő 90 nap. A sommás eljárás tilos. Elektronikus adatok ideiglenes hozzáférhetetlenné tétele 90 napig engedélyezett, további 90 nappal meghosszabbítható.

6) Sérülékenységvizsgálat és incidenskezelés: A sérülékenységvizsgálat végzésére és az incidenskezelés személyi feltételeire vonatkozó nemzetbiztonsági kritérium kikerült. Másik változás, hogy a bejelentést a sérülékenységvizsgálat megkezdése előtt 60 nappal kell megtenni a szervezet vezetőjének.

7) Hatósági együttműködés: A kritikus szervezetekről történő kijelölésről tájékoztatni kell a kiberbiztonsági hatóságot.

8) Adatkezelési és törlési szabályok: A hatósági nyilvántartásban szereplő adatok törlési határideje 5 év, az intézkedés megtörténtét követően. Közfeladatot ellátó szervek esetén a közérdekű adatigénylést 20 évig elutasítható, ha teljesítése kiberbiztonsági érdeket veszélyeztet.

Az auditok gyakorlati tapasztalatai egyre inkább körvonalazódni látszanak, melynek kapcsán iránymutatások, szakmai segédanyagok látnak napvilágot. Ezekben több témát érintően is az SZTFH által javasolt és elvárt tartalmak jelennek meg (pl: közreműködővel kötött szerződés tartalma, MI rendszerek besorolása az EIR struktúrába stb.) Magyar Kereskedelmi és Iparkamara az alábbiak szerint javasolja ezen iránymutatások figyelembevételét:

„A NIS2 által érintett vállalkozások számára ezért ezen iránymutatások a megfelelés gyakorlati zsinórmértékét jelentik. Betartásuk

a legbiztonságosabb út a hatósági elvárások teljesítéséhez, míg az azoktól való eltérés kockázatot jelent."

Ebből következik, hogy a fenti iránymutatások pusztán ajánlás jellegűek, mindig az adott szervezet – mérlegelést követően – dönt intézkedései és dokumentumai tartalma kérdésében.

Az NKI az aktuális trendek tekintetében aktívabb, rendszeres éves kiberbiztonsági jelentést ad ki a kiberfenyegetettségi helyzetről, a hatáskörökről és az irányadó joganyagról. Emellett folyamatosan frissítésre kerülnek a NIS2 megfeleléshez kapcsolódó űrlapok is

2.4. NIS 2-megfelelés értelmezése a Whitepaperben

A dokumentum értelmezése szempontjából kulcsfontosságú megérteni, hogy a szervezeteknek nem közvetlenül a NIS 2 irányelvnek kell megfelelniük, hanem annak a magyar jogrendbe átültetett szabályainak. A NIS 2 ugyanis egy európai uniós irányelv, amely minden tagállamot kötelez elveinek és követelményeinek nemzeti szabályozásba történő beépítésére. Magyarországon ez az előző fejezetben ismertetett jogszabályokon keresztül valósult meg, amelyek közül az érintett szervezetek megfelelése és a jelen Whitepaper szempontjából az alábbi négy bír kiemelt jelentőséggel:

- 2024. évi LXIX. törvény,
- 418/2024. (X. 30.) Korm. rendelet,
- 7/2024. (XI. 15.) MK rendelet,
- 1/2025. (I. 31.) SZTFH rendelet.

Azért szükséges mindezt külön kiemelni, mert a köznyelvben és a szakmai kommunikációban széles körben elterjedt a „NIS 2 audit", „NIS 2 megfelelés" vagy hasonló kifejezések használata, és emiatt jelen Whitepaper szerzői is gyakran így fogalmaznak. Valójában azonban ezek minden esetben a magyar törvényeknek és rendeleteknek való megfelelést jelentik. Ez alól kivételt jelent, ha a szövegkörnyezetből egyértelműen kiderül, hogy nemzetközi értelemben magára az irányelvre történik a hivatkozás, utalás.

Fontos kiemelni, hogy a gyakorlatban az uniós szintű elvárások önmagukban nem elegendőek: az audit során a magyar hatóság kizárólag a hazai törvények és rendeletek teljesülését vizsgálja. A félreértések elkerülése érdekében minden további hivatkozás ennek fényében értendő.

03

Érintett szervezetek azonosítása

Az érintett szervezetek pontos azonosítása a NIS 2-megfelelés egyik legkritikusabb első lépése, hiszen a jogszabály követelményei és kötelezettségei csak a hatálya alá tartozó szereplőkre vonatkoznak. A helyes besorolás nem mindig egyértelmű. Sok esetben szakértői segítségre van szükség a tevékenységi kör, a méretkategória vagy a szolgáltatásnyújtás földrajzi kiterjedése alapján történő meghatározáshoz. Külön kihívást jelenthet a kis- és középvállalkozások méret szerinti határértékeinek pontos értelmezése, a hazai és uniós tevékenységi körök közötti eltérések, illetve a nemzetközi szolgáltatásnyújtásból fakadó komplexitás. Ebben a fejezetben ezeknek a kérdéseknek a tisztázásához nyújtunk támpontokat, hogy a szervezetek megalapozott döntést hozhassanak saját besorolásukról.

3. Érintett szervezetek azonosítása

Írták: Biró Gabriella, Borbély Zsuzsa, Frey Krisztián, dr. Kálmán Kinga, Mészáros Etele, dr. Simon Ádám, dr. Szilágyi Emese

3.1. Önazonosítás

A NIS 2 érintettek körét a Kiberbiztonsági tv. szabályozza. Lényegében az határozza meg, hogy egy vállalkozás vagy szervezet NIS 2 érintett-e, hogy mi annak a tevékenysége, továbbá mekkora a mérete és mennyi a bevétele.

A szervezeteknek saját maguknak szükséges felismerniük érintettségüket, amelyet követően SZTFH rendeletben meghatározott adataikat – az SZTFH 420 számú nyomtatványt[18] használva – a cégkapun keresztül a Hatóság felé nyilvántartásba vételre meg kell küldeniük. Számos szervezetben merült és merül fel a kérdés, hogyan tudják az önazonosításukat elvégezni, hogyan bizonyosodhatnak meg érintettségükről.

Az önazonosítás nem minden esetben egyszerű, ettől függetlenül egy fontos feladat, ami elvégzése kapcsán általában a vezetőség is motivált. Tudni érdemes, hogy a határidők betartásáért, a nyilvántartásba vételi kérelem benyújtásáért az érintett vállalkozások első számú vezetői személy szerint felelősek, és ezt a felelősséget másra átruházni nem lehet!

Becslések szerint ma Magyarországon 3-4 ezer vállalat és szervezet lehet érintett a NIS 2 szabályozásban. a hatóság tájékoztatása alapján mostanáig, több mint 3700 regisztráció érkezett az SZTFH-hoz. Ez a szám a jövőben folyamatosan változni fog, mert egyes szervezet és vállalat idővel kikerülhet, újak pedig bekerülhetnek a NIS 2 hatálya alá.

A becslések statisztikák, nyilvántartások alapján történnek, leginkább a tevékenységi körök figyelembevételével. Emiatt fontos megemlíteni, hogy Magyarországon gyakori, hogy a vállalkozások olyan tevékenységeket is szerepeltetnek a nyilvántartásokban, melyet ténylegesen nem végeznek, azonban annak törléséről sem gondoskodnak.

Mérete és bevétel

A NIS 2 jelentősen bővíti az érintett szervezetek körét. a törvény hatálya alá alapértelmezetten a minimum középvállalati besorolást elérő szervezetek tartoznak. a vállalkozás méretét a magyar jogrendszer a Kkvtv.[19] alapján határozza meg, az uniós meghatározással[20] összhangban.

A középvállalkozásokra meghatározott küszöbértékeket (50 fő munkavállalói létszám vagy 10 millió EUR, azaz kb. 3,9 milliárd HUF éves árbevétel feletti) elérő vagy meghaladó szervezetek – ideértve azokat is, amelyek a kapcsolt vállalkozásokkal együtt számított foglalkoztatotti létszám vagy pénzügyi mutatók alapján középvállalkozásnak minősülnek – méret és bevétel szerint NIS 2 érintettek.

18 Érintett szervezet nyilvántartásba vételére irányuló kérelem

19 2004. évi XXXIV. törvény a kis- és középvállalkozásokról,

20 2003/361/EK bizottsági ajánlás a KKV-k meghatározásáról,

2. ábra (Forrás: SZTFH) Letöltve: 2025. 07. 02.

Például előfordulhat, hogy egy 35 főt foglalkoztató társaság önmagában kisvállalkozásnak minősülne, azonban egy nagyobb kapcsolt vállalkozással együtt számítva már középvállalkozásnak tekintendő, így a NIS 2 szabályozás hatálya alá kerül.

Fontos azonban, hogy ez önmagában nem elegendő az érintettség meghatározásához.

A NIS 2 hatálya elsősorban a középvállalkozásokat érinti, de kisvállalkozások is érintettek lehetnek, ha egyéb (például kritikus szolgáltatást nyújtanak) kockázati szempont alapján az irányelv hatálya alá kerülnek. Az irányelv 2. cikk (2) bekezdése[21] alapján a szabályozás nem alkalmazandó a kis- és mikrovállalkozásokra, kivéve, ha azok:

- a NIS 2-ben meghatározott kritikus ágazatokban működnek (pl.: energia, közlekedés, egészségügy, digitális infrastruktúra),
- és tevékenységük „jelentős közérdeket érint”.

Ezért nem elegendő kizárólag a méret alapján kizárni egy vállalkozást a NIS 2 hatálya alól, a tevékenységi kör és szolgáltatás jellege is döntő tényező.

3. ábra (Forrás: SZTFH) Letöltve: 2025. 07. 02.

21 (EU) 2022/2555 irányelv – a hálózat- és információbiztonság magas szintjének biztosításáról az Unióban (NIS 2),

Tevékenységi körök

Mind a NIS 2, mind a hazai törvény mellékletei[22] táblázatos formában tartalmazzák az érintett ágazatokat, alágazatokat és az adott alágazatban érintett szervezetek leírását. A méretkorláton túl-, illetve attól függetlenül a tevékenységi kör és szolgáltatás jellege alapján szükséges azt vizsgálni, hogy egy adott szervezet a NIS 2-szabályozás hatálya alá tartozik-e, továbbá mely hatóság látja el a felügyeletét.

Amennyiben egy szervezet a Kiberbiztonsági tv. 2. vagy 3. mellékletében felsorolt ágazatok valamelyikében végez tevékenységet, akkor potenciális NIS 2 érintett lehet, függetlenül attól, hogy hány alkalmazottal vagy mekkora üzletmenettel működik.

Az alábbi szolgáltatók, melyek azonosíthatók a nyilvántartásukat vezető hatóságok által, méretüktől függetlenül -azaz akár mikro- vagy kisvállalkozásként is- érintettek. (A magyar hatóságok megjelölését lásd zárójelben)

- elektronikus hírközlési szolgáltatók (Nemzeti Média- és Hírközlési Hatóság (NMHH) nyilvántartásában szereplők)
- bizalmi szolgáltató (NMHH által nyilvántartottak)
- DNS-szolgáltatást nyújtó szolgáltató
- legfelső szintű doménnév-nyilvántartó (Magyarországon az egyetlen szervezet: ISZT Nonprofit Kft.)
- doménnév-regisztrációt végző szolgáltató (az ISZT által üzemeltetett domain.hu oldalon elérhető regisztrátorok)

Fentiek közül alapvető szervezetnek minősülnek a minősített bizalmi szolgáltatók, DNS-szolgáltatást nyújtó szolgáltató, legfelső szintű doménnév-nyilvántartó.
A kiberbiztonsági hatóság illetékességét befolyásolja az a tény, hogy az adott szervezet közigazgatási ágazathoz tartozik-e, többségi állami befolyás alatt álló gazdálkodó szervezet-e, vagy honvédelmi kapcsolódású. Az NKI alábbi ábrája jól szemlélteti egyes szervezetek többes érintettségét.

Ha a méretkorlát teljesül, azaz közép- vagy nagyvállalkozásról van szó, vizsgálni kell az egyes mellékletekben felsorolt ágazatok szerinti tevékenységeket. Mivel a nyilvántartásba vételi űrlapon a tevékenységekről tételesen kell nyilatkozni a törvényi mellékletek alapján, mindenképp javasolt a tevékenységek mindegyikét megvizsgálni.

Bár a NIS 2 mellékletében kiemelten kockázatos kategóriában szerepelnek a banki szolgáltatások és pénzügyi piaci infrastruktúrák is, ezen ágazatokra a NIS 2 4. cikke szerint ágazatspecifikus szabály irányadó. Ekként a DORA rendelettel érintett szervezetek esetén a NIS 2 csak abban az esetben alkalmazandó, ha a DORA nem tartalmaz specifikusabb szabályozást.

A pénzügyi szervezetek kiberbiztonsági felügyeleti szerve az MNB.

Szintén a kiemelten kockázatos kategóriában szerepel a közigazgatás, a nemzeti joggal összhangban meghatározott, központi kormányzathoz tartozó, illetve regionális szintű közigazgatási szervek köre.

Az önazonosítás során vizsgálandó ágazat, illetve tevékenység feltétele az engedélyköteles tevékenységek esetén a társhatóságoknál vezetett nyilvántartások alapján, míg egyéb esetekben -jellemzően a gyártás ágazatban- a TEÁOR kód vagy egyéb szám alapján vizsgálható, melylyel kapcsolatban több kérdés is felmerülhet. A

22 2004. évi XXXIV. törvény a kis- és középvállalkozásokról,

besorolás értelmezése alágazatonként is gyakorlati problémákat vethet fel.

> Egy szoftverfejlesztő például önmagában a fejlesztési tevékenysége alapján nem sorolandó be, azonban vizsgálni kell, hogy kihelyezett szolgáltatónak minősül-e, mivel a gyakorlatban sokszor a fejlesztő cég a fejlesztéshez kapcsolódó egyéb szolgáltatásokat is nyújt, melyek miatt érintetté válhat.

Az azonosítást befolyásolhatják az egyes ágazathoz tartozás értelmezésében eltérően átvett tagállami szabályok.

A magyar gyakorlatban előfordul, hogy a vállalkozások olyan tevékenységeket is szerepeltetnek a nyilvántartásokban, melyet ténylegesen nem végeznek, azonban annak törléséről sem gondoskodtak. Kérdésként merülhet fel ezen tevékenységi besorolási rendszer alapján vajon hány olyan vállalkozás kerül amiatt a hatóság látószögébe, mert a nyilvántartások szerint vélelmezetten végez alapvető- vagy fontos ágazat szerinti tevékenységet. Bár a tevékenységi kör módosítása sok esetben egyszerű adminisztratív aktus, felmerülhetnek aggályok a tevékenység tényleges végzésének elbírálása és az önazonosítás emiatti elmaradásának szankcionálása esetén.

Egyéb esetekben a szabályozás többnyire szakhatósági engedélyt feltételez. Az egyes ágazatokhoz rendelhető magyar hatóságok:

- villamos energia, távfűtés, víziközmű, földgáz: Magyar Energetikai és Közmű- szabályozási Hivatal
- közlekedés: Építési és Közlekedési Minisztérium (közlekedési hatóság)
- élelmiszeripar: Nemzeti Élelmiszerlánc-biztonsági Hivatal
- gyógyszeripar, készletezés, egészségügyi szolgáltatók, vegyipar: Nemzeti Népegészségügyi és Gyógyszerészeti Központ
- elektronikus hírközlési, bizalmi és postai szolgáltatók: Nemzeti Média- és Hírközlési Hatóság
- hulladékgazdálkodás: környezetvédelmi hatóság.

> Példaként említhető az élelmiszeripar, ahol korábban az érintettek köre a magyar szabály szerint tágabb kört ölelt fel, mivel a Kibertantv-ben „az élelmiszerláncról és hatósági felügyeletéről szóló törvény szerint élelmiszer-vállalkozások” kerültek megjelölésre, míg a NIS 2 mellékletében „élelmiszer-vállalkozások, amelyek nagykereskedelemmel, ipari termeléssel és feldolgozással foglalkoznak” szerepel. A hatályos Kiberbiztonsági tv. már a NIS 2-vel összhangban szabályoz és az élelmiszerlánc-felügyeleti szervek adatszolgáltatására alapozza ezen ágazatban érintettek azonosítását.

A fentiek szerint annak megítélésében, hogy a NIS 2, illetve a nemzeti rendelkezések szerint egy vállalkozás érintettnek minősül-e, jogi, compliance, pénzügyi és informatikai területen működő szakemberek közösen segíthetik a vezetőséget a válaszadásban.

A Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezettel szemben kiszabható kiberbiztonsági bírság mértéke a nyilvántartásba vétel kapcsán a Kormányrendelet 3. melléklete alapján az alábbiak szerint alakulhat:

3.2. Segítő szereplők

Annak ellenére, hogy az azonosítás a szervezeteknek önmaguknak kell elvégezniük, vállalaton belül és azon kívül is vannak, akik ebben segíthetnek. Amennyiben segítségre van szükség, célszerű az alábbi szereplőkhöz fordulni tanácsért:

Jogászok, jogtanácsosok

Számos szereplőt jogilag határoz meg a Kiberbiztonsági tv., mely magyar jogszabályi hivatkozás esetén többnyire szakhatósági engedélyt feltételez. Az egyes ágazatokhoz rendelhető hatóságok:

- Magyar Energetikai és Közmű-szabályozási Hivatal: villamos energia, távfűtés, víziköz- mű, földgáz,
- Építési és Közlekedési Minisztérium (Közlekedési hatóság): közlekedés szektor,
- Nemzeti Élelmiszerlánc-biztonsági Hivatal: élelmiszeripar,
- Nemzeti Népegészségügyi és Gyógyszerészeti Központ: gyógyszeripar, készletezés, egészségügyi szolgáltatók, vegyipar,
- Nemzeti Média- és Hírközlési Hatóság: elektronikus hírközlési, bizalmi és postai szolgáltatók,
- Pest Vármegyei Kormányhivatal: hulladékgazdálkodás,
- Szabályozott Tevékenységek Felügyeleti Hatósága: kőolaj.
- Honvédelmi Minisztérium: honvédelmi ágazat
- Ha a vállalkozás rendelkezik valamely kijelölt hatóságtól engedéllyel, amennyiben van, a cég jogi területét vagy külsős jogászt érdemes felkeresni.

	A	B	C
1	A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
2	A Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő adatszolgáltatás nem teljesítése	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának 0,5%-a, de legalább 1 000 000 forint	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának legfeljebb 2%-a, de legfeljebb 150 000 000 forint
3	A Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő adatszolgáltatás határidőn túl történő teljesítése	50 000 forint	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának legfeljebb 0,1%-a, de legfeljebb 15 000 000 forint

Pénzügyi szakemberek

A Kiberbiztonsági tv. hatálya alá alapértelmezetten a minimum középvállalati besorolást elérő szervezetek tartoznak, tehát a Kkvtv. szerinti besorolást érdemes megvizsgálni.

A szervezetek pénzügyi területe (pénzügy-számvitel) a hatályos szabályokat általában ismeri, a cég besorolását – például pályázati lehetőségek miatt – naprakészen nyilvántartja.

Kiberbiztonsági és IT szakemberek

Az információbiztonsággal kapcsolatos meg felelősség terén leginkább az IT szakemberek, kiberbiztonsági szakértők a járatosak, illetve a minőségirányítás területén tevékenykedők személyek. Nagy valószínűséggel ezeken a területeken dolgozók segíteni tudnak abban, hogy pontosan megállapításra kerüljön, van-e a szervezetnek NIS 2 által érintett információs rendszere, szolgáltatása.

A nyilvántartásba vételhez szükséges nyomtatvány kitöltésben is fontos szerepük van a technológiát, információbiztonságot és megfelelősséget képviselő szakértőknek.

Tanácsadók, szakértők

A kiberbiztonság napjaink egyik legfontosabb kihívása, és a NIS 2 irányelv kulcsfontosságú lépés a digitális infrastruktúra védelmében, így nem meglepő, hogy számos tanácsadó cég foglalkozik a NIS 2-vel, végez tanácsadást, felkészítést a témában vagy nyújt egyéb NIS 2-höz köthető (pl.: IBF) szolgáltatást. Vannak tanácsadó cégek, akik különböző NIS 2-höz köthető kalkulátorokat hoztak létre, köztük olyat is, ami segít megállapítani egy szervezet érintettségét (pl.: RSM NIS 2 kalkulátor25, Datatronic NIS 2 érintettséget felmérő kérdőív26).

Számos kiberbiztonság terén tapasztalattal rendelkező szakembereket felvonultató, elismert tanácsadó vállalat van, akik a szervezet NIS 2 érintettségének megállapításában is segíteni tudnak, de érdemes nyitott szemmel járni, mert a nagy érdeklődés láttán megjelentek ezen a tanácsadói piacon olyan cégek is, amik mögött nincs tényleges tudás, tapasztalat.

Hatóságok

Az SZTFH és az NKI tájékoztató anyagokkal segíti az önazonosítást. Mindezek mellett a kettő szervezet számos egyéb módon végez tájékoztató tevékenységet a NIS 2 irányelvvel és annak hazai implementációjával kapcsolatban. Az SZTFH többállomásos országos rendezvénysorozatot indított, ezen felül számos konferencián adtak elő az NKI szakembereivel karöltve, mint vendégelőadók, továbbá a „Minden kiberül”27 nevezetű podcast-en keresztül is informálták az érdeklődőket.

Ha az önazonosítás során megakadt, senki nem tudott segíteni, kapcsolatba léphet a SZTFH-val, vagy benyújthatja a regisztráci- ós űrlapot, és a hatóság támogatást ad annak eldöntésében, hogy vállalata a NIS 2 irányelv hatálya alá tartozik-e vagy sem.

3.3 Nemzetközi szolgáltatásnyújtás kérdései

A NIS 2 Irányelv alapján főszabály szerint az érintett szervezetekre a letelepedésük szerinti tagállamnak van joghatósága. Tehát a leggyakoribb és legegyszerűbb esetben magyar cégek tevékenységét a magyar hatóságok felügyelik, még akkor is, ha határon átnyúló szolgáltatást nyújtanak (például, ha egy magyar székhelyű vegyipari cég vegyi anyagot árusít Ausztriában, ezzel a tevékenységével kapcsolatban a Kiberbiztonsági tv. Alkalmazandó elsőssorban).

Azonban a területi és személyi hatály kérdése nem ilyen egyszerű. Számos olyan eset elképzelhető, ahol a fenti példa nem érvényes. Ezek közül két olyan, az ületi életben jelentős gyakorlati eset szabályozását mutatjuk be ebben a fejezetben, amelyek eltérő helyzetet eredményeznek:

- Határon átnyúló Digitális Szolgáltatások nyújtása (például felhőszolgáltatás, kihelyezett (irányított) infokommunikációs szolgáltatás, kihelyezett (irányított) infokommunikációs biztonsági szolgáltatás) több tagállamban, vagy EU-n kívüli szervezetként az EU-ban,
- Elektronikus hírközlési szolgáltatások szabályozása.

A fenti esetekben a NIS 2 Irányelv 26. cikke alapelvi szinten rendezi azt, hogy az adott szervezet melyik tagállam joghatósága alá tartozik, tehát melyik tagállami implementáció hatálya fog nagy valószínűséggel kiterjedni a szervezetre. Figyelemmel azonban arra, hogy a NIS 2 Irányelv egy minimumharmonizációs jogszabály, amelytől a tagállamok viszonylag szélesebb körben eltérhetnek, minden esetben szükséges az adott tagállami jogszabályi környezetet is megvizsgálni a kiberbiztonsági megfelelés előkészítése körében határon átnyúló szolgáltatások esetén.

A következőkben általánosságban bemutatjuk a fenti két témában a NIS 2 Irányelv és a Kiberbiztonsági tv. releváns rendelkezéseit, majd kitérünk néhány olyan, jelenleg inkább bizonytalansággal övezett gyakorlati kérdésre, amelyekkel a nemzetközi szolgáltatást nyújtó szervezetek kiberbiztonsági megfelelése során, munkánk során találkozunk.

Mivel a nemzetközi szolgáltatásnyújtás alapvetően magánszektorban működő szervezetek esetében merül fel, a fejezet elsősorban ezen szervezetekre koncentrál. Ugyanakkor fontos hangsúlyozni, hogy a NIS 2 Irányelv (és ezzel összhangban a Kiberbiztonsági tv.) hatálya kiterjed az állami, közigazgatási szervekre is, ahol ugyanakkor ezek a joghatósági kérdések kisebb valószínűséggel merülnek fel. Ezen túl a tagállamok fenntarthatják a jogot, hogy az adott országban, egyes szektorokban működő kritikus, vagy az ország védelme szempontjából jelentős szervezeteket kijelölés útján saját joghatóságuk alá vonják. Ezen kérdések szintén fontos részét képezik a NIS 2 megfelelés témakörének, azonban részletesebb elemzésük szétfeszítené a fejezet, valamint a whitepaper kereteit.

Határon átnyúló digitális szolgáltatások

A jogalkotó a NIS 2 Irányelv megalkotásakor praktikus megoldást próbált kidolgozni arra, hogy a minden tagállamban egyszerre interneten elérhető és hasonló határon átnyúló digitális szolgáltatások üzemeltetőinek ne kelljen minden tagállamban a helyi NIS 2 implementációnak megfelelni és elkerülje az ezzel járó adminisztratív terheket.

A NIS 2 Irányelv a DNS-szolgáltatásokat, a legfelső szintű doménnév-nyilvántartó szolgáltatásokat, a domainnév-nyilvántartási szolgáltatásokat, a felhőszolgáltatásokat, az adatközpont-szolgáltatásokat, a tartalomszolgáltató hálózati szolgáltatásokat, az irányított szolgáltatásokat és az irányított biztonsági szolgáltatásokat, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platform szolgáltatásokat sorolta ebbe a kategóriába (együttesen: Digitális Szolgáltatások).

A Digitális Szolgáltatások határokon átnyúló jellegének figyelembevétele érdekében a NIS 2 Irányelv bevezet egy egyablakos megfelelési rendszert, az úgynevezett onestop-shop mechanizmust. Ennek értelmében a Digitális Szolgáltatások feletti joghatóságot az a tagállam gyakorolja, ahol az érintett szervezet EU-n belüli üzleti tevékenységének fő helye található, ezáltal más tagállam joghatósága nem terjedhetne ki a szolgáltatóra.

Az üzleti tevékenység fő helyének meghatározására a NIS 2 Irányelv egy három lépcsős tesztet dolgozott ki. Az üzleti tevékenység fő helyének azt kell tekinteni:

- ahol az EU-ban túlnyomórészt meghozzák a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket. E körben az elektronikus információs rendszerek jelenléte és használata önmagukban nem meghatározó kritériumok az üzleti tevékenység fő helyének meghatározásához, legtöbb esetben a központi ügyvezetés helyén történik a döntéshozatal;
- ha ilyen tagállam nem határozható meg, vagy az ilyen döntéseket nem az EU-ban hozzák meg, az üzleti tevékenység fő helye abban a tagállamban található, ahol a kiberbiztonsági műveleteket végzik, és
- amennyiben ilyen tagállam sem határozható meg, akkor abba a tagállamban lesz az üzleti tevékenység fő helye, ahol a szervezet a legtöbb munkavállalót foglalkoztatja.

Vállalatcsoportok esetén a NIS 2 Irányelv (114) preambulumbekezdése alapján az irányító vállalkozás üzleti tevékenységének fő helye lesz a meghatározó. Azonban felívjuk a figyelmet, hogy a NIS 2 Irányelv ebben a körben komoly ellentmondást tartalmaz és jelenleg nem állapítható meg egyértelműen, hogy az üzleti tevékenység fő helyét a vállalatcsoportban minden szervezetre külön-külön kell meghatározni, vagy egy teljes vállalatcsoport tekintetében lehetséges az üzleti tevékenység fő helyének meghatározása az EU-ban.

Jelentős probléma továbbá, hogy számos tagállam – a 2024. október 18. átültetési határidő ellenére – nem implementálta még a NIS 2 Irányelvet, ezért lehet, hogy az üzleti tevékenység fő helye egy olyan tagállamban található, ahol jelenleg nincs helyi hatályos jogszabály. Így praktikusan nincs is olyan közvetlenül alkalmazandó jogszabály, ami megállapítaná az adott tagállam joghatóságát a szervezet által nyújtott Digitális Szolgáltatások tekintetében, valamint a szervezet nem tudja milyen szabályoknak kéne megfelelni, így NIS 2 értelemben „hontalanná” válik a Digitális Szolgáltatásokat nyújtó szervezet.

Olyan esetekben, amikor az EU-ban nem letelepedett szervezet az EU-n belül kínál Digitális Szolgáltatásokat, ki kell jelölnie egy Unión belüli képviselőt. Nemzetközi szolgáltatásnyújtások körében tapasztalatunk alapján sokszor felmerül, hogy a multinacionális vállalatcsoport EU-n kívüli leányvállalata nyújt minden EU-ban letelepedett szervezet számára kihelyezett infokommunikációs és infokommunikációs biztonsági szolgáltatásokat, vagy felhőszolgáltatásokat. Ilyen esetben gyakori az EU-n belüli fő tevékenység helye szerinti leányvállalat képviselőként történő kijelölése.

Elektronikus hírközlési szolgáltatások

A NIS 2 Irányelv a főszabály alóli további kivételként kimondja, hogy a nyilvános elektronikus hírközlő hálózatok szolgáltatóit, vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókat azon tagállam joghatósága alá tartozónak kell tekinteni, ahol szolgáltatásaikat nyújtják. Ezáltal ezen szolgáltatókra külön és egyidejűleg mindazon tagállami implementáció hatálya kiterjed, ahol a szolgáltató elektronikus hírközlő hálózatot vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújt.

A Kiberbiztonsági tv. szabályozása

A magyar szabályozás a fenti keretekkel nagyrészt összhangban áll, ugyanakkor nem teljesen követi a NIS 2 Irányelv logikáját.

A Kiberbiztonsági tv. rendelkezéseit kell alkalmazni a Magyarország területén letelepedett vagy letelepedett képviselővel rendelkező szervezetekre, a Magyarország területén szolgáltatást nyújtó elektronikus hírközlési szolgáltatókra, és azokra a digitális szolgáltatókra, amelyek üzleti tevékenységének fő helye Magyarország területén található. Az üzleti tevékenység fő

helyének meghatározása is lényegében követi a NIS 2 Irányelv rendszerét.

Lényeges különbség azonban, hogy a Kiberbiztonsági tv. minden, nem Magyarországon bejegyzett szervezetet kötelez egy Magyarország területén működő képviselő kijelölésére, amennyiben a szervezet a Kiberbiztonsági tv. hatálya alá tartozó elektronikus információs rendszert működtet. Ez a rendelkezés jelentősen bővíti a NIS 2 Irányelv hatályát az EU-n kívül letelepedett digitális szolgáltatókon túl minden, a Kiberbiztonsági tv. hatálya alá eső külföldi szervezetre, ideért- ve a bármely Magyarországon kívüli EU tagállamban letelepedett szolgáltatókat is. A képviselő funkciója az értelmező rendelkezések alapján látszólag egy helyi kapcsolattartót feltételez, azonban a Kiberbiztonsági tv. Alapján a Magyarország területén működő képviselő a törvény végrehajtásáért a szervezet vezetőjére vonatkozó szabályok szerint felel. Ez az egytemleges felelősségi rezsim a szervezet vezetői és a képviselő között jelentős jogi kockázatot jelent a képviselők részére és megnehezít a gyakorlatban a magyar képviselők kinevezését.

Gyakorlati kérdések nemzetközi szolgáltatásnyújtás esetén

Ha magyar leányvállalat nyújt Digitális Szolgáltatást akár cégcsoporton belül, akár harmadik felek számára más tagállamban, a one stop shop mechanizmust figyelembe kell venni a joghatóság meghatározása során. E körben meg kell határozni az üzleti tevékenység fő helyét, amely a leányvállalat magyar székhelye ellenére nem teljesen egyértelmű, hogy Magyarország lesz. Ilyen eset előfordulhat például, ha a szervezet kiberbiztonsággal foglalkozó belső szervezeti egysége nem Magyarországon működik. Tovább bonyolíthatja a helyzetet, ha a belső kiberbiztonsági szervezeti egység részterületei különböző, akár EU-n kívüli országban találhatók. A vállalati struktúrától függ, hogy ezt a vizsgálatot a szervezet, vagy a vállalatcsoport szintjén szükséges elvégezni.

Amennyiben vállalatcsoport esetén a külföldi anyavállalat nyújt magyarországi leányvállalata számára Digitális Szolgáltatást, a one stop shop mechnanizmus alapján főszabály szerint a Digitális Szolgáltatás nem fog a Kiberbiztonsági tv hatálya alá tartozni. EU-n kívüli anyavállalat esetén a one stop shop meghatározásán túl EU-n belüli képviselőt is szükséges lehet az anyavállalat képviseletére kijelölni.

Nem Digitális Szolgáltatások esetében főszabály szerint a Kiberbiztonsági tv. hatálya alá tartozik a Magyarországon letelepedett szervezet által nyújtott szolgáltatás, így nagy valószínűséggel nem lesz alkalmazandó más tagállam NIS 2 Irányelv implementációja. Multinacionális vállalatok esetében azonban – különös tekintettel, ha a termelés és for- galmazás több országon és entitáson keresztül zajlik – érdemes helyi jogásszal konzultálni minden érintett országban, mert tapasztalataink alapján lehetnek eltérések a joghatóság értelmezésében.

A magyar kiberbiztonsági jogszabályi és gyakorlati környezet alapján főbb intézmények értelmezése vagy kötelezettségek teljesítése számos gyakorlati kérdést vet fel abban az esetben is, ha az érintett szervezet nem Magyarországon letelepedett, ideértve a magyar kiberbiztonsági audit és kiberbiztonsági képzési elvárásokat külföldi menedzsment ta- gok és EIRBF-ek tekintetében, valamint a re- gisztrációval kapcsolatos lokális elvárások teljesítését. Kiemeljük, hogy külföldi szervezetnek regisztrálni az SZTFH 420 nyomtatványon 2025. februárig nem volt lehetősége. Emellett a külföldi szolgáltatók magyar szolgáltatásaival kapcsolatos elektronikus információs rendszerek kiberbiztonsági auditja számos kérdést felvet, amelyekre a gyakorlatnak kell majd választ adnia.

04

Szerepkörök és felelősségek

A NIS 2 irányelv és a kapcsolódó hazai szabályozás egyik alapvető pillére a kiberbiztonsági szerepkörök és felelősségi körök egyértelmű kijelölése. a kiberbiztonsági feladatok szétosztása és dokumentálása elengedhetetlen a szervezet működésének átláthatósága, a gyors reagálás és az elszámoltathatóság biztosítása érdekében. a szabályozás megköveteli, hogy minden érintett szervezet egyértelműen meghatározza az információbiztonsági irányításban, az incidenskezelésben, a megfelelőség nyomon követésében és a beszállítói kapcsolatok felügyeletében érintett felelősöket, valamint rögzítse ezek feladat- és hatáskörét. a világos felelősségi rendszer nemcsak a jogszabályi megfelelést segíti, hanem a szervezet kiber-ellenállóképességét is növeli, hiszen csökkenti a felelőtlenségből vagy félreértésekből eredő biztonsági kockázatokat.

4.Szerepkörök és felelősségek

Írták: Biró Gabriella, dr. Jeney Andrea, Nagy Imre, dr. Novák Anett

4.1 Információbiztonsági szerepkörök

Az információbiztonsági feladatok ellátása összetett és szerteágazó tevékenység, amely különböző szerepkörök szoros együttműködésére épül. A megfelelő feladatmegosztás és felelősségi körök tisztázása érdekében célszerű először az egyes szereplőket áttekinteni, hogy a szerepkörök gyakorlásának, kialakításának és dokumentálásának módja világossá váljon.

> Egy szoftverfejlesztő például önmagában a fejlesztési tevékenysége alapján nem sorolandó be, azonban vizsgálni kell, hogy kihelyezett szolgáltatónak minősül-e, mivel a gyakorlatban sokszor a fejlesztő cég a fejlesztéshez kapcsolódó egyéb szolgáltatásokat is nyújt, melyek miatt érintetté válhat.

A NIS 2 irányelv új alapokra helyezi és szigorítja a vezetői felelősség intézményét. Kiemeli, hogy a szervezet felső vezetése – a hierarchia legmagasabb szintjén – viseli a felelősséget az információbiztonsággal kapcsolatos stratégiai döntések meghozataláért. A vezető jóváhagyja a kockázatértékeléseket, dönt a védelmi intézkedésekről, valamint kijelöli az információbiztonságért felelős személyt, akivel folyamatos, napi szintű együttműködést folytat. A szakmai szempontok mérlegelése szintén az ő felelősségi körébe tartozik.

A szakmai irányítást az információbiztonsági vezető látja el, akit a szervezet vezetője nevez ki. Feladata az összes, információbiztonságot érintő szakmai kérdés koordinálása – ideértve a szabályozás kialakítását, az incidenskezelé- si eljárások meghatározását, a belső és külső kapcsolattartást, valamint a tudatosságnövelő képzések megszervezését. Az információbiztonsági vezető szoros együttműködésben dolgozik az IT vezetővel és az informatikai csapattal, akik a technikai infrastruktúra működtetéséért és a napi IT üzemeltetésért felelősek. Fontos hangsúlyozni, hogy az információbiztonsági vezető nem alárendeltje az IT vezetőnek, hanem önálló szakmai hatáskörrel rendelkezik.

A szervezet további fontos szereplői közé tartoznak az alkalmazásfejlesztők, akik az üzleti igényekhez illeszkedő szoftveres megoldások fejlesztéséért, testreszabásáért felelnek, valamint a beszerzési felelősök, akik a dobozos szoftverek és egyéb IT eszközök beszerzésének folyamatát irányítják. Emellett belső auditorok is működhetnek a szervezetben, akik az információbiztonsági rendszerek és eljárások belső ellenőrzését végzik a szervezet érdekeit szem előtt tartva.

Az, hogy a fenti szerepkörök ellátására a szervezet belső munkavállalókat jelöl ki, avagy egyes feladatokat kiszervez, minden esetben üzleti döntés kérdése, ezt a szervezet vezetése, valamint belső eljárásrendek határozzák meg. Ilyen döntés során nemcsak jogi, hanem átláthatósági és szervezeti transzparenciára vonatkozó szempontokat is figyelembe kell venni. A megfelelő dokumentáltság ugyanis nem csupán megfelelőségi követelmény, hanem a hatékony működés és az elszámoltathatóság alapfeltétele is.

Amennyiben a szervezet a belső megoldás mellett dönt, ez esetben az információbiztonsági feladatokat saját munkavállalóival látja el. E munkatársak munkaköri leírása pontosan meghatározza a tevékenységi köröket, a szervezeti struktúrában való elhelyezkedést, valamint a felelősségi viszonyokat.

A döntés hátterében több tényező állhat: pénzügyi szempontok, a meglévő szakértelem szintje, a szervezeti hierarchia, valamint

vezetői érdekek. A belső megoldás választása számos előnyt kínál, ugyanakkor kihívásokkal is járhat – ezek mérlegelése elengedhetetlen a megalapozott döntéshozatalhoz.

Előnyök

A belső megoldások egyik legfőbb előnye, hogy nagyobb kontrollt és átláthatóságot biztosítanak: a szervezet ugyanis ily módon közvetlenül irányítja az információbiztonsági tevékenységeket, külső közvetítő nélkül. Ez különösen incidenshelyzetekben előnyös, amikor a gyors és közvetlen reakció kulcsfontosságú. A dokumentumokhoz (pl.: logfájlok, rendszer-naplók) való közvetlen hozzáférés egyúttal az auditálhatóságot is javítja, mivel azok könnyebben ellenőrizhetők és naprakészen karbantarthatók.

További előnyt jelent, hogy a belső munkatársak mélyrehatóan ismerik a szervezet működését és folyamatait, ami lehetővé teszi az üzleti célokkal összhangban álló, testreszabott védelmi stratégiák kialakítását. Ez a belső tudás komoly értéket képvisel, különösen a szervezet információbiztonsági érettségének fejlesztése során.

A szervezeten belüli kommunikáció egyszerűbb és közvetlenebb, így az információbiz- tonsági kérdések az IT, jogi vagy üzleti megbeszélések szerves részévé válhatnak. A közös szervezeti nyelv, a belső munkatársak jobb együttműködési hajlandósága és a közös értékrend révén a problémák és igények gyorsabban feltérképezhetők és hatékonyabban kezelhetők, mint egy külsős szolgáltató bevonása esetén.

Továbbá a szervezeti kultúra és az elköteleződés is erősebb lehet belső megoldás esetén. A munkavállalók saját céljuknak érzik a szervezet biztonságát, így szabálykövetési hajlandóságuk és incidenskezelési együttműködésük is magasabb. Ez ellentétben állhat a külső szakértők szempontjaival, akik gyakran projektalapon dolgoznak, és nem kötődnek szorosan a szervezet hosszú távú érdekeihez.

Végül meg kell jegyezni, hogy a szervezeti döntés hátterében mindig a költségvetés is meghatározó tényező. A belső megoldás – bár kezdetben erőforrásigényesebb lehet – hosszú távon költséghatékonyabbá válhat, különösen, ha az információbiztonsági ismeretek házon belül fokozatosan kiépülnek és fenntarthatók.

Hátrányok

Az információbiztonsági feladatok belső megoldása számos előnnyel jár, ugyanakkor jelentős kihívásokat és potenciális kockázatokat is rejt magában. Ezek figyelembevétele elengedhetetlen a szervezet hosszú távú, fenntartható és hatékony működése érdekében.

Az információbiztonsági szakemberek toborzása, megtartása és folyamatos képzése komoly anyagi ráfordítást jelent. Mivel ez a szakterület dinamikusan fejlődik, ezért az alkalmazottaknak rendszeresen frissíteniük kell tudásukat, részt kell venniük tanfolyamokon, konferenciákon, illetve szakmai minősítéseket kell szerezniük. Ez önmagában is nagy költség, ráadásul egy komplex információbiztonsági rendszer kiépítése, a megfelelő technológiák beszerzése és karbantartása további pénzügyi terhekkel jár. Ezeket a kiadásokat a szervezeti költségvetésbe tudatosan be kell építeni.

További probléma az információbiztonsági szakterületeken szükséges specifikus tudás, vagy szakértelmi rétegzettség kérdése. A kibertámadások egyre kifinomulttá válásával a szakmai részkompetenciák folyamatos fejlesztése indokolt a sikeres szervezeti működés érdekében.

A folytonos védelem érdekében az információbiztonságnak folyamatos, éjjel-nappali megfigyelést és gyors reagálást kell biztosítania. Egy belső csapatnál, különösen ha az erőforrások szűkösek, nehéz fenntartani a 24/7- es készenlétet. Ez azt eredményezheti, hogy támadás vagy incidens esetén a válaszreakció késedelmes, ami súlyosbítja a károkat. Az ügyeleti rendszerek

és gyors beavatkozási protokollok kiépítése plusz szervezési és anyagi terhet jelent.

Ha az információbiztonsági vezető alárendelve van az IT vezetőnek vagy erős operatív szerepet tölt be, fennáll a veszélye, hogy a biztonsági kockázatok alulértékelődnek a gyors üzleti folyamatok érdekében. A belső szereplők érdek- és hatalmi viszonyai tehát befolyásolhatják a szakmai döntések objektivitását, illetve a kockázatok megfelelő kezelését.

Szintén akadály, ha a kritikus információbiztonsági feladatok egy-két kulcsszemélyhez kötődnek, akkor egy váratlan távozás vagy hosszabb távú távollét komoly problémát okozhat. Tudás, kapcsolatok, folyamatok, dokumentációk hiányos átadása esetén a működés megbénulhat, vagy hibás döntések születhetnek. A tudásmegosztás, helyettesítési rend kialakítása és a folyamatos dokumentálás elhanyagolása növeli a szervezet sérülékenységét.

A szervezet növekedése, új szabályozások bevezetése vagy technológiai fejlesztések igénye gyors kapacitásnövelést követelhet meg. Egy belső csapat létszámának és kompetenciájának gyors bővítése azonban nehéz és időigényes.

Ezzel szemben a külső szolgáltatók általában rugalmasabbak, képesek az igényekhez igazítani szolgáltatásaikat, például SOC (Security Operation Center) szolgáltatás, behatolástesztelés vagy speciális tanácsadás formájában.

Ezen túlmenően az információbiztonsági eszközök (pl.: SIEM, IDS/IPS, jogosultságkezelő rendszerek) beszerzése, üzemeltetése, licencdíjai, frissítései jelentős költséget jelentenek, amelyet a belső megoldások esetén a szervezetnek kell viselnie. Ezek a költségek gyakran alulbecsültek, és nem csak az elsődleges beszerzést, hanem a folyamatos karbantartást, szakértői támogatást, integrációt, tréninget is magukban foglalják.

Ahogy az korábban említésre került, a belső információbiztonsági feladatok átláthatóságának megőrzése érdekében folyamatos, precíz dokumentáció szükséges: munkaköri leírások, szabályzatok, incidensnaplók, rendszeres jelentések, nyomon követhető kockázatelemzések stb. Ezek elkészítése, karbantartása és rendszeres frissítése idő- és munkaigényes, amely terhet ró a szervezetre, és elvonhatja a fókuszt a napi operatív védekezéstől.

Ezzel szemben a külső szolgáltatók, tanácsadók széles körű tapasztalatukkal és több szervezetnél szerzett tudásukkal naprakész piaci és technológiai információkat hoznak be a szervezetbe. Egy kizárólag belső megoldás esetén a szervezet könnyen „beszűkülhet”, és nem biztos, hogy reálisan látja saját információbiztonsági érettségét, vagy észreveszi a piac új kihívásait, trendjeit.

Az, hogy ténylegesen melyik megoldás érvényesül, mindig szervezetspecifikusan, a fenti körülmények együttes mérlegelésével, a szervezeti igények alapján a szervezeti vezető dönti el. A belső modell sikeres működéséhez elengedhetetlen vezetői elköteleződés és megfelelő költségvetési keret biztosítása.

Szerepkörök alapján akár a következőket lehet figyelembe venni (példa)

Szerepkör	Felelősség / Feladatkör
Vezető tisztségviselő / felsővezetés	- a szervezet kiberbiztonságának általános irányítása – Megfelelés biztosítása a NIS 2 és Kbtv. követelményeinek – Kockázati szint elfogadása, erőforrások jóváhagyása
Kibervédelmi felelős (pl.: CISO)	- Információbiztonsági irányítás kialakítása - Kockázatkezelés, szabályzatalkotás, tudatosság növelése - Auditok, jelentések, eseménykezelés koordinálása
IT vezető / rendszergazda	- Technikai védelem működtetése - Frissítések, naplózás, jogosultságkezelés - Események technikai elemzése és reakció
Kockázatkezelési felelős	- Éves kockázatértékelés koordinálása - Kockázatcsökkentési intézkedések nyomon követése
Incidenskezelési felelős / CSIRT kapcsolat	- Kiberbiztonsági események fogadása, elemzése, jelentése – Kapcsolattartás az NBSZ NKI-vel (Nemzeti Kiberbiztonsági Intézet) – Határidős bejelentés biztosítása (24-72 óra)
HR és oktatási felelős	- Kiberbiztonsági tudatosság- és képzésmenedzsment – Beléptetéshez kapcsolódó biztonsági oktatás – Szabályzatok megismertetése
Adatvédelmi tisztviselő (DPO) (ha van)	- a személyes adatok védelmének biztosítása - Koordináció a GDPR és NIS 2 elvárások között
Üzletfolytonossági felelős	- Üzletmenet-folytonossági tervek (BCP) és vész-helyzeti eljárások összehangolása – Kiberbiztonsági kockázatok integrálása az üzleti szcenáriókba

Szerep- és felelősségi mátrix (rövid minta)

Tevékenység	Vezetőség	CISO	IT	HR	DPO	CSIRT
Kockázatelemzés jóváhagyása	R	A	C	C	I	I
Szabályzat frissítése	A	R	C	C	C	I
Képzés indítása	C	C	I	R	I	-
Incidensbejelentés NKI-nek	I	C	C	-	-	R
Backup és hozzáféréskezelés	-	C	R	-	-	I

R – Felelős (Responsible),
A – Jóváhagyó (Accountable),
C – Konzultált (Consulted),
I – Tájékoztatott (Informed)

4.2. Szükséges IBF készségek és tanúsítványok

Kinek és miért is van szükség IBF-re?

Egy ideális világban minden szervezetnek szüksége lenne Információ Biztonsági Felelősre (IBF). Az IBF feladatköre az IT alapvető fontosságúvá válásával lett nélkülözhetetlen. Egy jó IBF alapvetően csapatjátékos. Egy olyan projektvezető, aki egyensúlyba tudja hozni az üzleti célokat az IT lehetőségeivel úgy, hogy kiberbiztonság szempontjai is megvalósulnak az elvárható szinten.

Elvárható készségek, közkeletű tévhitek

Nagyon sok vezető azt hiszi, hogy mivel az IBF elnevezésében ott a felelős, akkor ezt a pozíciót egy jelenleg is a szervezetben vezető pozíciót betöltő embernek kell betöltenie. a másik véglet, hogy a rendszergazda, vagy IT-ért felelős személynek kell ezt a pozíciót betöltenie. Biztos van ilyen, de alapvetően ez rossz a kiindulási pont, mert az IT és az információbiztonság között érdekellentét is lehet. Az egyik azt szeretné, hogy működjön, a másik pedig azt, hogy biztonságos legyen – ez nem mindig sikerül egyszerre.

Az IBF-nek az információbiztonsági tudás mellett erős interperszonális készségekkel kell rendelkeznie – vagy ahogy manapság hivatkoznak rá, soft skillekkel:

- csapatorientált és csapatjátékos,
- jó kommunikációs készséggel rendelkezik,
- kezeli a konfliktusokat,
- jól közvetít,
- tudja kezelni a stresszt,
- és gyorsan tud reagálni az új helyzetekre.

Az IBF elvárt képességeivel kapcsolatban támpontot nyújthat az ENISA European Cybersecurity Skills Framework (ECSF) szerepkör leírásai és az ECSF leképezése a NIS 2-höz kapcsolódó feladatokra.

Kinek kötelező, jogszabályi háttér

Vannak szervezetek, ahol az IBF kinevezése nem döntés kérdése, hanem törvényi előírás. Kiberbiztonsági tv. hatálya tartozó szervezeteknek kötelező IBF-et kijelölni. Hogy ki lehet alkalmas, abban a Kormányrendelet és a 17/2025-ös EM rendelet ad iránymutatás, a mindenkori elfogadható képzettségek listáját pedig az NKI berkein belül működő Nemzeti Koordinációs Központ (NCC-HU) teszi közzé weboldalán (https://ncc.gov.hu/ibf-kepzesek-listaja/).

Akinek kötelező – állami szféra

A Kiberbiztonsági tv. azonban különbséget tesz a kötelezettek közt. a kijelölt közigazgatási és állami szerveknek kötelezően elő van írva, hogy minek kell megfelelnie egy IBF-nek, akit le is kell jelentenie az NKI-nak. Aki ezt a feladatot el akarja látni, szerepelnie kell az NKI IBF nyilvántartás oldalán. a nyilvántartásba vételhez jelenleg a következő elvárásokat támasztják:

- Rendelkezzen felsőfokú végzettséggel. Ez diplomát jelent. MKKR szerinti minimum 6-os szintet érje el a megszerzett oklevél. De nem kell szakirányúnak lennie!
- Szakmai képzettség
    - Jelenleg az alábbi szakképzettséget fogadják el:
    - Elektronikus információbiztonsági vezető,
    - Certified Information Systems Auditor,
    - Certified Information Systems Manager,

    - Certified Information Systems Security
    - Professional,Certified in Risk and Information
    - Systems Control.
- Vagy igazolt legalább 5 éves szakmai tapasztalat az alábbi területeken
    - Információbiztonsági irányítási rendszer tervezése, kialakítása vagyműködtetése,
    - Információbiztonsági ellenőrzés vagy felügyelet,
    - Információ-biztonsági kockázatelemzés,
    - Információbiztonsági tanúsítás
    - Információbiztonsági tesztelés
    - (etikus hacker tevékenység).

Akinek kötelező – gazdasági szféra

Az állami szférával ellentétben – bár a Kiberbiztonsági tv. hatálya alá tartozóknak kötelező ugyanúgy bejelentenie IBF-et az NKI-nak vagy az SZTFH-nak (attól függően, hogy keletkezett a kötelezettség) – a gazdasági szervezet szabad kezet kap, hogy kit jelöl a pozícióba. a fentiek jó kiindulási alapot jelentenek, de érdemes végiggondolni hogy kire és mire van szüksége az adott szervezetnek. Általában 3 irányból szoktak érkezni az IBF-ek:

- műszaki, főleg IT végzettséggel rendelkező személy, aki erős IT szakmai háttérből indulva, de ismerve egy gazdasági szervezet folyamatait látja el a feladatot, de a jogi témák se állnak tőle távol;
- gazdasági végzettséggel, mert a folyamatokat jól ismeri egy cégnél, de emellett rendelkezik egy erős IT tudással, így szót tud érteni az IT-s kollégákkal, illetve a jogi témákat is jól kezeli;
- jogi oldalról, így a jogi szabályozásokkal tisztában van, de ismeri a folyamatokat és szintén van egy erős IT tudása, hogy mindenkivel szót tudjon érteni.

A fentiekből is látszik, hogy az IBF olyan ember, aki sok területtel van kapcsolatban, tudása sok mindenre kiterjed, de nem rendelkezik, – mert nem szükséges – mély szakmai ismerettel mindegyik területen.

Kiberbiztonsági képzések

Jelenleg már itthon is elérhetőek képzések kiberbiztonsági/adatvédelmi területen. Ezek a képzések szintén jó kiindulási alapot jelentenek egy IBF-nek, de ezeken belül is megfigyelhetőek a fenti hangsúlyok, specializációk. Ha a szervezet saját kollégát akar kijelölni erre a feladatra, akkor az alábbi képzések jó kiindulópontot jelentenek a szükséges tudás elsajátításához. Ezek a képzések jelenleg:

Alapképzésen

- Óbudai Egyetem – Kiberbiztonsági mérnöki,
- Mesterképzésen
- Óbudai Egyetem – Kiberbiztonsági mérnöki,
- Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterszak,
- Széchenyi István Egyetem – Modern technológiák és kiberbiztonság joga,

Szakirányú továbbképzésen

- Nemzeti Közszolgálati Egyetem – Elektronikus Információbiztonsági Vezető,
- Óbudai Egyetem – Információbiztonsági szakmérnök/szakember,
- Széchenyi István Egyetem – Jogi szakokleveles kiberbiztonsági szaktanácsadó,
- Gábor Dénes Egyetem – Adatvédelmi és információbiztonsági menedzser.

05

Kockázat-kezelési keretrenszer kialakítása

A kockázatkezelési keretrendszer kialakítása a NIS 2 irányelvnek való megfelelés egyik alapkövetelménye, amely biztosítja a szervezet működésének és szolgáltatásainak folyamatos védelmét. a cél egy olyan átfogó rendszer létrehozása, amely segít azonosítani és értékelni a kiberbiztonsági kockázatokat, majd megfelelő intézkedésekkel csökkenteni azok hatását. a kockázatkezelés nem egyszeri feladat, hanem folyamatos, ismétlődő folyamat, amely reagál a változó technológiai és fenyegetési környezetre. a jól kialakított keretrendszer támogatja a tudatos döntéshozatalt, növeli a szervezet ellenálló képességét, és megalapozza a hosszú távú információbiztonsági érettséget. a fejezet célja tehát annak bemutatása, hogy a kockázatértékelési keretrendszer nem csupán megfelelési eszköz, hanem a szervezet hosszú távú, hatékony kibervédelmének és ellenálló-képességének alapkövetelménye is.

5. Kockázatkezelési keretrendszer kialakítása

Írták: Arató György, Ács Bálint, Bódis Péter, Gedra János, dr. Jeney Andrea, dr. Lendák Imre, Maczkó Péter, Major Róbert, Mészáros Csaba, Molnár Ferenc, Nagy Ágnes Beáta, Szűcs Krisztina

5.1. A kockázatkezelési keretrendszer

A NIS 2 irányelv alapjaiban formálta át a kockázatkezeléssel szemben támasztott követelményrendszert. a kockázatértékelés innentől kezdve nem pusztán adminisztratív kötelezettség, hanem a szervezeti ellenálló képesség egyik kulcseleme. a kockázatalapú megközelítés nemcsak az informatikai rendszerekre, hanem a teljes informatikai ökoszisztémára – technológiákra, folyamatokra és emberi tényezőkre – kiterjed, és a szervezet irányítási rendszereinek szerves részévé válik. Egyúttal a biztonsági érettség alapját képezi, és meghatározó szerepet játszik a jogszabályi megfelelés elérésében is.

A kockázatértékelési keretrendszer célja, hogy strukturált módon azonosítsa, értékelje és kezelje azokat az információ- és kiberbiztonsági kockázatokat, amelyek veszélyeztethetik a szervezet működésének folytonosságát, illetve szolgáltatásainak megbízhatóságát. Ehhez elengedhetetlen a komplex szemlélet, vagyis a kockázatértékelés összehangolása a szervezet egyéb kontrollfolyamataival és irányítási rendszereivel. Csak így biztosítható, hogy a biztonságkezelés ne különálló tevékenységként, hanem a szervezeti működés integrált elemeként valósuljon meg.

Fontos hangsúlyozni, hogy a kockázatértékelés nem egyszeri feladat, hanem iteratív, ciklikusan ismétlődő folyamat, amely rendszeres felülvizsgálatot és folyamatos felügyeletet igényel. a szervezet csak ilyen módon képes hatékonyan reagálni a technológiai fejlődésre, az újonnan megjelenő fenyegetésekre, valamint a változó szabályozói környezetre.

Az MK rendelet külön fejezetben részletezi a kockázatkezeléssel kapcsolatos elvárásokat. Különös hangsúlyt fektet a kockázatkezelési folyamat meglétére, illetve az azonosított kockázatra adott válaszok meglétére, ami alatt elsősorban az értékelések, ellenőrzések és vizsgálatok megállapításaira köteles megfelelő választ adni. A válaszokat kockázat vezérelt módon szükséges megválasztani, így azok lehetnek egy adott biztonsági intézkedés azonnali bevezetése vagy több intézkedés felvétele az intézkedési tervbe különböző határidőkkel és felelős személyekkel.

5.2. Mit kell tartalmaznia a kockázatkezelési keretrendszernek?

A kockázatkezelési keretrendszer célja, hogy segítse a szervezetet abban, hogy az informatikai és üzleti kockázatokat azonosítsa, értékelje, és megfelelő intézkedésekkel kezelje – még mielőtt azok valós problémává válnának. Nem elég általános irányelveket megfogalmazni, hanem olyan keretrendszert kell kialakítani, amely a mindennapi működésbe illeszkedik, és valódi védelmet nyújt a fenyegetésekkel szemben. Ehhez azonban világosan kell látni, mit is jelent maga a rendszer, és milyen elemekből áll össze.

A keretrendszer szívét egy átfogó, strukturált és naprakészen tartott kockázatkezelési folyamat jelenti. Ez egy olyan logikusan felépített munkamenet, amely lépésről lépésre vezeti végig a szervezetet a veszélyek felismerésétől a konkrét védelmi intézkedések bevezetéséig. Ahhoz, hogy ez jól működjön, a keretrendszernek az alábbi fő elemeket szükséges tartalmaznia:

1. Szervezeti szintű szabályozás: világosan meghatározott felelősségi körök, hatáskörök, eljárások és döntési mechanizmusok, amelyek rögzítik, hogy a kockázatkezelés során ki mit tehet, és milyen esetekben.
2. Kockázatértékelési módszertan: egyértelmű, dokumentált eljárás annak meghatározására, hogyan azonosítjuk a fenyegetéseket, hogyan mérjük fel azok valószínűségét, hatását és hogyan soroljuk be a kockázatokat azok súlyossága szerint. Ezen módszertannak tükröznie kell a szervezet saját működési környezetét és szabályozási kötelezettségeit is (pl.: Kiberbiztonsági tv., MK rendelet, GDPR).
3. Fenyegetés- és sérülékenységkatalógus: egy testreszabott lista a leggyakoribb kockázatokról, amelyek a szervezet EIR-jeit, adatvagyonát, munkafolyamatait veszélyeztethetik[23]. Ez nem elméleti gyűjtemény, hanem a konkrét technológiai, fizikai és emberi tényezőkre szabott, általában ágazat-specifikus térkép.
4. Értékelési és döntési sablonok: egyszerűen használható táblázatok, űrlapok, amelyek segítik a kockázatok egységes dokumentálását, osztályozását és nyomon követését.
5. Intézkedési terv: az azonnali és hosszú távú védelmi intézkedések, ellenőrzési pontok és felelősök listája. a kockázatokat csak akkor tekinthetjük kezeltnek, ha az ellenintézkedések pontosan meghatározottak, felelőshöz rendeltek és határidejük van.
6. Felülvizsgálati és frissítési folyamat: az információbiztonsági környezet nem statikus. Ezért a keretrendszernek tartalmaznia kell az éves felülvizsgálat, az auditálás és a rendkívüli módosítás lehetőségét is. Egy elavult kockázatelemzés többet árt, mint használ.
7. Kapcsolódás más kontrollrendszerekhez: a kockázatkezelési keretrendszer akkor lesz igazán hatékony, ha nem önállóan, hanem szoros kapcsolatban működik más szabályozási területekkel is: például adatvédelem (DPIA), üzletmenet-folytonosság, incidenskezelés, változáskezelés vagy IT-üzemeltetés.

A kockázatkezelési keretrendszer nem csupán egy dokumentumcsomag. Akkor működik jól, ha valós döntéstámogató eszközzé válik a vezetés, az informatikusok és az üzleti területek számára is. Egy jól kidolgozott keretrendszer képes előre jelezni, ha egy EIR túl sebezhető, vagy ha egy üzleti folyamat olyan adatokat érint, amelyeket jobban kell védeni. Ezzel nemcsak a jogszabályi megfelelés biztosítható, hanem elkerülhetők a pénzügyi, hírnévbeli vagy működési károk is.

A gyakorlatban a legfontosabb kérdés így hangzik: „Mit veszítünk, ha ez a rendszer sérül, leáll, vagy adatvesztés történik?” Ha erre őszintén és rendszerszinten tudunk válaszolni, az annak a jele, hogy valóban működő kockázatkezelési keretrendszerrel rendelkezünk.

5.3. Kockázatkezelés: a meglévő keretrendszer része legyen, vagy különálló rendszerként működjön?

A szervezeti szintű kockázatkezelési folyamat bevezetésekor szükséges eldönteni, hogy az információbiztonsági kockázatkezelés a meglévő, egységes keretrendszer része legyen, vagy különálló rendszerként működjön. Ezt a döntést elsősorban olyan nagyobb szervezetekben szükséges meghozni, ahol már létezik egy egységes, szervezeti szintű általános kockázatkezelési folyamat, amely azonban nem tér ki a kiberbiztonsági kockázatokra is.

A NIS 2 irányelv célja, hogy az EU-ban egységesen magas szintű kiberbiztonságot teremtsen. a Kiberbiztonsági tv. alapján az érintett szervezeteknek kockázatalapú információbiztonsági irányítást kell alkalmazniuk. Ennek kulcseleme

23 3. melléklet az MK rendelethez

a kockázati keretrendszer kialakítása – amely lehet integrált vagy különállóan kezelt.

A döntés megkönnyítése érdekében az alábbi táblázatokban összegyűjtöttük az integrált kockázati keretrendszer mellett szóló érveket, valamint azokat a szempontokat, amelyek az integrációval szembeni fenntartásokat indokolhatják.

Érvek az integráció mellett:

Érv	Magyarázat
Egységes irányítás	Könnyebb vezetői támogatás és átláthatóság
Költséghatékonyság	Meglévő eszközök és folyamatok újrahasznosítása
Audit szinergiák	ISO, GDPR és NIS 2 auditok összehangolhatók
Hatékonyabb képzés	Egységes biztonsági kultúra
Jobb incidenskezelés	Gyorsabb reagálás és riportolás
Beszállítói megfelelés	Könnyebb beszállítói lánc megfelelés
Vezetői támogatás	Kevesebb belső ellenállás
Fókuszált működés	NIS 2 a teljes governance részévé válik

Ellenérvek az integrációval szemben:

Ellenérv	Magyarázat
Szabályzati ütközések	Nehéz összehangolni eltérő struktúrákat
Komplexitás növekedése	Bonyolultabb compliance modell
Lassabb bevezetés	Több egyeztetést és validálást igényel
Auditálhatósági nehézségek	NIS 2-specifikus elemek nehezebben elkülöníthetők
Belső ellenállás	Szervezeti módosításokat nehezebben fogadják el
Fókuszvesztés	NIS 2 háttérbe szorulhat más szabályozások mellett

A NIS 2 kockázati keretrendszer szervezeti integrációja vagy különálló kezelése olyan stratégiai döntés, amelyet nem sablonos megoldások, hanem a szervezet sajátosságai alapján érdemes meghozni. a bemutatott érvek és ellenérvek világosan mutatják, hogy mindkét megközelítésnek megvannak a maga előnyei és kihívásai.

Az integrált modell különösen akkor jelent előnyt, ha a szervezet már rendelkezik érett információbiztonsági keretrendszerrel, például ISO/IEC 27001 tanúsítvánnyal, és célja a hosszú távú, fenntartható és költséghatékony megfelelés. a meglévő irányítási struktúra rugalmassága, a vezetői támogatás erőssége, valamint az auditok összehangolhatósága mind hozzájárulnak ahhoz, hogy az integráció ne csak technikai, hanem üzleti szempontból is megtérülő lépés legyen.

Ugyanakkor vannak olyan helyzetek, amikor célszerű lehet a NIS 2 követelmények külön kezelésére törekedni. Ilyen eset például, ha a szervezet jelenlegi struktúrája merev, túlterhelt vagy ha belső ellenállás tapasztalható a meglévő szabályozások módosításával szemben.

A különálló kezelés gyorsabb implementációt, egyszerűbb auditálhatóságot és dedikált felelősségi köröket kínálhat, ami egyes szervezeti kultúrákban hatékonyabb lehet.

A cél nem csupán a szabályoknak való megfelelés, hanem egy olyan kockázatkezelési modell kialakítása, amely valódi értéket teremt a szervezet számára üzleti stabilitás, reputációs védelem és működési biztonság formájában.

Bármely megközelítést választja is a szervezet, akkor jár el helyesen, ha azt stratégiai szemlélettel, az érintett vezetők tudatos együttműködésével, az intézményi sajátosságokra és a hosszú távú biztonsági célokra építve alakítja ki.

5.4. Rendelkezésre állási követelmények

A NIS 2 és a kapcsolódó magyar jogszabályok célja, hogy minden szervezet átlátható, mérhető és auditálható módon biztosítsa rendszerei és adatai folyamatos elérhetőségét, még váratlan események esetén is. Ehhez elengedhetetlen a kockázatok felismerése, az üzleti hatáselemzés (BIA) (lásd: 5.5.1. fejezet módszertan alkalmazása, a mentési és helyreállítási folyamatok kidolgozása, a magas rendelkezésre állású technikai megoldások alkalmazása, a dolgozók képzése, a vezetői felelősségvállalás, valamint a beszállítói megfelelőség és a folyamatos tesztelés.

A jogszabályi elvárások alapján minden szervezetnek rendszeresen fel kell mérnie, milyen kockázatok fenyegetik az informatikai rendszereiket (pl.: kibertámadás, hardverhiba, természeti katasztrófa). Ezekre a kockázatokra arányos, technikai és szervezeti védelmi intézkedéseket kell bevezetni (pl.: tűzfal, hozzáférés-kezelés, naprakész szoftverek, megfelelő fizikai védelem stb.). Minden dolgozónak tisztában kell lennie az alapvető információbiztonsági szabályokkal, és tudnia kell, mit kell tennie incidens esetén.

A szervezeteknek rendszeres adatmentéseket kell végezniük, amelyek legalább egy példánya fizikailag vagy logikailag elkülönítve van tárolva. a mentések visszaállításának sikerességét és a védelmi intézkedések hatékonyságát rendszeresen ellenőrizni kell. Mindezek mellett a rendszerek állapotát és a mentések eredményességét folyamatosan monitorozni és tesztelni szükséges.

A szolgáltatások folyamatos elérhetőségét redundáns (tartalék) szerverek, hálózati eszközök, terheléselosztási (load balancing) és automatikus átkapcsolási (failover) megoldások biztosítják. Ezek a megoldások lehetővé teszik, hogy egy hiba esetén a szolgáltatás ne álljon le teljesen, hanem a tartalék rendszer azonnal átvegye a feladatot. a kritikus útvonalban lévő elemeknél több rétegű redundanciát és automatikus failovert kell kialakítani. Magasabb biztonsági osztályok esetén alternatív működési helyszíneket (például tartalék szerverek, felhőszolgáltatások) is biztosítani kell.

A BIA eredménye alapján készül el az üzletmenet-folytonossági terv (BCP), amely mentén a helyreállítási feladatok prioritási sorrendbe sorolhatók, valamint a katasztrófa-helyreállítási terv (DRP) is elkészíthető, melynek pontosan tartalmaznia kell, hogy egy váratlan esemény után milyen lépésekben állítható helyre a működés.

A rendelkezésre állást nemcsak az egyes rendszerek önálló működése, hanem azok kölcsönös függőségei is befolyásolják. Egy szolgáltatás kiesése láncreakciót indíthat el, ezért a rendszerarchitektúrában szükséges jelölni minden komponens függőségét. a helyreállítási tervekben szerepelnie kell a függőségek sorrendjének és a helyreállítási prioritásoknak, hogy a „legalsó réteg” (pl.: hálózat, tápellátás) mielőbb visszaálljon.

A kritikus szolgáltatások esetében elvárás, hogy azok éves rendelkezésre állása legalább 99,9% legyen, ami legfeljebb 8,76 óra éves kiesést jelent. a rendelkezésre állás kiszámítása a következő képlet segítségével történhet:

Rendelkezésre állás (%) = ((éves üzemidő – állásidő) / éves üzemidő) × 100

> Például, ha egy szolgáltatás egész évben, éjjel-nappal üzemel (365 nap × 24 óra = 8760 óra), és az állásidő – például tervezett karbantartás, átállás vagy esetleges hibák miatti kiesés – éves szinten 8,76 órát tesz ki (ami a teljes éves üzemidő, azaz 8760 óra 0,1%-a), akkor a rendelkezésre állás:
> ((8760 – 8,76) / 8760) × 100 = 99,9%

Ha az informatikai működés részben külső partnertől (pl.: felhőszolgáltató, hoszting szolgáltatás, vagy IT üzemeltetés) függ, szerződésben szükséges rögzíteni a rendelkezésre állási,

mentési és helyreállítási követelményeket, és rendszeresen ellenőrizni kell ezek teljesülését (pl.: SLA, azaz szolgáltatási szint megállapodás formájában). Az SLA-k mellett a szervezeten belül, egyes részlegek vagy operatív egységek között is szükség lehet hasonló megállapodásokra, ezeket nevezzük OLA-knak. Az OLA célja, hogy a belső szolgáltatók és felhasználók között világosan rögzítse a szolgáltatási szinteket, felelősségeket és elvárásokat, biztosítva ezzel az SLA-ban vállalt külső kötelezettségek teljesítését is.

A hatékony üzemzavar- és karbantartás-értesítés alapját két kiegészítő nyilvántartás képezi:

- Érintetti kör nyilvántartás (stakeholder-regiszter): amely tartalmazza az üzemzavar vagy karbantartás által érintett személyek és szervezeti egységek elérhetőségi adatait, valamint a szükséges kommunikációs csatornákat és értesítési igényeket.
- Kiértesítési lánc (eszkalációs mátrix): folyamatleírás, amely meghatározza, hogy egy hiba vagy karbantartás esetén kinek, milyen sorrendben, milyen módon és milyen határidővel kell értesítést küldeni.

Mindkét nyilvántartás testreszabható Excelben vagy ITSM-rendszerben, így a kommunikáció megbízható, nyomon követhető és szabályozott marad. Együttes alkalmazásuk biztosítja, hogy minden érintett időben, a megfelelő formában és sorrendben kapjon tájékoztatást üzemzavar vagy halaszthatatlan karbantartás esetén.

5.5. Adatvagyon és BIA (üzleti hatáselemzés) szerepe

Egy szervezet úgy éri el célját, hogy termékeket szállít és szolgáltatásokat nyújt az ügyfeleinek. Olyan folyamatokat kell bevezetnie és fenntartania, amelyek szisztematikusan elemzik az üzleti hatásokat, értékelik a zavarok kockázatait és amelyek eredményei lehetővé teszik a szervezet számára az üzletmenet-folytonossági stratégiák és megoldások meghatározását.

Az üzleti hatáselemzés lehetővé teszi a szervezet számára, hogy prioritásokat határozzon meg a megszakadt tevékenységek folytatása érdekében. Fő célja, hogy a szervezet azonosítani tudja és fontossági sorrendbe tudja állítani (priorizálni) azokat a tevékenységeket, amelyek megszakadása sürgős intézkedést igényelhet, mivel a gyors folytatásuk elmulasztása elfogadhatatlan mértékű káros hatást eredményezhet. Lehetséges, hogy a gyorsan helyreállítandó tevékenységeken kívül más – vele függőségi viszonyban lévő – tevékenységeket is prioritássá kell tenni. Az elemzésnek ki kell terjednie az üzletmenet-folytonosság irányítási rendszer (BCMS) hatóköre alá tartozó valamennyi tevékenységre.

Az üzleti hatáselemzési folyamat első lépése a termékek és szolgáltatások rangsorolása, amelyet számos üzleti hatáselemzési folyamat (opcionális) és üzleti hatáselemzési tevékenység követ. Az egyes üzleti hatáselemzések hatóköre korlátozott lehet, de együttesen le kell fedniük a BCMS teljes hatókörét.

5.5.1. BIA folyamata

A BIA elkészítését előre meghatározott folyamat mentén kell elvégezni, mely folyamatlépések a következők:

BIA Tervezés

A BIA előkészítési szakaszának fő lépései a következők:

- Szükséges erőforrások elkülönítése,
- Termékek szolgáltatások csoportosítása,
- Folyamatokhoz tartozó kulcs szereplők azonosítása,
- Elvárások kommunikálása a résztvevők felé

BIA Folyamatra vonatkozó megközelítés elfogadása

A BIA sikeres megvalósítása érdekében a szervezetnek olyan keretrendszert kell kialakítania, amely egységesen kezeli a hatások feltárását, a kritériumok meghatározását és az időkeretek kijelölését. Ennek során az alábbi fő szempontok érvényesülnek:

- Hatások megértése: a BIA-folyamat következetes módon feltárja a termékek és szolgáltatások nyújtásának megszakításából eredő szervezeti hatást. A zavar származhat a vállalaton belülről, az ellátási láncból vagy más külső forrásból – ezek mindegyike az ügyfelek és más érdekelt felek részére történő egy vagy több termék és szolgáltatás nyújtásának zavarát eredményezheti. Fontos kiemelni, hogy a BIA során nem a zavar bekövetkezésének okait vizsgáljuk, hanem azt, hogy bekövetkezésük milyen üzleti hatással jár. A kockázat és a fenyegetés vizsgálata külön folyamat, a kockázatelemzés feladata.
- Hatás típusok és kritériumok meghatározása: a hatástípusok nem azonosak a kockázatkezelésben használt következménytípusokkal vagy kategóriákkal. A hatás a szervezetet érő zavar következménye. A hatástípusok és kritériumok kiválasztását befolyásolja a szervezet ágazata, kontextusa és tevékenységeinek jellege, valamint a szervezeti kultúra. Egy vagy több hatástípus és kritérium kiválasztásának – beleértve a mennyiségi és minőségi hatásinformációk szükségességét és az összegyűjtött részletesség szintjét – alkalmasnak kell lennie arra, hogy a szervezet kiválassza vagy igazolja az üzletmenet-folytonossági prioritásokat és követelményeket.
- Időkeret meghatározása: a hatások idővel szinte mindig növekednek. A hatások azonban nem mindig ugyanolyan ütemben növekednek. Az időbeli hatás nagyságrendjének értékeléséhez a szervezet választhat meghatározott számú időkeretet, amelyen belül a hatás nagyságrendjét vizsgálja (pl.: 1 óránál, 6 órá-nál, 24 óránál, 3 napnál, 1 hétnél), vagy meghatározott számú időkeretet, amelyen belül a hatás növekvő nagyságrendjét vizsgálja (pl.: 0-tól 1 óráig, 1-től 6 óráig, 6-tól 24 óráig). A választott tartományok a szervezetek között a kontextustól függően változhatnak.
- Módszertan meghatározása: Olyan egységes módszertant kell kialakítani, amely biztosítja, hogy minden termék, szolgáltatás és tevékenység értékelése során ugyanazokat az elveket és kritériumokat alkalmazzák – függetlenül attól, mikor történik az értékelés, vagy melyik csoport végzi azt.
- Meg kell határozni azt az időkeretet (MTPD), amelyen túl a zavar a szervezet számára már elfogadhatatlan. Emellett rögzíteni kell a megszakadt tevékenységek helyreállításának időkeretét is (RTO), amelyet az elfogadható szint figyelembevételével kell meghatározni. Fontos, hogy az RTO időtartama nem haladhatja meg az MTPD-t.

Termékek és szolgáltatások meghatározása a felsővezetés bevonásával

A folyamat célja, hogy a felsővezetés iránymutatása alapján világosan kijelölésre kerüljenek a szervezet által nyújtott termékek és szolgáltatások prioritásai, valamint a hozzájuk tartozó folytonossági elvárások:

- Áttekintés: a felsővezetésnek meg kell határoznia a szervezet által az ügyfeleinek nyújtott termékek és szolgáltatások prioritásait.

- Bemenetek meghatározása: a szolgáltatási prioritásokat nagyban befolyásolja az ügyfél igény, az esetleges jogi követelmény, teljesítés elmaradásának hatás vizsgálata. Ezeket előzetesen össze kell gyűjteni, és elemezni a döntéshozatalhoz.
- Termék- és szolgáltatási prioritás meghatározása: Az elfogadott módszertan alapján a felsővezetésnek minden egyes termék- és szolgáltatáscsoportra vonatkozóan el kell döntenie, hogy mennyi idő után válik elfogad-hatatlanná a szervezet számára, ha továbbra is elmarad a teljesítés. Ez határozza meg a kezdeti helyreállítás minimálisan elfogadható kapacitását, és azt, hogy milyen gyorsan kell visszatérni a teljes kapacitáshoz.
- Eredmények: Az eredményeknek egy listát kell alkotniuk a rangsorolt termékekről és szolgáltatásokról, valamint azok folyamatossági követelményeiről, amelyet a tevékenységek rangsorolásánál használnak fel.

Prioritást élvező tevékenységek meghatározása

A folyamat célja, hogy a szervezet egyértelműen azonosítsa és rangsorolja azokat a tevékenységeket, amelyek a termékek és szolgáltatások folytonosságának fenntartásához nélkülözhetetlenek. Ennek során a tevékenységek hatásait, időbeli követelményeit és függőségeit egységes módszertan alapján kell meghatározni:

- Áttekintés: a termékek és szolgáltatások prioritása befolyásolja a hozzájuk kapcsolódó tevékenységek prioritását. Azokban az esetekben, amikor egy tevékenység egy üzleti folyamat része, lehetséges, hogy a tevékenységet az üzleti folyamat többi tevékenységével együtt kell elemezni.
- Bemenetek meghatározása: a tevékenységek rangsorolásához szükséges inputok a következők: (1) a BIA-eljárás hatóköre; (2) hatástípusok és kritériumok; (3) a felsővezetés által meghatározott termékek és szolgáltatások prioritásai; (4) az ismert függőségek; (5) jogi, szabályozási és szerződéses követelmények (kötelezettségek).
- Tevékenységek azonosítása: a BIA-folyamat hatókörébe tartozó minden egyes termék és szolgáltatás esetében meg kell határozni a kapcsolódó tevékenységeket a hozzájuk tartozó felelősökkel.
- **A tevékenységek RTO-jának beállítása:** a hatástípusok és kritériumok, a meghatározott időkeretek és az elfogadott módszertan alapján a tevékenységek felelőseinek értékelniük kell a zavarból eredő időbeli hatásokat, meg kell határozniuk az MTPD-t, és meg kell határozniuk az RTO-t az egyes tevékenységek minimálisan elfogadható kapacitásával együtt.
- **A rangsorolt tevékenységek meghatározása:** a tevékenységek RTO-ja alapján a szervezetnek el kell készítenie egy listát a prioritást élvező tevékenységekről. a prioritást élvező tevékenységek stratégiákat és megoldásokat igényelnek, melyet a felső vezetésnek el kell fogadnia és jóvá kell hagynia.
- **Eredmények**: Megkapjuk a prioritási sorrendbe állított tevékenységek jóváhagyott listáját és minden egyes tevékenységre vonatkozóan a következőket: (1) a termékek és szolgáltatások, valamint a tevékenységek közötti kölcsönös függőségek és kapcsolatok azonosítását; (2) időbeli hatásokat; (3) megfelelő MTPD-ket; (4) megfelelő RTO-kat; (5) minimálisan elfogadható kapacitásokat.

Erőforrások és egyéb függőségekmeghatározása

A prioritást élvező tevékenységek kijelölését követően a szervezetnek pontosan fel kell

mérnie, hogy azok működéséhez, helyreállításához vagy fenntartásához milyen erőforrásokra és kapcsolódó függőségekre van szükség. a folyamat célja, hogy részletes áttekintést adjon a napi erőforrásigényekről és az azokhoz kapcsolódó feltételekről:

- **Az erőforrás és egyéb függőségi követelmények meghatározása:** a prioritást élvező tevékenységek meghatározása után a szervezetnek részletes képet kell kapnia a napi erőforrásigényekről, hogy azonosítani tudja a prioritást élvező tevékenységek helyreállításához vagy fenntartásához szükséges erőforrásokat.

Az erőforrások azonosításakor nem a az a döntő, hogy az erőforrás számvitelileg kinek a könyveiben szerepel, hanem a rendelkezési jog. Ha egy anyavállalat üzemelteti a rendszert és a helyi leányvállalatnak nincs ráhatása a beállításokra vagy a helyreállításra, akkor a helyi szervezetnek nincs rendelkezési joga, így a függőségi listában külső szolgáltatásként (függőségként) kell kezelnie, nem saját erőforrásként.

Erőforrásigény: Az azonosított erőforrásokra vonatkozóan a következő információkat kell összegyűjteni: (1) mennyiség, azaz a szükséges erőforrások mennyisége vagy száma időben (2) az időkeret(ek), amelyben az erőforrásoknak rendelkezésre kell állniuk; (3) az erőforrás jellemzői; (4) az információs erőforrások maximálisan tolerálható adatvesztése; (5) más erőforrásoktól való függőségek; (6) alkalmazandó jogi vagy szabályozási követelmények.

BIA eredmények elemzése és konszolidálása

A szervezetnek el kell végeznie egy végső elemzést (vagy az elemzések összevonását), ami magában foglalja a BIA-folyamat minden szintjéről összegyűjtött, validált és jóváhagyott információk áttekintését, és olyan következtetések levonását, amelyek az üzletmenet-folytonossági prioritásokhoz és követelményekhez vezetnek.

A szervezetnek ki kell választania a megfelelő kvantitatív és kvalitatív elemzési megközelítés(eke)t, amelyet befolyásolhat a szervezet típusa, mérete vagy jellege, valamint az erőforrás és készségbeli korlátok.

BIA eredményeinek felsővezetői jóváhagyása

A szervezetnek az alábbi kulcsfontosságú BIA-eredményeket a felsővezetés rendelkezésére kell bocsátania felülvizsgálatra, módosításra (ha szükséges) és jóváhagyásra, mielőtt a következő lépést megtenné:

- a termékek és szolgáltatások rangsorolása,
- az üzleti folyamatok rangsorolása (ha vállalták),
- a tevékenységek rangsorolása,
- az eredeti BIA hatályának megerősítése vagy a módosított BIA hatályának jóváhagyása.

BIA felülvizsgálata

- A Business Impact Analysis (BIA) rendszeres felülvizsgálata biztosítja, hogy a folyamat és az eredmények mindig naprakészek legyenek, és igazodjanak a szervezet aktuális működéséhez, környezetéhez és kockázataihoz:
- A BIA folyamatának és módszertanának felülvizsgálata: a BIA folyamatát és módszertanát felül kell vizsgálni a minőség folyamatos javítása érdekében. Az eredmények minőségének javítása miatt idővel különböző megközelítéseket lehet fontolóra venni, például a hatástípusok, az időkeretek, az információgyűjtési módszerek vagy a résztvevők megváltoztatásával.
- A BIA eredményeinek felülvizsgálata: a BIA eredményeit rendszeresen (jellemzően évente) felül kell vizsgálni, valamint

minden olyan esetben, amikor a szervezeten belül vagy a működési környezetében olyan jelentős változások történnek, amelyek hatással lehetnek az üzletmenet-folytonossági prioritásokra és követelményekre. a szervezet azon területein, amelyek a legutóbbi BIA óta alig változtak, elegendő lehet a korábbi BIA eredményeinek validálása a teljes BIA elvégzése helyett.

Egy jól elkészített üzleti hatáselemzés kulcsfontosságú eredményeket hoz, amelyek segítik a vállalatot abban, hogy a szervezet felkészüljön a váratlan eseményekre és fenntartsa a működés folytonosságát.

5.5.2. Várható eredmények

Az alábbiakban soroljuk fel a várható eredményeket:

Stratégiai eredmények

- Kritikus üzleti folyamatok azonosítása: pontosan meghatározható, mely tevékenységek elengedhetetlenek a működéshez.
- Prioritások felállítása: segít rangsorolni, mely folyamatokat kell elsőként helyreállítani egy zavar esetén.
- Válaszidők és tolerálható kiesések meghatározása: például RTO (Recovery Time Objective) és RPO (Recovery Point Objective) értékek.

Operatív eredmények

- Erőforrásigények feltérképezése: megmutatja, milyen humán, technológiai és pénzügyi erőforrásokra van szükség a kritikus folyamatok fenntartásához.
- Kockázatok és hatások számszerűsítése: lehetővé teszi a pénzügyi veszteségek, ügyfélvesztés vagy reputációs károk előrejelzését.
- Üzletmenet-folytonossági terv (BCP) megalapozása – a BIA eredményei alapján készül el a konkrét vészhelyzeti terv.

Védelmi és helyreállítási előnyök

- Helyreállítási stratégiák kidolgozása: például alternatív munkavégzési helyszínek, tartalék rendszerek vagy kommunikációs protokollok.
- Gyorsabb reagálás vészhelyzetekre: a BIA révén a szervezet nemcsak reagál, hanem proaktívan megelőzi a nagyobb károkat.
- Ügyfélbizalom és hírnév megőrzése: a zökkenőmentes működés biztosítása révén elkerülhető az ügyfélvesztés és a negatív megítélés.

5.6. Üzleti folyamatok feltérképezése

Az üzleti folyamatok feltérképezése kulcsfontosságú lépés a hatékony működés, digitalizáció, a kockázatkezelés és az információbiztonság felé. Segítségével átláthatóvá válik, hogyan működik egy szervezet, hol vannak szűk keresztmetszetek, és milyen fejlesztési lehetőségek rejlenek a folyamatokban. Egyúttal segíti a jogszabályi- és szabványi megfelelést (NIS 2, ISO 27001), valamint támogatja az auditálást és üzletmenet folytonosságot.

Módszertanok az üzleti folyamatokfeltérképezésére

- BPM (Business Process Management): Strukturált megközelítés, amely a folyamatok tervezését, modellezését, bevezetését, monitorozását és optimalizálását foglalja magában.
- BPR (Business Process Reengineering): Radikális újratervezés, ha a meglévő folyamatok nem hatékonyak.
- Folyamatábra és Sequence diagram: Vizualizáljuk a lépéseket, döntési

pontokat, szereplőket / erőforrásokat és adatáramlást.

- Hatáselemzés és kockázatelemzés: a folyamatok fontosságának / kritikusságának és sérülékenységének meghatározása.

Az elsődleges lépés az üzleti-, és támogató szolgáltatások (SLA, OLA) professzionális biztosítása, nyújtása tekintetében ezen szolgáltatásokat biztosító folyamatok meghatározása, sztenderdizálása, majd optimalizálása, egészen az automatizációig. Az üzleti folyamatok feltérképezése nem csak az üzleti célokat támogató tevékenység, de a feltérképezés, valamint a folyamat-érettségi szint emelése, újabb és újabb üzleti célokat hozhat.

Az üzleti- és támogató folyamatok rögzítése és kezelése többek között a szolgáltatáskatalógusban, a folyamatkatalógusban, az adatvagyonleltárban és a rendszerelem leltárban történik.

Az üzleti folyamatok érettségi szintje azt mutatja meg, hogy egy szervezet mennyire fejlett a folyamatai kezelésében, fejlesztésében és optimalizálásában. Ezeket az érettségi modelleket gyakran használják a vállalatok teljesítményének értékelésére és fejlesztési lehetőségek azonosítására.

A NIS 2 követelményrendszere kiemelt figyelmet fordít a folyamatok szabályozására és átlátható működtetésére, különösen az információbiztonsági támogató folyamatok terén. a cél, hogy az üzleti működés hosszú távon is biztonságosan és fenntartható módon valósulhasson meg.

Ide tartoznak többek között az EIR-ek engedélyezési és beszerzési folyamatai, a biztonságot alapértelmezésként kezelő fejlesztési (security by design, security by default) és telepítési eljárások, a konfigurációkezelés, a tesztelési és hibajavítási folyamatok, valamint a képzések és a karbantartás menedzsmentje. Ugyanilyen fontos a változáskezelés, az esemény- és incidenskezelés, a kommunikációs és onboarding folyamatok, a jogosultságok kezelése, a naplózási és kontrollmechanizmusok működtetése, a védelmi intézkedések felügyelete, az információbiztonsági mérési és ellenőrzési tevékenységek, az üzletmenet-folytonossági és kockázatelemzési eljárások, a sérülékenység-menedzsment, az EIR-ek teljes életciklusának kezelése, valamint a titkosítási, anonimizációs és beszállítói folyamatok biztosítása beleértve az ellátási lánc biztonságának fenntartását is.

Az üzleti- és támogató folyamatok feltérképezésének lépései

1. Célkitűzés meghatározása: Mely területekre fókuszálunk? (pl.: IT, HR, beszerzés stb.)
2. Érintettek bevonása: Kik a kulcsszereplők? (pl.: folyamatgazdák, végrehajtók, vezetők) + Workshopok, interjúkat, a valós működés megértése
3. Folyamatok azonosítása: Dokumentációk, szabályzatok + Fő- és alfolyamatok, kritikus folyamatok
4. Folyamatlépések részletes feltérképezése: Ki végzi? Mit csinál? Milyen eszközt használ? Milyen output keletkezik?
5. Folyamatok elemzése: Szűk keresztmetszetek, párhuzamosságok, felesleges lépések + Hol automatizálható?
6. Optimalizálási javaslatok kidolgozása: Egyszerűsítés, digitalizálás, szabványosítás + KPI-ok meghatározása a mérhetőséghez
7. Dokumentálás és kommunikáció
8. Folyamatos felülvizsgálat: Rendszeres audit, visszajelzések gyűjtése + Folyamatok frissítése a változásoknak megfelelően

5.7. A kockázatelemzés, figyelembe véve az ellátási lánc kockázatait

Az eddigiekben a kockázatelemzés általános szempontjait vizsgáltuk, a szervezeten belüli rendszerek, folyamatok és erőforrások szintjén. a teljes körű kockázatkezeléshez azonban elengedhetetlen, hogy figyelembe vegyük az ellátási láncban rejlő kockázatokat is – legyen szó beszállítókról, szolgáltatókról, logisztikai partnerekről vagy külső adatfeldolgozókról. Ezek a tényezők közvetlen hatással lehetnek a szervezet működésére, ezért elemzésük és beépítésük a kockázatkezelési rendszerbe különösen fontos.

A kockázatkezelés egy háromlépcsős ciklus, amelyet az ellátási lánc sajátosságaira is alkalmazni szükséges.

Kockázatok azonosítása

A potenciális veszélyforrások szisztematikus feltérképezése; az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) is kiemelt figyelmet fordít több kiadványában is az ellátási lánc elleni támadásokra.[24] Főbb kockázati területek, sebezhetőségi pontok, vagy kitettségi tényezők az ellátási láncban

- Humán és működési kockázatok: Adatszivárgás, a szolgáltatás leállása (pl.: zsarolóvírus miatt), vagy a beszállító munkatársai által elkövetett szándékos vagy véletlen károkozás (bennfentes fenyegetés) és a kiberbiztonsági tudatosság hiánya miatt bekövetkező incidensek.
- Szoftverellátási lánc: Kártékony kód bejuttatása a szállított szoftverbe, vagy annak nyílt forráskódú (OSS) komponenseibe, ahogy az a SolarWinds-incidens esetében is történt.
- Hardverellátási lánc: Manipulált vagy hamisított hardvereszközök, alkatrészek beépítése.

Kockázatok értékelése

Az azonosított kockázatokat rangsorolni kell a súlyosságuk alapján.

Kockázat = Bekövetkezési valószínűség x Hatás

A kockázat alapvetően két tényező szorzataként értelmezhető: a bekövetkezési valószínűség és a hatás mértéke. a bekövetkezési valószínűség azt jelöli, hogy mekkora eséllyel történik meg egy adott nem kívánt esemény egy meghatározott időtávon belül, míg a hatás a bekövetkező esemény pénzügyi, működési vagy reputációs következményeinek súlyosságát mutatja.

Például egy zsarolóvírus-támadás egy autóipari beszállítónál a termelési láncra gyakorolt hatása révén a vevő oldalán akár 5%-os termeléscsökkenést is eredményezhet. Ez jól szemlélteti, hogy a kockázat túlmutat az elsődleges célponton, és jelentős üzleti következményekkel járhat.

24 pl.: ENISA THREAT LANDSCAPE 2024 September 2024. DOI: 10.2824/0710888.

Egy adott incidens valószínűségének meghatározását segítheti az alábbi táblázat.

táblázat 5.1 Valószínűség meghatározása ötlépcsős skálán

Szint	Leírás
Nagyon alacsony	Nem ismertek korábbi hasonló támadások. A támadók nem motiváltak. Nincs ismert sérülékenység.
Alacsony	Nehezen támadható sérülékenységek léteznek. Ágazaton belül nem ismertek ilyen támadások. A támadók motivációja alacsony.
Lehetséges	Léteznek ismert sérülékenységek. A támadók motivációja közepes. Egyéb ágazatokban voltak ilyen támadások.
Várható	Léteznek ismert sérülékenységek, de a támadások nehezen automatizálhatóak. A támadók viszonylag motiváltak. Voltak hasonló korábbi támadások ágazaton belül.
Elkerülhetetlen	Léteznek ismert sérülékenységek és eszközök azok hatékony támadására. Nincs ismert ellenintézkedés. A támadók különösen motiváltak.

Egy adott incidens várható hatásának meghatározását pedig a következő táblázat tudja segíteni.

táblázat 5.2 Hatás meghatározása ötlépcsős skálán

Szint	Hatás leírása
Elenyésző	Elenyésző anyagi kár. A hírnév nem sérül. Házon belül hárítható. Nincs büntetés. Nincs környezeti hatás. A berendezések nem sérülnek. Emberi sérülés nincs. Személyes adatok nem érintettek.
Alacsony	Kisebb anyagi kár. Könnyen kezelhető hatás a jó hírnévre. Kisebb mennyiségű személyes adat érintett.
Közepes	Kellemetlenül magas anyagi kár és/vagy büntetések. Drága külső szakértők bevonása már szükséges. Minimális környezeti hatás. Közepes mennyiségű személyes adat érintett.
Jelentős	Jelentős anyagi kár és hírnév csorbulás. Még tartható mértékű büntetések. Korlátozott környezeti hatás. Személyi sérülés. Eszközök kisebb mértékű sérülése a fizikai térben. Jelentős mennyiségű személyes, illetve kevesebb érzékeny személyes adat érintett.
Katasztrofális	Emberi életek kerülnek közvetlen veszélybe. Jelentős környezeti hatás. Nagyobb horderejű berendezés-sérülés. Saját forrásból nem fedezhető anyagi kár vagy büntetések, amelyek csődhöz vezetnek. A jó hírnév teljes elvesztése. Nagy mennyiségű érzékeny személyes adat érintett.

Kockázatok kezelése

- Minden azonosított kockázatról döntést kell hozni. a négy fő stratégia:
- Elfogadás: a kockázat olyan alacsony, hogy tudatosan vállaljuk.
- Csökkentés: Kontrollok bevezetésével mérsékeljük a kockázatot. Ez a leggyakoribb eljárás.
- Áthárítás: a kockázat pénzügyi következményeinek áthárítása, jellemzően kiberbiztosítás révén.
- Elkerülés: a kockázatot hordozó tevékenység megszüntetése

5.8 Compliance scoring és a folyamatos megfelelés mérése

5.8.1 A compliance scoring szerepe a NIS2 megfelelési modellben

A NIS 2 irányelv egyik alapvető paradigmaváltása, hogy a korábbi, jellemzően statikus megfelelési megközelítést felváltja a folyamatos, kockázatalapú és vezetői felelősségen alapuló megfelelőség. Ennek megfelelően a megfelelőség nem értelmezhető kizárólag akként, hogy biztos dokumentumok léteznek-e a szervezetnél vagy időszakos auditok eredményeként, hanem dinamikusan változó állapotként, amelyet mérni, értékelni és irányítani szükséges.

E cél megvalósításának egyik kulcseszköze a compliance scoring rendszer, amely strukturált módon, objektív szempontok mentén képes számszerűsíteni egy szervezet NIS 2-nek való megfelelési állapotát. A compliance scoring egyszerre szolgálja:

- a kockázatalapú döntéshozatalt,
- a vezetői felügyelet bizonyíthatóságát,
- az auditálhatóságot,
- valamint a folyamatos fejlesztés (continuous improvement) elvét.
- valamint a folyamatos fejlesztés (continuous improvement) elvét.

A NIS 2 irányelv 21. cikke által előírt technikai és szervezési intézkedések, valamint a 32. cikk szerinti vezetői felelősség teljesítése csak akkor tekinthető hitelesnek, ha azok állapota mérhető és visszakövethető.

5.8.2 Jogszabályi háttér és megfelelőségi elvárások

A compliance scoring alkalmazása közvetetten több jogszabályi kötelezettség teljesítését is támogatja, különösen az alábbiak vonatkozásában:

- (EU) 2022/2555 irányelv (NIS2)
    - 21. cikk: kockázatkezelési és védelmi intézkedések
    - 23. cikk: incidensjelentési kötelezettség
    - 32. cikk: irányító testület felelőssége
- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és felügyeletről (Magyarországon a NIS2 végrehajtásának kerettörvénye)
- 2016/679/EU rendelet (GDPR) – különösen az elszámoltathatóság (accountability) elve

A compliance scoring önmagában nem jogszabályi követelmény, azonban bizonyíthatóan támogatja a fenti előírások teljesítését, különösen a vezetői kontroll és a felügyeleti hatóság felé történő alátámaszthatóság szempontjából.

5.8.3 A compliance scoring céljai és alapelvei

A compliance scoring rendszer kialakításának fő céljai az alábbiak:

1. Objektív mérhetőség: A megfelelőség szubjektív megítélése helyett számszerűsíthető, összehasonlítható állapot meghatározása.
2. Kockázatalapú priorizálás: Nem minden hiányosság azonos súlyú. A scoring lehetővé teszi a kritikus kockázatok azonosítását és priorizálását.
3. Vezetői döntéstámogatás: A vezetői testület számára értelmezhető, aggregált mutatók biztosítása.
4. Audit- és hatóságállóság: A megfelelőségi állapot időbeli alakulásának bizonyítható dokumentálása.
5. Folyamatos fejlesztés ösztönzése: Trendek és romló/javuló területek azonosítása.

Alapelvként érvényesül, hogy a scoring:

- arányos legyen a szervezet méretével és kockázati profiljával,
- transzparens módszertanon alapuljon,
- ismételhető és auditálható legyen.

5.8.4 A compliance scoring dimenziói

A NIS2-nek való megfelelés komplexitása miatt a scoring többdimenziós modellben értelmezhető. A javasolt fő dimenziók:

- Governance és szervezeti megfelelés
    - szerepkörök és felelősségek definiáltsága
    - vezetői felügyelet és jóváhagyások
    - belső szabályozottság (IBSZ, eljárásrendek)
- Technikai védelmi intézkedések
    - hozzáférés-kezelés, MFA
    - hálózati szegmentáció
    - naplózás, monitorozás
    - mentések és helyreállítás
- Kockázatkezelés és vagyonleltár
    - információs- és rendszervagyon nyilvántartása
    - rendszeres kockázatelemzés
    - kritikus szolgáltatások azonosítása
- Ellátási lánc és beszállítói megfelelés
    - beszállítói átvilágítás
    - szerződéses biztonsági követelmények
    - folyamatos vendor monitoring
- Incidenskezelési képesség
    - incidenskezelési terv
    - bejelentési határidők betartása
    - gyakorlatok és tanulságkezelés
- Dokumentáltság és evidenciák
    - auditnyomok megléte
    - naprakész dokumentáció
    - visszakövethetőség

5.8.5 Pontozási modell és súlyozás

A compliance scoring tipikusan 0–5-ig vagy 0–100-ig terjedő skálán történik, ahol az egyes dimenziók külön-külön értékelhetők, majd aggregálhatók.

Ajánlott megközelítés:

- 0 – nincs megvalósítva
- 1 – részben szabályozott
- 2 – dokumentált, de nem működik következetesen
- 3 – működik, de nem mérik
- 4 – működik és mérik

- 5 – optimalizált, automatizált

A NIS2 kritikus szolgáltatásaihoz kapcsolódó kontrollok magasabb súlyt kapnak, különösen:

- incidenskezelés,
- ellátási lánc,
- hozzáférés-kezelés.

5.8.6 Compliance Scoring mintatáblázat (alkalmazási példa)

Az alábbi minta bemutatja, hogyan lehet a compliance scoring módszertanát gyakorlati ellenőrzési táblázat formájában alkalmazni. A táblázat célja a kontrollok strukturált értékelése és az evidenciák rögzítése.

Kontroll terület	Kontroll leírása	NIS2 hivatkozás	Pontszám (0–5)	Evidencia	Megjegyzés
Governance	Kiberbiztonsági felelősségek formális kijelölése	21. cikk			
Governance	Vezetői szintű kiberbiztonsági jelentések	21. cikk			
Kockázatkezelés	Információs vagyonleltár megléte	21. cikk			
Kockázatkezelés	Rendszeres kockázatelemzés	21. cikk			
Technikai kontrollok	Többfaktoros hitelesítés alkalmazása	21. cikk			
Technikai kontrollok	Hálózati szegmentáció	21. cikk			
Monitorozás	Naplózás és naplóelemzés	21. cikk			
Incidenskezelés	Incidenskezelési eljárásrend	23. cikk			
Incidenskezelés	Incidensgyakorlatok végrehajtása	23. cikk			
Ellátási lánc	Beszállítói kiberbiztonsági követelmények	21. cikk			

A pontozás során minden kontrollhoz pontszám rendelhető a 0–5 skálán, rövid indoklás és dokumentált evidencia társítható, valamint rögzíthetők a szükséges fejlesztési intézkedések. A táblázat rendszeres frissítése lehetővé teszi a megfelelési állapot időbeli követését, valamint támogatja a vezetői szintű kiberbiztonsági döntéshozatalt. A módszer különösen hatékony akkor, ha a táblázatot egy központi governance, risk and compliance (GRC) rendszer vagy dedikált megfelelőségkezelő eszköz támogatja.

5.8.6 Riportolás és vezetői dashboard

A compliance scoring valódi értéke a vezetői riportolásban jelenik meg. A javasolt riportolási szintek:

- Operatív szint: részletes pontszámok, hiányosságok (GAP-ek),
- Menedzsment szint: dimenziónkénti összesített értékek,
- Vezetői testület: trendek, kockázati hőtérkép.

A dashboard alkalmas a romló megfelelési trendek jelzésére, audit előtti felkészülésre, és a hatósági megkeresések alátámasztására. A compliance scoring eredményeit legalább az alábbi gyakorisággal ajánlott riportálni:

Operatív szint: negyedévente,

Menedzsment szint: félévente,

Vezetői testület: évente, vagy jelentős incidens esetén rendkívül.

A riportoknak tartalmazniuk kell a pontszámokat dimenziónként, az előző időszakhoz viszonyított változásokat, a fő kockázati megállapításokat. A compliance scoring rendszer egyik legfontosabb célja a vezetői döntéstámogatás. Ennek érdekében célszerű egy olyan dashboard kialakítása, amely egyszerre biztosít áttekinthetőséget és megfelelő részletezettséget.

Egy vezetői NIS 2 dashboard tipikusan az alábbi elemeket tartalmazza:

- **Összesített megfelelési mutató**
    - Teljes szervezeti compliance pontszám,
    - Előző időszakhoz viszonyított változás,
    - Célértékek.
- **Dimenziónkénti megfelelési állapot** (a fő kontroll területek pontszámait például radar diagram vagy oszlopdiagram formájában):
    - Governance,
    - Kockázatkezelés,
    - Technikai kontrollok,
    - Incidenskezelés,
    - Ellátási lánc biztonság,
    - Dokumentáció és evidenciák.
- **Kritikus kockázatok:** A dashboard kiemeli a legalacsonyabb pontszámú kontrollokat, a kritikus infrastruktúrákat érintő kockázatokat és a beszállítói kockázatokat.
- **Incidens- és eseménystatisztikák**
    - Jelentett incidensek száma,
    - Incidenskezelési idő,
    - Incidensgyakorlatok eredményei.
- **Fejlesztési intézkedések állapota**
    - Folyamatban lévő biztonsági fejlesztéseket,
    - Határidőket,
    - Felelős szervezeti egységeket.

A NIS 2 szabályozás egyik lényeges eleme a vezetői felelősség erősítése. Ennek megfelelően a compliance scoring és a vezetői dashboard nem csupán technikai eszköz, hanem a szervezeti kiberbiztonsági irányítás kulcseleme. A rendszeres és strukturált riportolás biztosítja, hogy a vezetői testületek megfelelő információk birtokában hozhassanak döntéseket a kiberbiztonsági kockázatok kezeléséről.

06

Azonosított EIR-ek és rendszer-elemek

A NIS 2 irányelv magyarországi alkalmazása az információ- és kiberbiztonság általános szintjének növelését célozza meg, továbbá új fogalmakat és kötelezettségeket vezet be a szervezetek és szolgáltatók folyamataiba. Az egyik legfontosabb ilyen fogalom az EIR, azaz az Elektronikus Információs Rendszer, amely nem csupán technikai eszközök halmazát jelenti, hanem egy komplex, funkcionálisan összekapcsolt rendszert, amely adatokat kezel, szolgáltatásokat nyújt, és közvetlen hatással van a szervezet működésére.
Ez a fejezet arra vállalkozik, hogy közérthetően bemutassa, mit is értünk pontosan EIR alatt, hogyan lehet ezeket a rendszerelemeket azonosítani, csoportosítani, és milyen szempontok szerint kell őket biztonsági osztályba sorolni. a cél nem csupán a megfelelés biztosítása, hanem a szervezet kiber-ellenállóképességének tudatos és fenntartható fejlesztése.

6. Azonosított EIR-ek és rendszerelemek

Írták: dr. Albert Ágota, Barbul Gergő, Bódis Péter, dr. Jakobetz András, dr. Lendák Imre, Lóth Tamás, Maczkó Péter, Major Róbert, Mandrik Edina, Máté Márk, Dr. Tiszolczi Balázs Gergely

6.1. Mit tekintünk EIR-nek?

Az EIR, mint definíció

Az EIR fogalmának megértéséhez a jelenleg hatályos jogszabályok a következő támpontokat adják. a Kiberbiztonsági tv. definíciója – 24. elektronikus információs rendszer – alapján az EIR:

„a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,

[A 2003. évi C., az elektronikus hírközlésről szóló törvény 22. Elektronikus hírközlő hálózat definíciója: jelek vezetékes vagy vezeték nélküli úton elektronikus hírközlő eszközökkel történő továbbítását lehetővé tevő, állandó infrastruktúrán vagy központilag adminisztrált kapacitáselosztáson alapuló rendszerek, továbbá adott esetben kapcsoló vagy útválasztó eszközök, valamint más erőforrások, beleértve a nem aktív hálózati elemeket is. Elektronikus hírközlő hálózat különösen a műholdas hálózat, a helyhez kötött – vezetékes vagy vezeték nélküli – hálózat és a mobil rádiótelefon-hálózat; az energiaellátó kábelrendszerek olyan mértékben, amennyiben azokat a jelek továbbítására használják, valamint a műsorterjesztő hálózat.]

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy

c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;”

A fenti definíció többféle azonosítási és értelmezési megközelítést is lehetővé tesz. Összefoglalva azonban az EIR-t célszerű inkább jogi kategóriaként kezelni, nem pedig informatikai értelemben, ahol általában IT rendszerek vagy megoldások bizonyos szempontú gyűjtőhalmazáról van szó. Ennek megfelelően az EIR általában nem feleltethető meg egyetlen konkrét IT rendszernek, hanem inkább IT megoldások csoportjának tekinthető.

Az azonosításhoz és csoportosításhoz a következő fejezetek nyújtanak további támpontot. Mielőtt azonban ezekre rátérnénk, érdemes áttekinteni azt is, hogy mi az, amit nem célszerű EIR-ként azonosítani.

Miért fontos az EIR-ek azonosítása?

Audit díjakat befolyásolja: az SZTFH rendelet szerint az EIR-ek száma hatással van a kiberbiztonsági audit és hatósági felügyeleti díj költségére
Kockázatkezelés alapja: az EIR-ekhez kapcsolódó kockázatok azonosítása kulcsfontosságú a NIS 2 megfeleléshez
Biztonsági osztályba sorolás: az MK rendelet alapján minden EIR-t biztonsági osztályba kell sorolni, és ehhez védelmi intézkedéseket kell rendelni

Mit nem azonosítunk EIR-ként?

A jogszabályi áttekintésből és értelmezésből kiderül, hogy a szervezetek nem kapnak olyan részletes iránymutatást, amely alapján egyértelműen meghatározható lenne, mely elemeket célszerű EIR-ként azonosítani, és mely informatikai megoldások nem tartoznak ebbe a körbe.

A helyes EIR azonosítás kulcsa, hogy a kritikus függőségeket, az üzleti folyamatok fontosságát

és a kockázatokat is figyelembe vegyük, és minden esetben funkcionális egységként kezeljük az informatikai rendszereket.

Ennek megfelelően, az azonosítást megelőzően javasolt ezeket a szempontokat áttekinteni, különösen az üzleti folyamatokat és kockázatokat. Továbbá ezek kritikusságát szem előtt tartva célszerű értékelni és rangsorolni az egyes informatikai megoldásokat és azok fontosságát.

Ha ez az értékelés rendelkezésre áll, annak alapján meghatározható, mely megoldásokat nem célszerű EIR-ként azonosítani, mivel sem a fő üzleti tevékenységekhez nem kapcsolódnak, sem pedig olyan kockázati szinttel nem rendelkeznek, amely a kockázatokkal arányos védelem elve szerint ezt indokolná.

Elsődleges és támogató rendszerelemek

Az EIR olyan, egymással szorosan összefüggő informatikai komponensek logikus egysége, amely egy adott üzleti vagy közigazgatási célt szolgál. Az EIR meghatározásakor elsődleges szempont, hogy ne technikai elemek szerint, hanem üzleti funkcionalitás alapján történjen a rendszer lehatárolása. Az infrastruktúra-elemek – hálózat, szerver, operációs rendszer, alkalmazás, adatok, üzemeltetési folyamatok és a kapcsolódó személyzet – egységesen alkotják azt a rendszert, amely az üzleti vagy közigazgatási folyamatok működését biztosítja.

A gyakorlat azt mutatja, hogy az érintett szervezetek általában egy-egy üzleti funkció ellátását biztosító IT rendszerek összességét szokták EIR-ként azonosítani pl. Internet szolgáltatással foglalkozó cégeknél azon eszközök és folyamatok halmazát, amelyek szükségesek a szolgáltatás szállításához és folytonosságához, ide értve a betápokat, router-eket, üzleti szoftvereket és akár az ügyfél-oldali eszközöket is, amennyiben azok a szolgáltató birtokában vannak, illetve kritikus gyártásnál egy vagy több teljes gyártó üzemet.

Ahogyan az az előző fejezetben is kifejtésre került, a helyes EIR-azonosítás alapja a kritikus függőségek, az üzleti folyamatok jelentősége és a kockázatok figyelembevétele, valamint a rendszer következetes, funkcionális egységként való kezelése. Ez a megközelítés biztosítja, hogy a védelem, a megfelelőség és az üzletmenet-folytonosság valóban a szervezet működését támogassa.

A szervezetek EIR-jeinek többsége saját irányítás, felügyelet és üzemeltetés alatt áll, azonban előfordulhatnak olyan rendszerek is, amelyek felett a szervezet nem rendelkezik teljes körű kontrollal. Ebbe a kategóriába azok az információs rendszerek tartoznak, amelyek irányítását, fejlesztését, üzemeltetését, felügyeletét vagy alapvető infrastruktúráját nem maga a szervezet, hanem külső szolgáltató vagy állami szerv biztosítja. Ilyenek például a külső felhőszolgáltatók által nyújtott, szervezeten kívül üzemeltetett Software-as-a-Service (SaaS) alkalmazások vagy az elektronikus közszolgáltatásokhoz kapcsolódó, a kormányzat által központilag biztosított infokommunikációs rendszerek.

Az EIR-ek azokat a technikai és emberi elemeket foglalják magukba, amelyek digitális adatok kezelésére szolgálnak, és kritikus szerepet játszanak az üzleti folyamatok működésében és védelmében. Mi számíthat üzleti tevékenységhez kapcsolódó rendszernek? Néhány példa ezekre:
ERP rendszerek (pl.: SAP, Navision)
CRM rendszerek (pl.: Salesforce, MiniCRM)
HR rendszerek (pl.: Nexon, Workday)

- Pénzügyi és könyvelési rendszerek
- Termelésirányító rendszerek (MES, SCADA)
- Dokumentumkezelő rendszerek (DMS)
- Webes platformok, webshopok, ügyfélportálok
- Mobil alkalmazások és API-k

Ezeket a rendszereket az EIR-nyilvántartásban nem saját rendelkezési jog alatt állóként kell szerepeltetni, figyelembe véve, hogy a szervezet felelőssége ezek esetében korlátozott, ugyanakkor a használatukból eredő kockázatok kezeléséről továbbra is gondoskodni szükséges.

Az EIR-ek meghatározásakor a komponensek szerepük szerint elsődleges és támogató rendszerelemekre oszthatók. Az elsődleges rendszerelemek azok a komponensek, amelyek közvetlenül támogatják az EIR által lefedett üzleti vagy közigazgatási folyamatot, és annak alapvető működését biztosítják. Ezek nélkül az adott folyamat nem lenne működőképes vagy kölcsönös hatást gyakorolnak egymásra.

A támogató rendszerelemek olyan komponensek, amelyek nem közvetlenül, de nélkülözhetetlenül hozzájárulnak az EIR működéséhez, vagy több EIR-hez is kapcsolódhatnak. Ezek jellemzően háttérfolyamatokat, kiegészítő szolgáltatásokat biztosítanak. Több EIR-hez is kapcsolódhatnak, nem kizárólagosak egy adott EIR számára. Funkciójuk támogató, de nélkülözhetetlen a teljes rendszer biztonságos és üzemszerű működéséhez.

A támogató rendszerelemek – mint például a közös infrastruktúra, hitelesítési szolgáltatások, mentési, monitoring vagy vírusvédelmi megoldások – jellemzően több elsődleges EIR-t is kiszolgálnak. Emiatt kockázati profiljuk és a rájuk vonatkozó kontrollok eltérhetnek az egyes üzleti vagy közigazgatási EIR-ekétől. Ilyen esetekben célszerű ezeket a támogató rendszerelemeket önálló EIR-ként vagy dedikált támogató EIR-csoportként kezelni, saját felelősségi és kockázatértékelési rendszerrel. Ez a megközelítés segít elkerülni, hogy a fő EIR-ek indokolatlanul bonyolulttá váljanak. Az elkülönítés akkor indokolt, ha a támogató rendszerelem ténylegesen több EIR működésére is hatással van, ilyenkor a kockázatértékelésnek önállóan, de a támogatott EIR-ekre gyakorolt hatás figyelembevételével kell megtörténnie, nem pedig azok kockázatainak automatikus átvételével.

A kockázatalapú kontroll-szelektálás lehetővé teszi, hogy az elsődleges EIR-hez képest arányos, a támogató rendszerelem funkciójához igazodó intézkedéseket alkalmazzunk. a kontrollszelektálás során üzleti hatáselemzés (BIA) alapján mérjük fel, mely komponensek kiesése milyen üzleti kárt okoz, és válasszuk a kockázattal arányos védelmi intézkedést. a támogató rendszerelemek kiesése csak funkció szintű, átmeneti zavart okoz, helyreállításukra külön terv (pl.: alternatív hitelesítési útvonal, mentésből történő visszaállítás) alkalmazandó.

Az EIR-ek átlátható és auditálható kezelésének alapja a naprakész adatvagyon leltár és eszközleltár vezetése. Ezek a leltárak biztosítják, hogy a szervezet pontosan ismerje, milyen adatokat, információs eszközöket és rendszerelemeket kezel, valamint ezek mely EIR-hez tartoznak.

A két leltár egymást kiegészítve, egységes rendszerben támogatja az EIR-ek helyes azonosítását, a felelősségek kijelölését, a kockázatok feltérképezését és a megfelelőségi követelmények teljesítését.

Nem a szervezet tulajdonában és rendelkezésében álló rendszerek

A kiberbiztonsági megfelelés egyik kulcskérdése, hogy egy szervezet milyen rendszerekért felel, és milyen határokon belül kell alkalmaznia a biztonsági kontrollokat, valamint vállalnia a rendszer működéséért és az abban bekövetkezett incidensekért a felelősséget. Ezt a megkülönböztetést mind a Kiberbiztonsági tv., mind az MK rendelet a „rendelkezésben levő” fogalmán keresztül határozza meg. a Kiberbiztonsági tv. a rendelkezésben állást a szervezethez tartozó rendszerként értelmezi, amelyre a biztonsági osztályba sorolás és a védelmi intézkedések kötelezően alkalmazandók. Bár a törvény nem ad külön definíciót, a gyakorlatban a rendelkezésben állás azt jelenti, hogy a szervezet irányítja

a rendszer működését, hozzáféréseit, adatkezelését vagy konfigurációját függetlenül attól, hogy a rendszer fizikai tulajdonban van-e.

A rendelet 2. § (3) bekezdése kimondja: „Ha a szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a [.] követelményeket ezen elemek és funkciók tekintetében kell teljesíteni."

Ez a rendelkezés kifejezetten elismeri a részleges rendelkezési jogot, és lehetővé teszi a rendszerhatárok vertikális és horizontális értelmezését. a rendelet tehát nemcsak a teljes rendszerekre, hanem azok komponenseire is alkalmazza a rendelkezésben állás fogalmát, amennyiben a szervezet felelősségi köre kiterjed rájuk.

Ez az értelmezés összhangban áll a NIST SP 800-37 által meghatározott „authorization boundary" fogalmával, amely az információs rendszer azon komponenseinek összességét jelöli, amelyeket egy hivatalos engedélyező személy jóváhagyásával működtetnek. Ez a határ kizárja azokat a rendszereket, amelyek külön engedéllyel rendelkeznek, még akkor is, ha kapcsolódnak az adott rendszerhez. a fogalom célja, hogy világos határt húzzon a biztonsági kontrollok alkalmazási területén belül, és meghatározza, ki felel az adott rendszer biztonságáért. a NIST SP 800-37 és a Kiberbiztonsági tv. eltérő szabályozási környezetből származnak, de közös céljuk a felelősségi körök és biztonsági határok egyértelmű meghatározása. a „rendelkezésben állás" és az „authorization boundary" fogalmai e cél mentén értelmezhetők.

A rendszerhatárok értelmezése során két dimenzió különíthető el:

- Horizontális értelmezés: a rendszer különböző komponensei eltérő szervezeti kontroll alatt állhatnak.
  Például egy szerver a vállalat tulajdonában van, de a hálózati infrastruktúrát az anyavállalat biztosítja. Ilyen esetben csak a szerver tartozik a szervezet rendelkezésében álló rendszerek közé.
- Vertikális értelmezés: Egy szolgáltatás technológiai rétegei közötti felelősségmegosztás. Felhőszolgáltatás esetén a szervezet akkor is rendelkezési joggal bírhat, ha nem birtokolja fizikailag a rendszert, de ő irányítja valamely réteg – például az alkalmazás szintű hozzáférések – működését.

Amennyiben az elválasztási elvek alapján megállapítható a részleges rendelkezési jog, az érintett elektronikus információs rendszert kötelezően be kell sorolni a megfelelő biztonsági osztályba. Ebben az esetben az auditor a szervezetnél lokálisan megvalósított kontrollokat (pl. jogosultságkezelés, konfigurációkezelés stb.) közvetlenül vizsgálja.

Helyes gyakorlat, ha a szervezet az EIR, vagy ha a részletezettség miatt szükséges, az informatikai eszközök nyilvántartásában (leltár) pontosan rögzíti a rendelkezési kategóriákat:

- Saját rendelkezésű: Teljes körű kontroll a szervezetnél.
- Külső (szolgáltatói) rendelkezésű: Pl. SaaS szolgáltatások, ahol a kontroll korlátozott.
- Osztott rendelkezésű: Pl. IaaS/PaaS környezetek vagy kiszervezett üzemeltetés.

Osztott rendelkezés esetén kritikus a felelősségi körök pontos elhatárolása (Felelősségi mátrix / RACI), definiálva, hogy mely rendszerelemek és funkciók felett gyakorol ellenőrzést a szervezet, és melyek tartoznak a szolgáltató hatáskörébe.

Napjainkban a digitális szolgáltatások kiszervezése, a felhőalapú megoldások térnyerése, a komplex beszállítói láncok és a globalizált szolgáltatások elterjedése következtében egyre gyakoribb, hogy a szervezetek olyan informatikai rendszereket, rendszerelemeket vagy rendszerfunkciókat vagy rendszerelemeket használnak, amelyek nem állnak közvetlen

rendelkezésükben. Ezek a rendszerek ugyanakkor gyakran üzletileg kritikus adatokat kezelnek, vagy alapvető szolgáltatásokat biztosítanak. a kiberbiztonsági megfelelés és a kockázatok kezelése érdekében elengedhetetlen, hogy a szervezet megfelelő kontrollokat érvényesítsen ezekben az esetekben is.

A saját rendelkezésben lévő rendszerekhez képest a különbség abban rejlik, hogy a védelmi követelmények teljesítése érdekében a hangsúlyt a szerződéses biztosítékok kialakítására, a beszállítói lánc kontrolljára, valamint az incidensmenedzsmentre kell helyezni. a szerződéses rendelkezéseknek ki kell terjedniük a szolgáltató mellékkötelezettségeinek pontos meghatározására és szükség esetén azok érvényesítésére. Kiemelt jelentőségű az SLA-k olyan módon történő meghatározása, amely lefedi a biztonsági és üzletmenet-folytonossági követelményeket, valamint az incidensek észlelésére, jelentésére és kezelésére vonatkozó elvárásokat. a megfelelőség biztosítása érdekében a szervezetnek rendelkeznie kell ellenőrzési joggal, és ténylegesen végre is kell hajtania a szolgáltatóval szembeni auditokat. Emellett célszerű előre meghatározni egy átgondolt exit stratégiát is, amely biztosítja a szolgáltatási viszony biztonságos és kontrollált lezárását.

6.2. Biztonsági osztályba sorolás irányelvei

A szervezet elektronikus információs rendszereit biztonsági osztályba sorolja. A biztonsági osztályba sorolás alapvető célja annak meghatározása, hogy egy adott rendszerrel kapcsolatban milyen súlyosságú következményekkel járhat egy biztonsági esemény bekövetkezése. A biztonsági osztályba sorolás irányelveit az MK rendelet intézményesíti, amely meghatározza azokat a szempontokat, amelyek alapján az elektronikus információs rendszereket minősíteni kell. A biztonsági osztályba sorolást minden esetben az adott elektronikus információs rendszerben kezelt adatok jellege, valamint a rendszer által ellátott funkciók határozzák meg. A besorolás elvégzése a szervezet felelőssége. Ennek során a szervezetnek meg kell vizsgálnia, hogy egy esetleges biztonsági esemény milyen hatást gyakorolhat az általa működtetett rendszerre, az abban kezelt adatokra, valamint a szervezet működésére.

A biztonsági osztályba sorolást megalapozó értékelés során az EIR-rel kapcsolatban fennálló fenyegetéseket is figyelembe kell venni. Ezek között lehetnek fizikai események (például tűz, vízkár, áramkimaradás), technológiai kockázatok (szoftverhibák, különböző kibertámadások), emberi tényezők (hibás kezelés, jogosulatlan hozzáférés), valamint szándékos károkozás (adatlopás, szabotázs).

A jogalkotó három biztonsági osztályt különböztet meg: alap, jelentős és magas. Az MK rendelet sajátossága, hogy nem közvetlenül az egyes biztonsági osztályok tartalmát definiálja, hanem azt határozza meg, hogy milyen jellegű és súlyosságú káresemények következhetnek be egy adott rendszer sérülése esetén, és ezekhez rendeli hozzá a megfelelő biztonsági osztályt. Ennek megfelelően az alap biztonsági osztályhoz csekély káresemény, a jelentős biztonsági osztályhoz közepes káresemény, míg a magas biztonsági osztályhoz nagy káresemény tartozik.

A csekély káresemény (~alap biztonsági osztály) az alábbi esetek valamelyikének fennállásával jellemezhető:

- az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
- a szervezet üzleti vagy ügymenete szempontjából csekély értékű vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
- a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy

- a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

A közepes káresemény (~jelentős biztonsági osztály) az alábbi körülmények valamelyikének fennállása esetén következhet be:

- nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
- a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,
- a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

A nagy káresemény (~magas biztonsági osztály) az alábbi esetek valamelyikének fennállásával jellemezhető:

- különleges személyes adat nagy mennyiségben sérülhet,
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
- nemzeti adatvagyon helyreállíthatatlanul megsérülhet,
- az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
- a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,
- súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

Megfigyelhető, hogy a (személyes) adatok mennyisége determinálhatja a káresemény súlyosságát, így kiemelt jelentősége van az egyes fogalmak elhatárolásának. Elsőként fontos (lenne) egyértelműen különbséget tenni „kis mennyiségű" és „nagy mennyiségű" személyes adat között. Számos szakmai diskurzus tárgya volt és vélhetően lesz is még ennek vizsgálata, azonban e körben mindeddig nem alakult ki konszenzus.

A jogértelmezési nehézség abban áll, hogy mennyiségi elhatárolások esetében a normavilágosság küszöbértékek meghatározásával biztosítható. Ilyen küszöbértékeket azonban autentikus jogforrás egyelőre nem intézményesített, és az sem jelenthető ki egyértelműen, hogy az értelmezési bizonytalanság rendezése hatósági, jogalkotói vagy esetleg uniós szinten lenne indokolt. Következésképpen jelenleg nem áll rendelkezésre egzakt válasz arra vonatkozóan, hogy mi tekinthető még „kis mennyiségű", illetve már „nagy mennyiségű" személyes adatnak. E körben ezért legfeljebb orientáló jellegű szempontok fogalmazhatók meg:

- bizonyosan már nagy mennyiségű személyes adatot tartalmaznak az országos vagy regionális adatbázisok, valamint azok a

rendszerek, amelyeken keresztül ilyen adatbázisok hozzáférhetők;

- kisebb, a helyi piacon versengő szolgáltatók adatbázisai vélhetően csak kis mennyiségű személyes adatot tartalmaznak, azonban egy kisebb településen egyedüliként szolgáltató szervezet adatbázisa – nagy lefedettség esetén – már nagy mennyiségű személyes adatot is tartalmazhat;
- szintén valószínűsíthetően kisebb mennyiségű személyes adatot tartalmaz egy szervezet belső „munkaügyi" nyilvántartása, amely alól kivételt képezhetnek a horizontálisan és/vagy vertikálisan tagolt, nagyobb létszámú munkavállalót foglalkoztató vállalatok adatbázisai.

Összességében tehát jelenleg nincs egyértelmű válasz arra, hogy hol húzódik a „kis mennyiség" és a „nagy mennyiség" határa, azonban a kérdés szinte minden szakmai fórumon napirendre kerül, ezért remélhetőleg a követelmény pontos tartalma a közeljövőben tisztul.[25]

Nem csak a személyes adatok mennyisége, de a minősége is növelheti a bekövetkező káresemény súlyosságát, ugyanis a jogalkotó szerint (mennyiségi jelző nélkül) „különleges személyes adat" sérülése esetén a káreseményt már közepes, nagy mennyiség esetén a káresemény nagy. A fogalom tartalma vélhetően ekvivalens a „különleges adat" vagy „személyes adat különleges kategóriája" fogalmakkal, amelyek az alábbiakat foglalják magukban:

- faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok
- genetikai adatok
- természetes személyek egyedi azonosítását célzó biometrikus adatok
- egészségügyi adatok
- természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok

A jelen alfejezet kereteit szétfeszítené a fenti adatok kezelésére (és annak tilalmára) vonatkozó jogi kötelezettségek bemutatása, ezért csak arra hívjuk fel a figyelmet, hogy könnyedén „megbújhat" egy-egy különleges adat (pl. megváltozott munkaképességre vonatkozó adat mint egészségügyi adat) egy szervezet nyilvántartásaiban, amit célszerű figyelembe venni már az elektronikus információs rendszerek tervezésénél, de legkésőbb a biztonsági osztályba sorolásnál.

Végezetül a káresemény súlyosságára értelemszerűen a közvetlen és közvetett anyagi kár és a szervezet nettó árbevételének aránya is hatással van. Főleg kisebb nettó árbevételt realizáló szervezetek esetében lehet első ránézésre különösen megszorító ez a szempont, azonban értelmezésünk szerint a bekövetkező káresemény hatásvizsgálata során figyelembe vehetők a kárenyhítést célzó intézkedések. Így például csökkenthető a bekövetkező kár mértéke egy eszköz esetében vagyonbiztosítással, míg egy nyilvántartás megsemmisüléséből fakadó kár ellen rendszeres és gyakori biztonsági mentésekkel lehet védekezni.

A besorolás nem egyszeri feladat. A rendszerek, folyamatok, fenyegetések és az üzleti környezet folyamatosan változnak, ezért a besorolásokat legalább évente, de nagyobb változás esetén azonnal újra kell értékelni. Fontos, hogy ne essünk sem túlértékelés, sem alábecsülés hibájába. Ha minden rendszer „kritikus", az erőforrásokat túlzottan szétterítjük, ha viszont alulértékelünk egy valóban érzékeny rendszert, akkor kockázatnak tesszük ki magunkat.

25 Magyar Kereskedelmi és Iparkamara (MKIK), „2026/1 A „nagy mennyiségű személyes adat" értelmezése az EIR-ek biztonsági osztályba sorolásánál", https://nis2.mkik.hu/iranymutatasok/1

A biztonsági osztályba sorolás eredménye megalapozza a védelmi intézkedések szintjét, valamint hozzájárul a kockázatok kezelési tervének és az információbiztonsági szabályozás- nak a kialakításához. A cél, hogy a vállalkozás minden EIR-e pontosan annyi figyelmet és védelmet kapjon, amennyit tényleges kockázati szintje indokol – se többet, se kevesebbet.

Ez az arányos megközelítés biztosítja, hogy a biztonság nem gátolja, hanem támogatja a Szervezet hatékony és felelős működését. Fontos hangsúlyozni, hogy a besorolás megfelelőségét az audit során az auditor is vizsgálja. Az SZTFH rendelet alapján az auditor ellenőrzi, hogy a biztonsági osztályba sorolás megfelelően történt-e, valamint hogy rendelkezésre állnak-e a besorolási döntéseket megalapozó bizonyítékok. Emellett azt is vizsgálja, hogy a besorolási döntéseket a szervezet vezetője jóváhagyta-e. A vizsgálat eredménye lehet megfelelő vagy nem megfelelő. Amennyiben az auditor a besorolást nem találja megfelelőnek, javaslatot tesz a helyes biztonsági osztályba sorolásra. Az elektronikus információs rendszerre vonatkozó követelmények teljesülését azonban az auditor a szervezet által megállapított biztonsági osztály figyelembevételével értékeli.

Az Operational Technology (OT) rendszerek esetében a biztonsági osztályba sorolás különös figyelmet igényel. Ezek a rendszerek – például ipari vezérlőrendszerek (ICS, SCADA, DCS) – közvetlenül befolyásolják a fizikai folyamatokat, így meghibásodásuk nemcsak üzleti kiesést, hanem a szervezeten belül nem kezelhető társadalmi-politikai hatása is lehet, pl. környezeti kárt okozhat, kritikus infrastruktúrák megbénulásához vezethet, szélsőséges esetben akár emberéletet is veszélyeztethet. OT környezetben tehát nem elegendő kizárólag az IT szempontokat vizsgálni. – itt a rendelkezésre állás és a biztonságos fizikai működés garantálása elsődleges fontosságú.

Az MK rendelet fenyegetéskatalógusa alkalmazása során különösen figyelembe kell venni az olyan OT-specifikus fenyegetéseket, mint például vezérlőjelek manipulációja, érzékelők és aktuátorok hibás működtetése, karbantartási hozzáférések kihasználása (pl.: USB-ről terjedő malware, távoli hozzáférésre biztosított munkaállomással történő visszaélés), illetve egyes ágazatokban a hálózati leválasztás hiánya (pl.: nem szegmentált OT/IT hálózat).

A biztonsági osztályba sorolás OT környezetben a társadalmi-politikai hatás miatt “magas” szintet eredményezhet, még akkor is, ha az érintett rendszer kevés adatot kezel, de közvetlen hatással van a működésfolytonosságra vagy az emberi biztonságra. A megfelelő szintű fizikai és logikai védelem (pl.: dedikált tűzfalak, fizikai hozzáférés-korlá- tozás, változáskövetés) elengedhetetlen.

6.3 OT rendszerek sajátosságai

A NIS 2 direktíva egységes, európai szintű kiberbiztonsági követelményrendszert állít fel, amely egyszerre érinti a hagyományos informatikai infrastruktúrát és az ipari vezérlőrendszereket. A két környezet közös célja az adatok és folyamatok megóvása, ám a védelem fókuszpontjai, a működési feltételek és a technológiai sajátosságok jelentősen eltérnek. A NIS 2 gyakorlati értelmezése az ipari környezetben külön figyelmet igényel. Az alábbiakban bemutatjuk azokat a konkrét OT-biztonsági kérdéseket, amelyekre a megfelelés során a legnagyobb hangsúly kerül.

Az IT- és az ICS/OT rendszerek biztonságát egyaránt a bizalmasság, a sértetlenség és a rendelkezésre állás hármas (CIA) igénye határozza meg. E három pillér mentén a NIS 2 megköveteli a kockázatalapú védelmi intézkedések kidolgozását, az incidensek gyors bejelentését, a felső vezetői felelősségvállalást és az ellátási láncban rejlő kockázatok kezelését. Szakmai alapvetés

a hálózat szegmentálás, amely az OT világában a Purdue-modell logikai szintjeit követi, biztosítva, hogy az üzleti IT és a gyártási folyamatok között szigorúan ellenőrzött DMZ réteg helyezkedjen el. A hálózat szegmentálás, a többlépcsős hitelesítés, a naplózás, valamint az átvitt adatok titkosítása mindkét területen alapvető védekezési módszer.

Bár az alapelvek megegyeznek, a fő hangsúlyok eltérnek. A vállalati IT-ben az adatok bizalmassága marad az elsődleges, az ICS/OT területen viszont a fizikai folyamatok folyamatos és biztonságos működése élvez előnyt, így a rendelkezésre állás és a sértetlenség kerül az élre. Az informatikai rendszerek általában szabványos hardver- és szoftverkörnyezetben, klimatizált adatközpontokban futnak, ahol a rendszeres frissítés elfogadott gyakorlat. Ezzel szemben az ipari berendezések gyakran zord környezetben, akár több évtizedes életciklussal dolgoznak, ahol a leállások magas termelés kiesést okoznak, ezért a frissítés ütemezése rendkívül körültekintést igényel. Az ipari rendszerek frissítése gyakran üzleti döntés, mivel akár órás leállás is komoly termelési kiesést okozhat – ez különösen jellemző a géppark elöregedése esetén. Olyan kritikus eszközöknél, ahol a patch-elés (frissítés) technikai vagy garanciális okokból nem kivitelezhető, a NIS 2 által elvárt védelmi szintet „Virtual Patching" alkalmazásával – azaz hálózati szintű IPS/IDS szűrőkkel – lehet biztosítani. Egyes ágazatokban a leállás nem is opció és életszerű a "régi" és "új", fejlesztés alatt álló rendszer párhuzamos üzemeltetése.

Technológiai szinten az IT-hálózatok elsősorban TCP/IP-re és modern felhőszolgáltatásokra támaszkodnak. Az ipari hálózatok viszont olyan speciális protokollokat használnak, mint a Modbus, a DNP3 vagy az IEC 61850. Míg az IT-ben az aktív sérülékenység-szkennelés megszokott, az OT-eszközök érzékenysége miatt itt a passzív hálózati forgalom elemzés (DPI – Deep Packet Inspection) alkalmazása javasolt a fenyegetések észlelésére. A valós idejű vezérlés, az alacsony, stabil késleltetés és a szélsőséges környezeti feltételekhez tervezett, úgynevezett rugged eszközök alkalmazása mindennapos követelmény.

Az ICS-architektúrában programozható logikai vezérlők, elosztott irányító rendszerek, távvezérlő egységek és ember-gép interfészek alkotnak egységet. Emellett olyan kiegészítő biztonsági megoldások jelentek meg, mint az Ethernet/IP-hez társított CIP Security vagy az OPC UA beépített hitelesítési és titkosítási mechanizmusai.

A digitális transzformáció következményeként az informatikai és ipari környezetek egyre inkább összefonódnak. Az IIoT-megoldások, a felhőalapú analitika és a prediktív karbantartást támogató mesterséges intelligencia új kapcsolatokat nyitnak a két világ között, ugyanakkor bővülő támadási felületet is teremtenek. Így a kibertámadások már nem csupán adatszivárgást, hanem akár fizikai károkat is okozhatnak.

A NIS 2-nek való megfelelés érdekében elengedhetetlen az IT- és OT-csapatok közötti szoros együttműködés, a közös kockázatértékelési folyamat, valamint az integrált incidenskezelés bevezetése. A vezetőségnek egységes stratégiát kell kialakítania, amely kiterjed a beszállítók értékelésére, az incidensek huszonnégy órán belüli jelentésére és az átfogó megfelelési ellenőrzésekre. A konvergált biztonsági platformok, a felhő-és hálózatvédelmi szolgáltatások integrációja, valamint az OT-specifikus detektálási és válaszmechanizmusok beépítése teszi lehetővé, hogy a szervezetek hatékonyan óvják mind az információs rendszerüket, mind az ipari folyamataikat. Az OT-biztonság nem IT-szabályozás kiterjesztése, hanem a működőképesség biztosításának feltétele. A megfelelés itt nem adminisztratív cél, hanem az üzletmenet megőrzésének eszköze.

A megfelelés során kiemelten fontos az ipari környezet működési sajátosságainak figyelembevétele. Az OT rendszerek esetében gyakori, hogy a gyártógépek nem támogatják

a többfelhasználós működést, így a kezelők közös technikai fiókot használnak. Ez ugyan nem felel meg a klasszikus szerepköralapú hozzáférés-vezérlés követelményeinek, azonban üzemi környezetben – különösen minőségbiztosítási okokból – indokolt lehet az ilyen megoldás megtartása. Ebben az esetben a hozzáférések naplózása, fizikai kontrollok és műszakos beosztás alapján történő azonosítás nyújthat megfelelő kompenzációt.

Hasonló kompromisszum szükséges az automatikus képernyőzárolás esetében is, amely egyes berendezéseknél működés leállást, újraindulást vagy hibát okozhat. Ilyen helyzetekben – az üzem folytonossága érdekében – alternatív kontrollokat kell alkalmazni, például kameraalapú felügyeletet, kezelői jelenlét regisztrálását, vagy a hozzáférési jogosultságok egyéb módon történő ellenőrzését. Az ilyen megoldásokat dokumentált módon kell indokolni, figyelembe véve a sérülékenységek kezelésére irányuló követelményeket.

A beszállítók, technológiai partnerek gyakran távoli eléréssel nyújtanak technikai támogatást. Az ilyen hozzáférések szabályozása kulcsfontosságú: időben korlátozott, naplózott, lehetőség szerint jump szerveren keresztül biztosított elérés javasolt, kétfaktoros hitelesítéssel kiegészítve. Az ideiglenes jogosultságokat minden esetben ellenőrzött módon kell kiadni, és a hozzáférés befejezését követően megszüntetni.

Az OT-rendszerek egy része – például HVAC vezérlés, épületautomatizálás, hozzáférés-ellenőrző rendszerek – nem klasszikus informatikai rendszer, azonban üzletkritikus szerepük miatt az elektronikus információs rendszerek közé sorolandók. A NIS 2-nek és a vonatkozó hazai rendeleteknek való megfelelés érdekében ezeket a rendszereket is be kell vonni a védelmi intézkedések körébe, figyelembe véve az elérhetőségi, rendelkezésre állási és helyreállítási követelményeket.

Az új OT-eszközök integrációja nem csupán műszaki, hanem információbiztonsági kérdés is. Már a telepítés előtt egyeztetni kell az IP- cím kiosztást, VLAN-besorolást, a hozzáférési jogosultságokat, a mentési és naplózási elvárásokat, valamint a tűzfalon való átjárhatóságot. Az új rendszerelemeket az üzembe helyezés előtt ICS-specifikus kockázatértékelésnek kell alávetni, és az EIR-nyilvántartásban isrögzíteni szükséges. A megfelelés egyik záloga az IT és a mérnökségi terület közötti napi szintű együttműködés.

6.4. EIR kiválasztása SEVESO és kritikus infrastruktúrájú üzemeknél

Szabályozási háttér

Az EIR kiválasztása SEVESO[26] és kritikus infrastruktúrájú környezetben komplex folyamat, amely szigorú szabályozási elvárások teljesítését igényli. a kulcstényezők az adekvált biztonsági szint elérése, a jogszabályi előírásoknak való megfelelés biztosítása, valamint a hosszú távú támogathatóság garantálása.

A sikeres implementáció alapja a részletes kockázatelemzés, a megfelelő standardok követése és a proaktív biztonsági intézkedések alkalmazása. a választott rendszernek képesnek kell lennie alkalmazkodni a folyamatosan változó kiberfenyegetési környezethez, miközben biztosítja a kritikus üzleti folyamatok zavartalan működését.

CER irányelv és kritikus szervezetek védelme

A Critical Entities Resilience (CER) irányelv alapján 2024-ben elfogadták a kritikus szervezetek ellenálló képességéről szóló törvényt (Kszetv.). Ez váltotta fel a korábbi létfontosságú rendszerek védelmére vonatkozó szabályozást.

26 ECHA Understanding Seveso

A cél az ellenállóképesség növelése: a kritikus szervezeteknek képesnek kell lenniük megelőzni, kivédeni, kezelni és túlélni minden releváns kockázatot, biztosítva az alapvető szolgáltatások folytonosságát válsághelyzetben is.

6.4.1. SEVESO környezet specifikus követelményei

Biztonsági Irányítási Rendszer (SMS)

A veszélyes üzemeknek Biztonsági Irányítási Rendszerrel kell rendelkezniük, amely kiterjed a technikai, szervezési és személyi intézkedésekre. Az EIR ennek a biztonsági rendszernek a része kell legyen, és meg kell felelnie a jogszabályi követelményeknek.

Kibervédelmi integrációs követelmények

SEVESO üzemekben elvárás a kiberbiztonsági tervek és incidenskezelési eljárások megléte. Az audit során ellenőrzik többek között:

- Tűzfalak, behatolásérzékelők működését,
- Hálózati szegmentáció megvalósítását,
- Hozzáférés-kezelés és naplózás a vezérlőrendszerekben.

Ajánlott minimum biztonsági követelmények beszerzésnél:

- VPN vagy titkosított protokollok támogatása távkommunikációhoz,
- Elkülönített hálózatban való működési képesség internetkapcsolat nélkül,
- Gyártói garancia a rendszer élettartam alatti frissítésére.

6.4.2. EIR kiválasztási folyamat és kritériumok

Regulációk azonosítása és compliance követelmények

Az EIR kiválasztásának elején tisztázni kell az alkalmazandó jogszabályokat:

- SEVESO előírások,
- NIS 2/CER követelmények,
- Ágazati specifikus előírások.

Konkrét követelmények megfogalmazása:

- NIS 2 esetén: naplózás, incidenskezelés, titkosítás,
- SEVESO üzem esetén: SIS integráció támogatása,
- Mérőszámokhoz rendelt standardok (pl.: „IEC 62443 szerinti SL2 szint támogatása”).

Adatvédelem és hozzáférés-kezelés

GDPR kompatibilitás biztosítása:

- Megfelelő adatszegmentálási képesség,
- Jogosultsági szintek implementálása,
- Adathozzáférések naplózása.
- Biztonsági követelmények:
- Nulladik napi (0-day) sérülékenységek elleni védelem,
- Behatolás-észlelési integráció támogatása,
- Végpontvédelmi szoftverekkel való kompatibilitás,
- Kettős hitelesítés (MFA) támogatása – alapkövetelmény kritikus rendszereknél,
- Biztonságos autentikációs protokollok (OAuth2, SAML).

Szabványkövetés és technikai követelmények

- Támogatott életciklusú termékek használata,
- Rendszeres biztonsági frissítések biztosítása,
- Sebezhetőségek kezelési képessége.

Naprakészség és támogatási garancia

Kritikus követelmények:

- Gyártói támogatás az életciklus során,
- Biztonsági patch-ek rendszeres biztosítása,
- Verziófrissítési ütemterv,
- Belső szabályozás a frissítésekre („X napon belül telepíteni kell a kritikus patch-et”).

Kerülendő:

- Elavult szoftverek használata,
- Támogatás nélküli rendszerek,
- Biztonsági frissítések nélküli megoldások.

6.4.3. Gyakorlati implementáció

Kockázatelemzés és védelmi szintek

1. Kiberkockázati elemzés elvégzése a rendszer bevezetése előtt,
2. Megfelelő Security Level (SL) meghatározása,
3. Védelmi intézkedések implementálása a meghatározott szint szerint,
4. Rendszeres felülvizsgálat és frissítés a változó fenyegetések miatt.

Audit és megfelelőség

SEVESO audit során ellenőrzött elemek:

- Kiberkockázati elemzés dokumentálása,
- Védelmi szint megfelelősége,
- Biztonsági vezérlőhálózat konfigurációja,
- Tűzfalak, behatolásdetektálás működése,
- Zárt hálózati működés és hozzáférés-kezelés.

Dokumentációs kötelezettségek

Kötelező dokumentumok EIR választásnál:

- Biztonsági követelmények specifikációja,
- Compliance mátrix a vonatkozó jogszabályokhoz (CER),
- Kockázatelemzési dokumentáció,
- Biztonsági konfigurációs terv,
- Incidenskezelési eljárások,
- Frissítési és karbantartási terv.

07

Nemzetközi kitettség és harmonizáció

A NIS 2 irányelv (EU 2022/2555) célja, hogy egységes és magas szintű kiberbiztonságot biztosítson az Európai Unióban, különösen a határon átnyúló szolgáltatások védelmének erősítésével. Bár az irányelv közös követelményeket rögzít, a tagállami implementációk jelentősen eltérnek mind az alkalmazott technikai és szervezeti kontrollok, mind a bevezetés ütemezése és a megfelelés módja tekintetében. Ez komoly kihívást jelent a több országban működő vállalatcsoportok számára, amelyeknek egyszerre kell megfelelniük a helyi jogszabályoknak és egy összehangolt cégcsoport szintű stratégiát is kialakítaniuk. a nehézségeket tovább fokozzák az eltérő auditmodellek, a beszállítói láncokra vonatkozó követelmények, a változó szektorlisták, valamint a hatósági és piaci kapacitáskülönbségek. Ebben a fejezetben röviden áttekintjük néhány tagállam NIS 2-vel kapcsolatos intézkedéseit és jogszabályi környezetét, rávilágítva a legjelentősebb eltérésekre.

7. Nemzetközi kitettség és harmonizáció

Írták: Pataki Norbert, Szabó Mária Etelka, Dr. Váczi Dániel

7.1. Más EU tagállamok hozzáállása

A fent említett különbségek fényében kiemelten fontos annak feltérképezése, hogy az egyes EU-tagállamok milyen stratégiával, jogi kerettel és gyakorlattal közelítik meg a NIS 2 végrehajtását. a harmonizáció ellenére a tagállamok szabadságot kaptak bizonyos részkérdésekben, így az implementációs részletek lényeges eltéréseket mutatnak, melyek a gyakorlatban befolyásolják a megfelelés tervezhetőségét, költségét és komplexitását.

A tagállamok folyamatosan, különböző ütemben vezetik be a jogrendjükbe a kapcsolódó előírásokat, ezért a bemutatott információk az aktuális állapotot tükrözik. a fejezetben szereplő adatok a 2025. augusztus 1-jei helyzetet rögzítik. Érdemes követni áttekintő térképeket, melyek jellemzően több-kevesebb konkrét linket tartalmaznak. a fejezet lezárásáig az alábbi ábra mutatja be az implementáció helyzetét a tagállamok tekintetében. a zölddel jelzett országok esetében már van hatályos jogszabály, míg a sárgáknál csak tervezetek érhetőek el.

Az alábbiakban néhány olyan ország helyzetét mutatjuk be, ahol már véglegesítették a kapcsolódó törvényeket vagy előrehaladott állapotban van a végrehajtás. Ezek az országok vagy a magyarországi szabályozás szempontjából fontos referenciát jelentenek, vagy azért kerültek kiválasztásra, mert gyakran előfordul, hogy egy hazai szervezet nemzetközi cégcsoport részeként ezekben az államokban is működtet leányvállalatot. a példákban rávilágítunk az eltérő auditmodellekre, megfelelési eszközökre, bejelentési határidőkre, valamint azokra a sajátos értelmezésekre (például EIR fogalma), amelyek az összehangolt csoportszintű működést nehezítik. a fejezet célja nem az országok részletes elemzése, hanem az, hogy kontextust és viszonyítási alapot adjon a magyar megfelelési keretrendszer elhelyezéséhez az európai térben.

7.1.1. Az EU követelményrendszere

Az Európai Unió rendelkezik egy minden tagállamban közvetlenül alkalmazandó rendelettel, amely a NIS 2 irányelv végrehajtását segíti. a (EU) 2024/2690 végrehajtási rendelet technikai és módszertani követelményeket határoz meg, különösen azoknak a digitális infrastruktúra-szolgáltató szervezeteknek, amelyek a NIS 2 hatálya alá tartoznak. Ide tartoznak többek között a DNS-szolgáltatók, TLD domain regisztrátorok, felhőszolgáltatók, adatközpontok, CDN-ek, IT-szolgáltatásokat nyújtó (managed service és security service) vállalatok, valamint az online piacterek, keresőmotorok, közösségi média platformok és bizalmi szolgáltatók. a rendelet minden tagállamban kötelező érvényű, és közvetlenül érvényesíthető az érintett szervezetekre.

7.1.2. Belgium

Belgium az elsők között fogadta el 2024. április 26-án a NIS 2-es törvényt, amely 2024. október 18-án lépett hatályba. a megvalósítást egy hozzá tartozó Royal Decree egészíti ki (2024. június 9.), amely előírja az irányelvek (pl.: CyFun vagy ISO 27001) szerinti megfelelés bizonyítását. Felügyeletét a Centre for Cybersecurity Belgium (CCB) végzi, és megszabja a bejelentési határidőket és nyilvántartási kötelezettséget.

A CyFun egy belsőleg, de nemzetközi normák szerint kidolgozott, kockázatalapú, tanúsítható keretrendszer, amely a NIS 2 elvárások hatékony

teljesítését támogatja. Kombinálja a NIST CSF felépítését, az ISO-27001 tisztaságát, a CIS Controls gyakorlati egyszerűségét és a CMMI érettségi modelljét. EU-s elismerése növekvőben van, és egyre több ország épít rá a saját megfelelőségi modelljében.

7.1.3. Franciaország

Franciaországban a NIS 2-transzpozíciós törvény (a „Loi Résilince", más néven „Resilience Bill") kidolgozása folyamatban van, de a parla-ment 2024. júniusában történt feloszlása miatt már az első fázisban komoly késedelmet szenvedett. A NIS 2 irányelv átültetésére irányuló törvénytervezet azóta több jelentős előrelépést is tett. A szenátus 2025. március 12-én néhány módosítással elfogadta, majd 2025. szeptember 10-én a nemzetgyűlés különbizottsága jóváhagyta. A törvény azonban még nem került véglegesen elfogadásra. A National Cybersecurity Agency of France (ANSSI), mint egyetlen kapcsolattartási pont koordinálja a munkát. Az átültetést szolgáló törvény nemcsak a NIS 2 irányelvet, hanem az Európai Uninó kritikus entitások ellenálló képességéről szóló 2022/2557 számú (CER) irányelvét és a digitális működési ellenálló képességről szóló 2022/2554 számú (DORA) rendeletét is lefedi. A hatókör robbanásszerűen bővült, az eredeti NIS 1 alá tartozó mintegy 500 entitásról több, mint 10 000 entitásra, beleértve a helyi önkormányzatokat és az egyetemeket. A jelenlegi tervek szerint az érintett szervezeteknek 2027. december 31-ig kell teljes mértékben megfelelniük a törvényi előírásoknak.

7.1.4. Szlovákia

A NIS 2 irányelvet Szlovákia a 69/2018 Coll. számú kiberbiztonsági törvény („Act on Cybersecurity") módosításával ültette át, a módosítást tartalmazó Act No. 366/2024 Coll. 2024. november 28-án került jóváhagyásra, hatályba pedig 2025. január 1-jével lépett. Az átültetés gyakorlatilag teljesen megegyezik az eredeti irányelvvel, komoly eltérések nélkül. Szlovákia azonban kihasználva a lehetőséget a helyi közigazgatást is a hatály alá vonta, valamint bizonyos kivételeket is alkalmazott (pl.: nemzeti biztonság, rendvédelmi szervek). a Szlovák National Security Authority az illetékes felügyeleti hatóság (a DSP-k és OES-ek esetén is) és egyben a SPOC ("egyablakos ügyintézési pont") szerepkörét is ő gyakarolja.

7.1.5. Ausztria

Ausztriában a jelenleg is hatályos osztrák Netz- und Informationssystemsicherheitsgesetz (NISG) törvény szabályozza az eredeti NIS irányelvet (EU 2016/1148), de a módosítás (NISG 2024 vagy 2025), amely átültetné a NIS 2-t, nemzeti szinten még nem került elfogadásra. a korábbi tervezetet 2024. július 3-án elutasította a Parlament (Nationalrat), így a jogszabálytervezet hatályba léptetése megtorpant. Igaz az új osztrák kormány 2025. február végi kormányprogramjában vállalta a NIS 2 tényleges beemelését az állami jogrendbe, de a végső elfogadásra és hatálybalépésre valószínűleg csak 2025. második felében kerülhet sor. Az osztrák belügyminisztérium (Bundesministerium für Inneres (BMI)) felelős a végrehajtásért, egységei működtetik az SPOC-ot, valamint a hatósági regisztrációs portált, a kancellária felügyeli a DSP-k és OES-ek szereplői regisztrációját, jelentési kötelezettségeit. a tervezet kulcselemei a kötelező entitás-regisztráció 3 hónapon belül a jogszabály hatályba lépését követően, jelentési kötelezettségek, szankciók, akár 2 % globális árbevételig terjedő bírságokkal, valamint a felelősség általános megerősítése a menedzsment szintjén.

7.1.6. Németország

A NIS 2 hatálybalépését követően a német kormány gyorsan megindította a NIS 2 nemzeti bevezetésének jogalkotási

folyamatát, és a német NIS 2 végrehajtásáról és a kiberbiztonság megerősítéséről szóló törvény (németül: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) első előzetes tervezetét négy hónappal az uniós irányelv hatályba lépése után tette közzé a belügyminisztérium (BMI).

A viszonylag hosszú kidolgozási idő után, Németország immáron törvényi szinten kezeli az EU NIS2-es irányelvét, mivel 2025. december 6. napján hatályba lépett „Gesetz zur Umsetzung der NIS2 Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" címmel.

A törvény értelmében a BSIG (Bundesamt für Sicherheit in der Informationstechnik Gesetz) rendszerében három fő érintetti kört határoz meg: „különösen fontos" (besonders wichtige), „fontos" (wichtige), „szövetségi közigazgatási szervek" (Einrichtungen der Bundesverwaltung). A törvény a 3 fő kategória alá az alábbiakban sorolja be a szervezeteket:

1. „Különösen fontos" (besonders wichtige) szervezetek (pl. kritikus létesítmények üzemeltetői, minősített bizalmi szolgáltatók / TLD registry / DNS-szolgáltatók, bizonyos távközlési szolgáltatók/hálózatüzemeltetők (méretküszöbökkel), valamint az 1. melléklet szerinti szervezettípusokba tartozó nagyobb szervezetek (létszám/árbevétel/mérleg eredmény küszöbökkel).
2. „Fontos" (wichtige) szervezetek (pl. bizalmi szolgáltatók, kisebb küszöbű távközlési szolgáltatók/hálózatüzemeltetők, az 1. és 2. melléklet szerinti szervezettípusokba tartozó, közepes méretű szervezetek.
3. Szövetségi közigazgatási szervek (Einrichtungen der Bundesverwaltung) (szövetségi hatóságok, szövetségi közigazgatás közjogi IT-szolgáltatói, egyéb, meghatározott szövetségi közjogi szervek. Ezekre alapvetően a „különösen fontos" szervezetek szabályai alkalmazandók, de több kivétellel (pl. nem vonatkozik rájuk 61. § felügyeleti audit-elrendelési szabály).

Ellentétben a magyar szabályozással, az auditkötelezettség nem iparág, hatósági érdekkör vagy méret szerint vonatkozik a szervezetekre, hanem a következők alapján:

- ha kritikus létesítmények üzemeltetői (Betreiber kritischer Anlagen), akkor számukra a 39.§ alapján kötelező a megfelelés igazolása biztonsági auditokkal / vizsgálatokkal / tanúsításokkal;
- a „különösen fontos" szervezeteknél a BSI elrendelheti független audit/ellenőrzés/ tanúsítás lefolytatását (§61), de ez nem minden esetben automatikus, hanem felügyeleti intézkedésként alkalmazható;
- a „fontos" szervezeteknél a BSI ellenőrzést/intézkedést akkor alkalmazhat, ha tények alapján valószínűsíthető a kötelezettségek nem megfelelő teljesítése (62.§, 61.§-re visszautalással).

Az auditra kötelezett szervezetek esetében, a 39§ alapján a kritikus létesítmények üzemeltetői felé támasztott fő követelmények is eltérnek a magyar szabályozástól, mert a szervezeteknek csupán igazolniuk kell az 30.§-ban meghatározott általános kockázatkezelési intézkedések, valamint a 31.§ -ban meghatározott kritikus létesítményekre vonatkozó speciális követelmények szerinti intézkedések megvalósítását. Az igazolás történhet biztonsági auditok, vizsgálatok vagy tanúsítások útján. Az auditot a BSI által meghatározott időpontban kell lefolytatni, ami legkorábban 3 évvel azután, hogy először (vagy ismét) kritikus létesítmény üzemeltetőjének minősülnek, majd ezt követően 3 évente.

A fentiekben nagyon röviden összefoglaltakból is már kitűnik, hogy a magyarországi és a németországi megközelítés lényegesen eltér egymástól. Ennek számos oka van, de a leglényegesebb, hogy Németországban 30 éve érvényben van

az ún. IT-Grundschutz. Ez a több száz oldalas anyag, rendszeresen frissített, a BSI (Bundesamt für Sicherheit in der Informationstechnik – Szövetségi Információbiztonsági Hivatal) által kidolgozott információbiztonsági módszertan és követelményrendszer, mely egy gyakorlati "biztonsági alapvédelmi" keretrendszer, ami segít szervezeteknek (állami és piaci szereplőknek is) az információbiztonság strukturált kialakításában, működtetésében és auditálásában.

A német jogszabálytervezet szerint a BSI (Bundesamt für Sicherheit in der Informationstechnik) lesz az illetékes hatóság és a SPOC is. Nemzeti CSIRT-ként a CERT-BUND, a BSI égisze alatt működő kiberbiztonsági incidenskezelő központ van kijelölve, 24/7 elérhetőséggel és felelősséggel incidensek kezelésére. Párhuzamosan a NIS 2 jogszabállyal átültetésre kerül a CER-irányelv (Critical Entities Resilience Directive, EU 2022/2557) is, amelyhez a német jogban a KRITIS-DachG (kritikus infrastruktúra átfogó törvénye) készült el.

7.1.7. Olaszország

Olaszország 2024-ben véglegesítette a NIS 2 irányelv nemzeti jogba történő átültetését a Decreto Legislativo 138/2024 rendelettel, amely 2024. október 16-án lépett hatályba. a rendelet jogi hátterét a 2024. június 28-án elfogadott 90. számú törvény (Legge n. 90/2024) biztosítja, amely általánosabb szabályozási keretet ad az ország kiberbiztonsági rendszerének megerősítéséhez, és szabályozza az informatikai bűncselekményekkel kapcsolatos eljárásokat is. Ez az implementációs modell eltér a legtöbb tagállamétól. Míg más országok jellemzően közvetlenül a NIS 2-t átültető törvényekből vezetnek le részletszabályokat, Olaszországban a NIS 2 előírásai egy szélesebb, nemzeti kiberbiztonsági törvényi környezet „alá" rendelődnek.

Az érintett szervezeteknek egy a NIST Cybersecurity Framework (CSF) alapjaira épülő megfelelőségi követelményrendszernek kell eleget tenniük, amely különösen a kockázatalapú megközelítésre és a biztonsági kontrollok körültekintő kialakítására helyezi a hangsúlyt. a megfelelés és az ellenőrzés felügyeletét az Agenzia per la Cybersicurezza Nazionale (ACN) látja el, amely egyben a nemzeti CSIRT, a kapcsolattartó pont és az EU-CyCLONE funkciók ellátásáért is felelős.

7.1.8. Lettország

Lettország 2024. szeptember 1-jével hatályba léptette a Nacionālās kiberdrošības likums OP 2024/128A.1 törvényt, amely a NIS 2 irányelv nemzeti végrehajtásaként szolgál. a Nemzeti Kibervédelmi Központ (NCSC/CERT.LV) az elsődleges hatóság és kapcsolattartási pont (SPOC), míg a Satversmes aizsardzības birojs (SAB) felelős a kritikus ICT infrastruktúrák felügyeletéért.

Az érintett szervezeteknek nem külső auditot kell lefolytatnia, hanem önértékelési jelentést (self-assessment report) kell benyújtaniuk, amely gyakorlatilag egy strukturált kérdőív kitöltésén alapul. a jelentés tartalmazza, hogy a szervezet mennyiben felel meg a kiberbiztonsági követelményeknek, valamint külön kitér az eltérések magyarázatára. a feladatot minden év október 1-ig kell elvégezniük az érintetteknek.

A fentiekben felsoroltakból kiderül, hogy bár az egyes tagállamok más-más határidőkkel, néhol kisebb fennakadásokkal, de nagyon magas szinten foglalkoznak az információbiztonsággal kapcsolatos szabályozással, a jogszabályi háttér megteremtésével és az érintett szervezetek támogatásával.

7.1.9. Dánia

Dánia a NIS2-t a „NIS 2-loven"-nel (Law on Measures to Ensure a High Level of Cybersecurity, magas szintű kiberbiztonság biztosítását célzó intézkedésekről szóló törvény) ültette át, amely 2025. július 1-jén lépett hatályba.

A kötelező regisztráció határideje 2025. október 1., az incidensbejelentés pedig a Virk

felületen keresztül érhető el (a dán hatóságok által üzemeltetett, vállalkozásoknak szóló hivatalos online ügyintézési portál). A felügyelet ágazati alapon működik (több illetékes hatóság), míg az egységes kapcsolattartó pont / nemzeti CSIRT-funkció a nemzeti kiberhatóságok köré szerveződik (CFCS/CERT).

A nyilvános útmutatókat és munkafolyamatokat aktívan karbantartják (pl. a digitális ágazatban a DIGST). Gyakorlatilag a 2026-os „implementációs munka" nagy része már nem az alapjogszabályok módosításáról szól (mert azok hatályban vannak), hanem a hatókör meghatározásáról és kijelölésről (ideértve a CER irányelvvel való átfedéseket), a irányítás/vezetői felelősség (governance, menedzsment-elszámoltathatóság) erősítéséről, valamint az incidensbejelentési rutinok érettségének növeléséről a több ágazati szabályozó/hatóság mentén.

7.1.10. Bulgária

Bulgária 2026. februárjában fejezte be a NIS2 átültetését a Kiberbiztonsági törvény módosításainak elfogadásával: a módosításokat 2026. február 5-én fogadták el, 2026. február 13-án tették közzé az Állami Közlönyben, és 2026. február 17-től hatályosak.

Egységes kapcsolattartó pontként a State e-Government Agency (állami e-kormányzati ügynökség) van megjelölve, és az új keretrendszer további végrehajtási lépéseket is aktivál (pl. a Minisztertanácsnak frissített stratégiát/rendeletet kell elfogadnia). Gyakorlatilag 2026 márciusa egy korai, „felfutási" szakasz: a kötelezettségek már élesben élnek, nagyon korlátozott átmeneti idővel; a hatóságok még kialakítják a felügyeleti gyakorlatot és az útmutatókat; sok érintett szervezet pedig egyszerre dolgozik a besorolás/kijelölés tisztázásán, valamint az incidensbejelentési és kockázatkezelési kontrollok felállításán, miközben a korai hónapokra hivatkozott, csökkentett szankciókkal járó időablak rövid.

7.2. Csoportosítási elvek: lehetőségek és buktatók

Magyarországon számos olyan szervezet érintett a NIS 2 által, melyek nemzetközi kitettséggel rendelkeznek, legyen az egy külföldi anyavállalattal fennálló nexus vagy egy SaaS típusú EIR használata.

A szervezetek részéről számos esetben felmerül, hogy mi történik akkor, ha egy olyan EIR-t használnak, amely nem áll teljesen a rendelkezési hatókörükben (pl.: az anyavállalat üzemelteti az EIR-t, ami egy nemzetközi entitás. Ilyen esetben a 6.1-ben megfogalmazottakat kell alapul venni, miszerint egy érintett szervezet addig felelős a NIS 2 által megfogalmazott követelmények teljesítéséért amíg a rendelkezési joga fennáll az adott EIR felett.

Tehát ha egy szervezet egy olyan EIR-t használ, amit egy másik entitás üzemeltet és a szervezetnek semmilyen ráhatása nincs az EIR-re, tehát tulajdonképpen "felhasználó" az adott EIR vonatkozásában, akkor ezt az EIR-t ki lehet zárni az audit hatóköréből. Azonban, ha bármi olyan ráhatása van a szervezetnek az EIR-re, ami a NIS 2 követelmények szempontjából értelmezhető (pl.: felhasználókezelés), akkor az audit hatókörét képezi az adott EIR. Ebben az esetben csak azok a kontrollok vizsgálhatók érdemben, melyekre az érintett szervezetnek ráhatása van. Minden más kontroll esetében meg kell indokolni, hogy az adott EIR vonatkozásában miért nincs ráhatása az érintett szervezetnek.

08

A hazai követelmények gyakorlati értelmezése és alkalmazása

A magyar NIS 2-implementáció több egymásra épülő, részletes jogszabályi előírást foglal magában, amelyek nem csupán a megfelelés elméleti kereteit határozzák meg, hanem a gyakorlati megvalósításban is számos kérdést és kihívást vetnek fel. Ez a fejezet átfogó képet ad az érintett szervezetek követelményei szempontjából fontos két rendelet (az MK rendelet és az SZTFH rendelet) tartalmáról és egymáshoz való viszonyáról, majd kitérünk azokra a tipikus megvalósítási nehézségekre, amelyekkel a szervezetek szembesülhetnek a napi működés során. Emellett gyakorlati tanácsokat adunk arra is, hogyan lehet a szabályozási elvárásokat a szervezeti realitásokhoz illeszteni, mikor és hogyan lehet helyettesítő intézkedéseket alkalmazni vagy eltérni a jogszabályban rögzítettektől, illetve milyen módon célszerű a szerződéses megfeleléseket kezelni.

8. A hazai követelmények gyakorlati értelmezése és alkalmazása

Írták: Ács Bálint, Barbul Gergő, Csarnai Gergő, Enyedi Alexandra, dr. Jeney Andrea, Lóth Tamás, Mészáros Csaba, Molnár Ferenc

8.1. 7/2024 vs 1/2025 rendelet összevetése

A két rendelet funkciójában eltérő – míg a 7/2024. (VI. 24.) MK rendelet az EIR-ek felett rendelkező szervezetekre ír elő követelményeket, az 1/2025 (I.31.) SZTFH rendelet főleg az auditorok számára fogalmaz meg iránymutatást, módszertant.

8.1.1. 7/2024. (VI. 24.) MK rendelet

Az MK rendelettel kapcsolatban a társadalmi egyeztetés 2024 január végén indult, az ennek során keletkezett dokumentumok a kormany.hu oldalon a mai napig elérhetők, mint pl.: a jogszabálytervezet Indoklása[27] és Hatásvizsgálati lapja[28]. Ezekből azonban mindössze annyi derül csak ki, hogy a rendelet a NIS 2 végrehajtásához szükséges, illetve, hogy a piaci szereplőkre gyakorolt esetleges hatásvizsgálata nem történt meg. Látható továbbá, hogy a 2024. február 8-ig beérkezett javaslatok alapján[29] a jogalkotó nem látta szükségesnek a rendelet módosítását. Az MK rendelet a whitepaper írásakor hatályos állapotát 2025. január 2-án nyerte el a 18/2024. (XII. 30.) MK rendeletben kihirdetett módosítások átvezetésével[30]. a rendeletet minden olyan szervezetnek alkalmaznia kell, amely a Kiberbiztonsági tv. hatálya alá tartozik.

Az MK rendelet forrásai

Az MK rendelet a NIST 800-53[31] és 800-53B[32] publikációkra épül. Ezek közül az előbbi egy kontroll katalógus, míg az 53B jelzésű az alacsony (low), mérsékelt (moderate) és magas (high) biztonsági szintekre alkalmazandó (továbbá az adatvédelemhez szükséges) kontrollokat határozza meg.

A NIST 800-53 célja, hogy *"átfogó keretrendszert nyújtson biztonsági és adatvédelmi kontrollokhoz olyan (szövetségi) szervezetek és rendszerek számára, amelyek információkat kezelnek. a kiadvány segít ezen szervezeteknek azonosítani a kockázatkezeléshez és a biztonsági követelmények teljesítéséhez szükséges kontrollokat, rugalmas katalógust kínálva, amely alkalmazkodik a változó fenyegetésekhez és technológiákhoz. Célja még ezen felül, hogy közös szókincset alakítson ki, amely megkönnyíti a szervezetek közötti kommunikációt a biztonság, adatvédelem és kockázatkezelés témáiban."*

A 800-53B publikáció *„biztonsági és adatvédelmi intézkedésekre referenciapontokat (baseline) határoz meg szövetségi információs rendszerek és szervezetek számára, valamint útmutatást ad ezen referenciapontok testreszabásához. a kiadvány bármely információt*

27 A miniszteri rendelet tervezete az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács 2022/2555 irányelv (NIS 2 irányelv) végrehajtásához szükséges egyes rendelkezéseket állapítja meg.

28 https://cdn.kormany.hu/uploads/document/3/39/39b/39be5fd49840b90e1e74bbac495db23af33c6bbd.pdf

29 https://cdn.kormany.hu/uploads/document/a/aa/aa3/aa32c78bfe46d772318e0caee9d83fb25cc2f164.pdf

30 MAGYAR KÖZLÖNY • 2024. évi 137. szám

31 Security and Privacy Controls for Information Systems and Organizations

32 Control Baselines for Information Systems and Organizations

kezelő szervezet számára alkalmazható (szövetségi, állami, vagy magánszektor) – azonban a minimális kontrollkészlet alkalmazása kötelező a szövetségi rendszerek esetében. a referenciapontok kiindulópontként szolgálnak, amelyeket a szervezetek küldetésük, az érintettek igényei és a kockázatértékelések alapján testre szabhatnak, hogy teljesítsék a rájuk vonatkozó biztonsági és adatvédelmi követelményeket."

A jogalkotó tehát átvette az USA szövetségi információs rendszereire vonatkozó követelményrendszert és azt, hogy melyik biztonsági osztályhoz mely intézkedéseket kell alkalmazni – mindezt nem csak a közigazgatási ágazathoz tartozó szervezetekre, hanem a gazdálkodó szervezetekre is.

Az MK rendelet felépítése

Az első 3 paragrafus tartalmaz érdemi információt. Amire nem tért ki külön a jogalkotó, az a követelményeknek való megfelelésre vonatkozó határidő, így az elvárás az, hogy a rendelet hatályba lépésekor a szervezetek feleljenek meg az abban foglalt követelményrendszernek. a 2. § (3) bekezdése rendkívül fontos, ennek alapján ugyanis csak azokra az EIR-ekre, EIR komponensekre kell a 2. mellékletben listázott intézkedéseket bevezetni, amelyekre a szervezet rendelkezési joga kiterjed. a rendelkezési jog az adott szervezet döntéshozatali lehetőségeivel függ szorosan össze.

Az MK rendelet mellékletei

Az MK rendeletnek 3 melléklete van, ezek a következők:

- 1. melléklet: (1.) a kockázatmenedzsment keretrendszer (lásd 5. fejezet), (2.) a biztonsági osztályba sorolás (lásd 6.2. fejezet), (3.) Eltérések (lásd 8.6. fejezet), (4.) Helyettesítő védelmi intézkedések (lásd 8.5. fejezet), (5.) Kockázatelemzés és a kockázatok kezelése.
- 2. melléklet – Védelmi intézkedések katalógusa: A katalógus 20 alpontból áll, érdemes lehet elsőként a 20-kal kezdeni, ez ugyanis a katalógus alkalmazási útmutatója és azt kellő részletességgel teszi meg. a NIST 800-53-ban 20 kontroll család található, míg az MK rendeletben csak 19, a különbség a kettő között a „Personally Identifiable Information Processing and Transparency (PT)", vagyis a „Személyes azonosításra alkalmas információk kezelése és átláthatósága" csoporthoz köthető. Ez érthető, hiszen ezt a területet, a GDPR, illetve a 2011. évi CXII. tv. (Info. tv.) szabályozza.
- 3. melléklet – Fenyegetések katalógusa: A katalógus forrása nem egy (vagy több) NIST publikáció, hanem a BSI IT-Grundschutz Compendium[33]. Az ebben a mellékletben listázott 47 fenyegetéshez így részletesebb leírást ebben a dokumentumban lehet találni, amely hozzájárulhat a kockázatmenedzsment keretrendszerrel kapcsolatos feladatok elvégzéséhez. Ne feledjük, hogy a táblázat B oszlopában lévő bizalmasság [B], sértetlenség [S] és rendelkezésre állás [R] információbiztonsági alapelveket a Kiberbiztonsági tv. is definiálta.

8.1.2. 1/2025 (I.31.) SZTFH rendelet

Bár lassan már a múltba vész, a Kibertan tv. alapján eredetileg 2024. év végéig kellett volna a jogszabály hatálya alá tartozó szervezeteknek szerződést kötni egy, az SZTFH által nyilvántartott auditorral. Hiányzott azonban a módszertan az audit díjának kalkulációjára, amely alapján az auditorok árajánlatot adhattak volna a szervezeteknek. a hatóság 2024 karácsony utáni

33 IT-Grundschutz Compendium Edition 2022

közleményében[34] értesítette a nyilvánosságot arról, hogy a vonatkozó szabályozás hiányában szankciót nem fog alkalmazni. 2025 január végén megjelent az SZTFH rendelet, amely, többek között, tartalmazta a kiberbiztonsági audit legmagasabb díjának számítását is, így nem volt több akadály az auditorok és a szervezetek előtt a szerződés megkötésére.

Az SZTFH rendelet célja: *„a kiberbiztonsági követelmények teljesülésének vizsgálatára irányuló kiberbiztonsági audit alapvető szabályainak lefektetése, valamint a kiberbiztonsági audit rendeletben korlátozott díjának meghatározása”.*

A rendelet hatálya azokra a szervezetekre terjed ki, amelyeknek a Kiberbiztonsági tv. 16. § (1) bekezdése alapján kiberbiztonsági auditot kell végeztetniük.

Az SZTFH rendelet forrása

A NIST 800-53A rev.5[35] (a rendelet 5. melléklet 1.1.1. pontja egyértelműen utal is erre), melynek célja, hogy *“útmutatást nyújtson hatékony biztonsági és adatvédelmi értékelési tervek készítéséhez, valamint átfogó eljárásokat biztosítson a rendszerekben és szervezetekben alkalmazott kontrollok hatékonyságának felméréséhez. a kiadvány konzisztensebb és hatékonyabb értékeléseket tesz lehetővé, elősegíti a szervezeti kockázatok jobb megértését, megkönnyíti a költséghatékony kiértékeléseket, és megbízható információkat teremt a kockázatkezelési döntésekhez. a szervezetek testreszabhatják az értékelési eljárásokat olyan tényezők alapján, mint a biztonsági besorolás és kockázatértékelések. Az értékelési folyamat információgyűjtő tevékenység, amely segít azonosítani a biztonsági gyengeségeket, priorizálni a kockázatra adható válaszokat, támogatni a monitoring tevékenységeket, valamint megalapozni az engedélyezési és költségvetési döntéseket.”*

Az SZTFH rendelet felépítése

A rendelet szakaszai rendelkeznek a jogszabály mellékleteinek használatáról, amelyről ez a fejezet részletesebben is ír. Meghatározza azt is, hogy az SZTFH nyilvántartásában[36] szereplő auditorok melyik biztonsági osztály auditálását végezhetik el. Ezeken felül a 6. § (3) bekezdése az auditált szervezet számára kötelezettséget állapít meg a bizonyítékok megőrzésének időtartamára (5 év a lezárás időpontjától számítva).

- 1-2. mellékletek: „Elektronikus információs rendszerek nyilvántartása”, valamint „A szervezetre vonatkozó kérdőív”: A rendelet 3. § (3). pontja alapján ezeket a mellékleteket a szervezeteknek az auditorok rendelkezésére kell bocsátaniuk, ezek alapján tudnak az auditorok árajánlatot adni a szerveteknek. Szintén ezen bekezdés szerint a hatóság egy kitöltési útmutatót elérhetővé tesz majd a honlapján, azonban az a Whitepaper írásáig még nem történt meg.
  Az 1. melléklet kitöltéséhez szükséges az MK rendelet használata is. a táblázat C oszlopa visszamutat az MK rendeletben ismertetett biztonsági osztályokra, a D – F oszlopok pedig a bizalmasság, sértetlenség, rendelkezésre állás hármasra. a táblázat kitöltésekor figyelembe vehető az MK rendelet 3. melléklete is (Fenyegetések katalógusa), így az egyfajta kockázatazonosítási gyakorlatként is szolgálhat.
- 3. melléklet: a kiberbiztonsági audit legmagasabb díja: Az árbevétel alapvetően adottság: nehezen elképzelhető, hogy bármely gazdasági szereplő az audit

34 NIS 2 – 2025-ben kerül sor egy fontos SZTFH rendelet kihirdetésére – Szabályozott Tevékenységek Felügyelet Hatósága

35 Assessing Security and Privacy Controls in Information Systems and Organizations

36 Auditorok – Szabályozott Tevékenységek Felügyelet Hatósága

legmagasabb díjának csökkentése érdekében alacsonyabb nettó árbevételre törekedne. Ennél fontosabb tényezők a legmagasabb biztonsági osztály, valamint az EIR-ek száma. Ezekről ezen whitepaper 6. fejezete ad részletesebb tájékoztatást. A KSH előzetes adatai alapján[37] 2023-ban a középvállalkozások átlag „Értékesítés nettó árbevétele" hozzávetőleg 4.051.936.155 Ft volt, míg a nem KKV körbe tartozó szervezetekre ugyanez az érték 16.022.697.871 Ft volt. a 3. melléklet 1.1 alpontja részletezi, hogy a szervezet előző üzleti évi nettó árbevételének összegét milyen szorzóval kell figyelembe venni.

Az audit díjának kiszámításához az árbevételen túl figyelembe kell venni a szervezet elektronikus információs rendszereinek darabszámát és biztonsági osztályát is, melyekhez a 3. számú melléklet ugyancsak szorzószámokat rendel. Az alábbi táblázat szemlélteti, hogy a KSH 2023-ban mért átlag árbevételi adatai esetén, az EIR darabszám és a biztonsági osztály figyelembevételével és a 3. számú melléklet által meghatározott szorzószámok alkalmazásával az audit díja hogyan alakulna. a jogszabály által előírást szorzószámok a szögletes zárójelen belüli értékek.

- 4. melléklet: Eltérések és helyettesítő védelmi intézkedések nyilvántartása: erről a whitepaper 8.6. fejezete nyújt részletesebb információkat.
- 5. melléklet: Auditori módszertan Erről a témakörről a whitepaper – 10. fejezete szól, egy példát azonban érdemes

37 9.1.1.17. a vállalkozások teljesítménymutatói kis- és középvállalkozási kategória szerint

		Biztonsági osztály		
	EIR darabszám	Alap [1x]	Jelentős [3x]	Magas [5x]
Középvállalkozás	1–5 [1x]	1.925.000	5.775.000	9.625.000
Nem KKV körbe tartozó szervezet		4.812.500	14.437.500	24.062.500
Középvállalkozás	6–15 [2,5x]			
Nem KKV körbe tartozó szervezet		12.031.250	36.093.750	60.156.250
Középvállalkozás	16 vagy annál több [4x]	7.700.000	23.100.000	38.500.000
Nem KKV körbe tartozó szervezet		19.250.000	57.750.000	96.250.000

a két rendelet viszonyát tárgyalva kiemelni. Az SZTFH rendelet 2.2.4.1.3.4. pontjában ismertetett „kritikus mértékű eltérés” jelentős átfedést mutat a tárgyalt MK rendelet 2.2.4. pontjában felsorolt káreseményekkel, mint pl.: személyi sérülés, nemzeti adatvagyon sérülése. Van azonban egy fontos eltérés: míg az MK rendelet a magas biztonsági osztálynál különleges személyes adatokat érintő káreseményre utal a 2.2.4.1. pontban, az SZTFH rendelet a különleges jelző nélkül, így az összes személyes adat bizalmasságának sérülésére utal. Figyelembe véve, hogy az EIR-ek jelentős részében megvalósul valamilyen személyes adat kezelése, legyen az pl.: egy egyedi felhasználói azonosító, így ennek a módszertani elvárásnak a jogszabály szövege szerinti végrehajtása könnyen eredményezhet(ne) kritikus mértékű eltérést, amely gyakorlatilag azonnal egy „nem felel meg” eredményt hozna magával.

- 6. melléklet: Meghatározza a kiberbiztonsági audit során alkalmazandó vizsgálati módszereket, valamint a követelménycsoportok audit eljárás szempontjából lényeges jellemzőit. Ezek közé tartozik, hogy egy adott intézkedéscsoportot szervezeti, vagy EIR szinten kell vizsgálni (B oszlop), a vizsgálati módszereket (C-E oszlopok), az intézkedés típusát (biztosító/támogató), amely megkülönböztetés a védelmi megfelelési index (VMI) számításánál fontos tényező, illetve azt, hogy egy adott követelménycsoport az értékelésből kizárható-e, vagy sem. a kizárt követelménycsoportok az audit során „nem alkalmazható” minősítést kapnak.
- A melléklet táblázatait átgörgetve feltűnhet, hogy egyes sorszámok hiányoznak, mint pl.: az 1.8. (Szervezeti Architektúra – Tehermentesítés), az 1.13. (Belső fenyegetés elleni program) stb. Ezek a kontrollok kiegészítő védelmi intézkedések az MK rendelet szerint („védelmi intézkedések, amelyek esetében a „C” „D” és „E” oszlopok egyaránt „-” jelölést tartalmaznak”) és az SZTFH rendelet, a 800-53A-val ellentétben, ezekre az intézkedésekre nem fogalmaz meg az audit szempontjából lényeges jellemzőket, illetve az értékelésükre vonatkozó instrukciókat a 7. mellékletben.
- 7. melléklet: Az MK rendelet szerinti követelménycsoportok értékelése. a táblázat elemi követelményekre bontja az MK rendelet követelményeit, és teszi mindezt rendkívül aprólékosan – lásd az alábbi táblázatokban. Nem tartalmazza azonban a biztonsági osztályokat, amelyekhez az adott intézkedések bevezetése az MK rendelet szerint elvárt. Javasolt az alap, illetve jelentős biztonsági osztályba sorolt szervezeteknek a két rendelet összevetése ebből a szempontból, így a szervezetek rendelkezésére állnak mind a követelmények, mind a követelmények megvalósulásának ellenőrzésére vonatkozó kérdések.
- 8. melléklet: Az auditjelentés tartalma. a melléklet címzettjei az auditorok. Az SZTFH rendelet 5. §-ában meghatározott, az auditjelentésre vonatkozó követelményeket pontosítja. a jelentést megkapja egyrészt az auditált szervezet nyomtatható, valamint az SZTFH gépi feldolgozást lehetővé tévő formátumban.

A rendeletek (és forrásaik) kapcsolata

MK rendelet	NIST 800-53
2.1. a szervezet: 2.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint	AC-1 POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
2.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó hozzáférés-felügyeleti szabályzatot, amely	1. [Selection (one or more): Organization-level; Mission/business process-level; System level] access control policy that:
2.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

SZTFH rendelet	NIST 800-53A
2.1. Szabályzat és eljárásrendek K02.001_P[1] meghatározott azon személyek vagy szerepkörök listája, akikkel meg kell ismertetni a hozzáférés-felügyeleti szabályzatot	AC-01 POLICY AND PROCEDURES ASSESSMENT OBJECTIVE: Determine if: AC-01_ODP[01] personnel or roles to whom the access control policy is to be disseminated is/are defined;
K02.001_P[2] meghatározott, hogy a hozzáférés-felügyeleti szabályzat szervezeti, folyamat- vagy rendszerszintű	AC-01_ODP[02] personnel or roles to whom the access control procedures are to be disseminated is/are defined;
K02.001_O.2.1.1.(a) a K02.001_P[2] szintű hozzáférés-felügyeleti szabályzatot a szervezet kidolgozta és dokumentálta	AC-01a.[01] an access control policy is developed and documented;
K02.001_O.2.1.1.(b) a hozzáférés-felügyeleti szabályzatot a szervezet kiadta K02.001_O.2.1.1.(c) a hozzáférés-felügyeleti szabályzatot a szervezet a K02.001_P[1] szerinti személyekkel vagy szerepkörökkel megismertette	AC-01a.[02] the access control policy is disseminated to <AC-01_ODP[01] personnel or roles>;
K02.001_O.2.1.1.1.1.(a) a hozzáférés-felügyeleti szabályzat meghatározza a célkitűzéseket	AC-01a.01(a)[01] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses purpose;
K02.001_O.2.1.1.1.1.(b) a hozzáférés-felügyeleti szabályzat hatálya meghatározásra került	AC-01a.01(a)[02] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses scope;

SZTFH rendelet	NIST 800-53A
K02.001_O.2.1.1.1.1.(c) a hozzáférés-felügyeleti szabályzat meghatározza a szerepköröket	AC-01a.01(a)[03] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses roles;
... és itt következne még az MK rendelet 2.1.1.1.1. pontja alapján a "felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat" , tehát K02.001_O.2.1.1.1.1.(a)-tól (g)-ig	
K02.001_O.2.1.1.1.2 a hozzáférés-felügyeleti szabályzat összhangban van a szervezetre vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal	AC-01a.01(b) the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines

"P" és "O" típusú elemi követelmények

A NIST 800-53-ban "organization-defined parameters (ODPs)"-ként hivatkoznak ezekre a szervezeti döntésektől függő változókra. Az SZTFH rendeletben hivatkozási kódjában "P" betű található.

Jellemzően az az MK rendelet követelmény elem, amiben megtalálható a "meghatározza", "meghatározott" kifejezés, az az SZTFH rendeletben egy paraméterként jelenik meg, amelynél mind a konkrét paraméter meghatározása, mind a paraméter szerinti tevékenység teljesülése auditálandó. Az MK rendelet 2.1.1.1., illetve a többi x.1.1.1., követelmény megfogalmazása alapján úgy tűnhet, hogy "szervezeti-, folyamat és rendszerszintű követelményeket" is kell a szabályzatoknak tartalmaznia, míg a 800-53, 800-53A és SZTFH rendeletek ezt inkább választási/döntési lehetőségként jelenítik meg.

Ahogy az a 2.1.1.1.1. -es követelmény elemnél ("meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat") és a hozzá kapcsolódó SZTFH K02.001_O.2.1.1.1.1.(a) – (g) -ig elemi követelményeknél látható, minden egyes elem, ami az MK rendelet felsorolásában megjelenik, egy külön sorszámmal ellátott, auditálandó intézkedés.

Apró eltérés(ek) a rendeletek között

A rendeletek, mivel a forrásként szolgáló NIST publikációk is, meglehetősen terebélyesek, így előfordulhatnak kisebb eltérések a két rendelet között. Példa erre a K05.001_P[1] és K05.001_P[2] paraméterek, amelyek a naplózásra és elszámoltathatóságra vonatkozó szabályzatra, illetve eljárásrendre mutatnak, holott az 5. intézkedés-csoport az "Értékelés, engedélyezés és monitorozás".

Hasznos források

Nemzeti Kiberbiztonsági Intézet Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója[38], valamint az ezen oldalon elérhető[39], amely magyarázatot, megvalósítási lépéseket és további hasznos információkat tartalmaz.

38 Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója – Nemzeti Kiberbiztonsági Intézet

39 Védelmi intézkedések katalógusa táblázat (ver. 1.0) letöltése

8.2. Gyakorlati megvalósítási tippek magas erőforrásigény mellett

A NIS 2 irányelv gyakorlati bevezetése nem csupán megfelelőségi kérdés, hanem komplex szervezeti és projektmenedzsment kihívás is. Különösen kritikus ez olyan intézményeknél, ahol az IT-biztonsági, compliance és jogi kapacitások korlátozottak. Az alábbi intézkedések és módszerek segítenek abban, hogy a megfelelést stratégiai prioritások mentén, fokozatosan és hatékonyan valósítsuk meg.

Prioritás-alapú bevezetés

Alakítsunk ki egy egyszerű, üzleti kockázatokon alapuló prioritási mátrixot, amely figyelembe veszi:

- az üzleti folyamatra gyakorolt hatást (kockázat),
- a megfelelőségi hiányosság súlyosságát,
- a megvalósítás becsült költségét és időigényét,
- a rendelkezésre álló szervezeti erőforrásokat.

Egy jól strukturált mátrix lehetővé teszi, hogy először a legnagyobb kockázatot jelentő és legalacsonyabb erőforrásigényű területeken kezdjük meg a munkát. a fázisolt, iteratív megközelítés csökkenti a párhuzamos terhelést és javítja az átláthatóságot.

Kis, fókuszált projektcsapat

Alakítsunk ki egy multidiszciplináris projektcsapatot az IT, információbiztonság, jogi, HR és üzleti területek képviselőiből. Az együttműködés sikeressége érdekében alkalmazzunk:

- RACI mátrixot a feladatkiosztáshoz,
- projekt chartert a célok és elvárások rögzítésére,
- rendszeres rövid státuszmegbeszéléseket a követéshez.

Egy jól szervezett, kis méretű csapat képes gyors döntésekre és minimális adminisztratív terhelés mellett képes reagálni a változó körülményekre.

Automatizálás, ahol csak lehet

A humánerőforrás-igény csökkentése érdekében a rutinfolyamatokat automatizálni szükséges. Javasolt területek:

- Naplózás és eseménykezelés: SIEM rendszerek, naplófájlok automatikus gyűjtése és elemzése.
- Hozzáféréskezelés: IAM vagy PAM eszközök használata a jogosultságok kezelésére.
- Képzés és tudatosság: e-learning platform integrálása, auditált részvétellel.

További lehetőségek: verziókövetés automatizálása, megfelelőségi riportok előállítása, frissítési emlékeztetők beépítése.

Agilis projektmenedzsment szemlélet

A hagyományos vízesésmodelltől eltérően a NIS 2-megfelelőség bevezetése során agilis, sprintalapú működés javasolt, különösen változó követelmények és korlátozott kapacitások esetén:

- Rövid, 1–2 hetes iterációk (sprint),
- Felhasználói történetek (user stories) a teendők leírásához,
- Rendszeres retrospektív megbeszélések, melyek segítik a tanulságok levonását,
- Demo fázisok a részmegvalósítások validálására.

Ez a módszertan növeli a reakcióképességet és elősegíti a fokozatos érést.

Külső erőforrások bevonása célzottan

Amennyiben belső kompetenciahiány tapasztalható, célszerű külső tanácsadók vagy szolgáltatók bevonása az alábbi területeken:

- Kockázatelemzés és osztályba sorolás,
- Szabályzatkészítés és belső eljárásrendek,
- Technikai biztonsági értékelések (pl.: penetration tesztek, belső auditok),
- Üzletmenet-folytonosság és incenskezelés.

A szerződéses feltételek kidolgozásánál ügyeljünk arra, hogy azok tartalmazzák a NIS 2-kompatibilis elvárásokat (pl.: SLA-k, adatbiztonság, minőségbiztosítási mechanizmusok).

+1. Tudatos kommunikáció és vezetői támogatás

A NIS 2-megfelelés szervezeti szintű kihívás, így elengedhetetlen a felsővezetés aktív támogatása és elkötelezettsége. Ennek része:

- stratégiai célkitűzések kommunikálása,
- rendszeres tájékoztatók a projekt állapotáról,
- döntési támogatás nyújtása a szűk keresztmetszetek feloldásához.

8.3. Szerződések kiegészítési javaslatai

A NIS 2 irányelv alapvető célkitűzése a kulcsfontosságú ágazatokban a kiberreziliencia fokozása, a fenyegetések mérséklése és a kiberbiztonsági képességek javítása. Ez az érintett szervezetek számára új jogi kötelezettségeket ír elő, amely a meglévő szerződések újragondolását, kiegészítését teszi szükségessé.

A fennálló szerződéseket ezért célszerű átfogó jogi szempontú vizsgálat alá vonni, figyelemmel a NIS 2 irányelv, a Kiberbiztonsági tv., és végrehajtás tárgyában kiadott Kormányrendelet, valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló MK rendelet vonatkozó rendelkezései alapján.

A felek között többfajta fennálló szerződés lehet (SLA megállapodás, SaaS, IT üzemeltetési megállapodás), melyek rendelkezései iparáganként, és szolgáltatásonként sokfélék lehetnek. Az alábbiakban néhány javaslat található módosító szerződéses rendelkezésekre, melyektől a szerződés jellegétől függően szabadon el lehet térni, azonban néhány gondolat sorvezetőként szolgálhat a szerződéses tartalom újragondolása során:

Alvállalkozók

Ellátási lánc biztonsága érdekében a szervezettel alvállalkozói jogviszonyban lévő jogalanyok tekintetében a NIS 2 előírások teljesítését elő kell írni, az alábbiak szerint:

„Új alvállalkozó bevonására csak a Megrendelő előzetes, írásbeli engedélye alapján kerülhet sor. Alvállalkozó kötelezi magát arra, hogy a NIS 2 irányelv rendelkezéseinek maga is megfelel, az EIR-jei felmérését, valamint biztonsági osztályba sorolását elvégzi, és a biztonsági osztály szerinti védelmi intézkedések megtételét teljesíti. Ezen kötelezettségét dokumentációval igazolja a Megrendelő felé legkésőbb az első kiberbiztonsági audit időpontját megelőző egy hónappal."

Incidenskezelés

A NIS 2 a kiberbiztonsági incidenskezelés tekintetében szigorú határidőket ír elő (bejelentési és jelentéstételi kötelezettség).

„Szerződő fél köteles az információbiztonsági rendszereit monitorozni, a rendszer logadatokat megvizsgálni és a logok biztonságos tárolásáról gondoskodni. Köteles továbbá az EIR-ek tekintetében általa észlelt minden információbiztonsági eseményről rendelkezésre álló információt haladéktalanul, de legkésőbb az észleléstől számított X órán beleül átadni a Megrendelőnek, annak érdekében, hogy az illetékes hatóságok

felé a bejelentést eszközölhesse. Köteles továbbá az érintett logokat Megrendelő részére átadni további vizsgálat érdekében, és a vizsgálat lefolytatása során a Megrendelővel együttműködni."

Dokumentumok összehangolása

A NIS 2 számos már elkészült, hatályban lévő dokumentumot érint, ezért ezek összehangolása nem mellőzhető. (IBSZ, Incidenskezelési Szabályzat, szükség esetén Adatkezelési és Adatbiztonsági Szabályzat, Hozzáféréskezelési Szabályzat, IB stratégia, IB politika stb.)

„Szerződő fél kötelezi magát, hogy valamenynyi, NIS 2 által érintett dokumentumát jogi megfelelőségvizsgálatnak veti alá, és a vizsgálat eredményeként az érintett dokumentumokat legkésőbb .....-ig módosítja, és a módosításokat a Megrendelő számára hozzáférhetővé teszi."

Felelősségi kérdések

Az esetleges kiberbiztonsági incidensek kezelésére minden esetben célszerű biztosítást kötni, amely egyebekben jogszabályi kötelezettség is. a szerződésben ki kell kötni a kártérítési felelősség és annak áthárításának körét, valamint az összeghatárt, és a biztosítási szerződés fenntartásának kötelezettségét.

„Szerződő fél kötelezi magát, hogy valamenynyi kiberbiztonsági eseményből származó kár viselése érdekében felelősségbiztosítást köt. a biztosítási kötvényt a Megrendelő rendelkezésére bocsátja, legkésőbb a Megrendelő első kiberbiztonsági auditját megelőző egy hónapon belül. a biztosított összeghatár megállapítása során figyelembe kell venni az áthárított tevékenység jellegét és a lehetséges kockázatokat. Ennek megállapítása érdekében a szerződő fél kockázatértékelést köteles végezni. Szerződő fél köteles a megkötött biztosítási szerződést a Megrendelő kiberbiztonsági auditját követően is fenntartani. Amennyiben a biztosítási szerződés feltételeiben változás következne be, erről a szerződő fél köteles haladéktalanul értesíteni a Megrendelőt."

Biztonságtudatosság, képzés

A biztonságtudatosság növelése a NIS 2 fontos célkitűzése, ez azonban csak akkor lehet hatékony, ha minden szerződő partner munkavállalói tisztában vannak a szervezetükre, munkakörükre irányadó információbiztonsági szabályokkal és azokat be is tartják. Ezért a kötelező képzést és a számonkérést minden esetben elő kell írni.

„Szerződő fél köteles évente szerepkör szerinti, rendszeres biztonságtudatosság oktatást tartani az általa irányított szervezet munkavállalói részére. Az oktatást számonkérés követi. Az ezzel kapcsolatos dokumentumokat (jelentléti ív, vizsgalapok) szerződő fél köteles a Megrendelő rendelkezésére bocsátani legkésőbb a Megrendelő első kiberbiztonsági auditját megelőző egy hónapon belül."

Együttműködési kötelezettség

A felek együttműködése kulcsfontosságú, ugyanis ennek hiányában a NIS 2 kötelezett nem tud eleget tenni az audit megfelelési kritériumoknak, ezért az együttműködési kötelezettséget expressis verbis ki kell mondani.

„Felek kötelesek a Megrendelő kiberbiztonsági auditjának sikeressége érdekében egymással együttműködni. Az együttműködés különösen az információbiztonsági és audit kritériumok teljesítésére terjed ki. Amennyiben a felek közül bárki ezen együttműködési kötelezettségét elmulasztja, e kötelezettségszegés súlyos szerződésnek minősül, és a felek közötti szerződés felmondását alapozza meg. a felmondás gyakorlásának nem feltétele a Megrendelővel szembeni bírság vagy hatósági intézkedés alkalmazása."

Jogszabályváltozások

Feleknek közösen vállalni kell, hogy jogszabály módosítás esetén további egyeztetéseket eszközölnek, és a fennálló szerződésüket ezek

tükrében módosítják. Ez a sikeres audit feltétele, hiszen az auditorok dokumentum szintű ellenőrzést is végeznek, ezért a dokumentumok naprakészsége elengedhetetlen.

„Felek kötelezik magukat, hogy esetleges jogszabályváltozás esetén egymással egyeztetnek, és szükség esetén a fennálló szerződésüket a jogszabályváltozás tükrében közösen módosítják."

IBF kijelölése

Lényeges, hogy az érintett felek információbiztonsági felelősei egymással rendszeres kapcsolatban álljanak, és szükség esetén egyeztessenek a teendő intézkedésekről.

„Felek külön kapcsolattartói pontot jelölnek ki X cég részéről ....., Y cég részéről..... személyében Az érintettek kötelesek egymással rendszeres időközönként egyeztetni, és megtett információbiztonsági intézkedéseikről egymást tájékoztatni, valamint intézkedéseiket a tájékoztatás ismeretében összehangolni."

Rendszeres kockázatértékelés

Felek kötelesek az EIR-ekkel kapcsolatos információs vagyonleltárt és az ehhez tartozó kockázatértékelést rendszeres időközönként frissíteni. Ez azért lényeges, mert a megváltozott körülmények más védelmi intézkedéseket tesznek indokolttá, ezt pedig csak időszakos felülvizsgálat, monitoring tudja biztosítani.

„Felek kötelesek az EIR-jeikhez kapcsolódó információs vagyonleltárt és kockázatértékelést évente felülvizsgálni és szükség esetén frissíteni. a naprakész vagyonleltár és kockázatértékelés alapján felek a megtett védelmi intézkedéseiket módosítják, illetve átértékelik."

A fenti szerződéses módosítások nemcsak a jogszabályi megfelelést, hanem a felek közötti bizalom fenntartását és a működési kockázatok minimalizálását is szolgálják. a szerződéses partnerek közös felelőssége ugyanis az, hogy a digitalizált környezetben a szolgáltatások folytonossága és a kritikus rendszerek védelme biztosított legyen, és az ehhez kapcsolódó jogi garanciák átláthatóak, számonkérhetőek legyenek.

A 2025-2026 év tapasztalatai

Az utóbbi 1-1,5 év tapasztalata, hogy a beszállítói kockázatértékeléssel kapcsolatos szerződéses rendelkezések kiemelt hangsúlyt kaptak. Itt kell megemlíteni a beszállítók monitoringját, auditálhatóságát, valamint szabályozott incidenskezelés fontosságát. Leggyakoribb szerződéses trendek az alábbiak:

- Beszállítói minimumkövetelmények meghatározása;
- Kötelező security policy alignment;
- Sub-supplier kontrollok;
- Beszállítói kockázati besorolás.

"A szerződő fél köteles biztosítani, hogy a szolgáltatás teljesítése során résztvevő beszállítók és alvállalkozók a jelen szerződésben előírt minimum információbiztonsági követelményeknek megfelelnek. A szerződő fél felel azért, hogy az alvállalkozók szerződéses kötelezettségei teljesítésével elősegítsék a megrendelő NIS 2-nek történő megfelelést."

Az auditálhatóság biztosításával a hatékony ellenőrzés keretei alakíthatók ki. Ehhez kapcsolódóan az audit jogok erősítése, az audit evidenciák kötelező szolgáltatása és a dokumentációhoz történő hozzáférés a legfontosabbak. Mindezek értelmében az audit bizonyítékok átadása és fokozott együttműködési kötelezettség immár gyakran szerződéses kötelező kritérium.

A szerződésekben megjelentek a konkrét biztonsági követelmények kötelezőként történő előírása is, úgy mint:

- Patch management;
- Sérülékenységvizsgálat;
- Logolás.

Ezek részletességének meghatározása szervezet és szolgáltatás függő.

"A szerződő fél köteles saját információbiztonsági rendszere tekintetében meghatározott időközönként az alábbi intézkedéseket teljesíteni:

Köteles a megrendelő által előírtak szerint évente patch management-et és sérülékenységvizsgálatot végezni, valamint a rendszer logadatokat ..... megőrizni és kiberbiztonsági incidens esetén a megrendelő rendelkezésére bocsátani."

Tekintettel arra, hogy a szerződő fél meg nem felelése közvetlenül veszélyeztetheti a megrendelő NIS 2 megfelelését is, így javasolt szankciós rendelkezések szerződésbe emelése is, a beszállítói lánc egységes védelmi rendszerének biztosítása érdekében.

„Amennyiben a szerződő fél súlyosan vagy ismételten megsérti a jelen szerződésben meghatározott információbiztonsági kötelezettségeit, és a megrendelő írásbeli felszólítása ellenére a jogsértést ésszerű határidőn belül nem orvosolja, a megrendelő jogosult a szerződést azonnali hatállyal felmondani."

A szolgáltatás jellegére tekintettel javasolt külön Kiberbiztonsági melléklet készítése, melynek az egyes szolgáltatás specifikus információbiztonsági kritériumok is felsorolásra kerülhetnek.

8.4. Meg kell-e felelni minden pontnak?

A megfelelés eléréséhez számos védelmi követelményponttal találkozhatunk, melyek a NIST 800-53 revision 5 nemzetközi szabványon alapulnak. Az EIR-ek biztonsági osztályba sorolása meghatározza, hogy hány követelménynek kell megfelelni.

Az érintett szervezetek különböző érettségi szinten vannak – különböző szintről indulnak a felkészülés megkezdésekor. Ezt figyelembe véve a Kiberbiztonsági tv. annyiban megengedő, hogy a szervezetek kockázatalapú megközelítést alkalmazhatnak. Mit is jelent ez? Minden cégnek fel kell mérnie a saját elektronikus információs rendszerének a biztonsági érettségi szintjét, biztonsági osztályba kell őket sorolnia – GAP elemzés elvégzésével és kockázatelemzést kell végeznie. a kockázatok meghatározása után tudja megmondani, hogy azokat milyen megoldásokkal tudja csökkenteni és ezek megtalálhatóak-e a védelmi intézkedések katalógusában. Amennyiben az nem tartalmaz eredményesen és kockázatarányosan alkalmazható intézkedést akkor helyettesítő védelmi intézkedést határozhat meg a kérdéses/hiányos kontrollok helyett. Erről nyilvántartást is kell készíteni melyet a menedzsmenttel jóvá kell hagyatni. Ehhez, az SZTFH rendelet 4. melléklete szolgál sablonként. Ezt a nyilvántartást az auditor cégek kérik az audit szerződés megkötésekor (vagy aláírása után 15 napon belül).

A helyettesítő intézkedéseket dokumentálni kell, majd az audit során evidenciákat kell bemutatni a működésükről.

8.5. A megfelelés túl- vagy alulteljesítésének kockázatai

A NIS 2 egyik fő követelménye a megfelelés biztosítása. Bár ez a folyamat kötelező, fontos megérteni, hogy mind a hiányos megfelelés (alulteljesítés), mind a túlzott megfelelés (túlteljesítés) komoly kockázatokat rejt. a cél egy arányos és ésszerű megközelítés.

Alulteljesítés kockázatai: a nem megfelelés ára

A NIS 2 követelményeinek be nem tartása azonnali és súlyos következményekkel járhat. Ide tartoznak a jelentős pénzbírságok (akár az éves árbevétel 2%-a), a különböző, tevékenységre vonatkozó korlátozások, vagy akár a tevékenységtől való eltiltás is. Működési szempontból megnő a kiberbiztonsági incidensek

(adatszivárgás, szolgáltatáskiesés) kockázata, ami reputációs károkat és az üzletmenet folytonosságának megszakadását okozhatja. Mindez jelentős pénzügyi terhekkel jár a helyreállítás és bevételkiesés miatt.

Túlteljesítés kockázatai: az „aranyozott ketrec”

Meglepő módon a túlteljesítés, azaz a túlzott megfelelés is hordoz magában kockázatokat, elsősorban erőforrás-pazarlás formájában. Felesleges kiadásokba verheti magát a szervezet a túlzott technológiai beruházásokkal, fölösleges szoftverek és hardverek beszerzésével. a NIS 2 megfelelést kínáló „dobozos” termékek bár segíthetik a megfelelés kialakítását és bizonyítását, önmagában egyetlen szoftver sem jelent garanciát a megfeleléshez. Mindezek mellett a humánerőforrás is túlterheltté válhat, ha túl sok munkaórát és szakembert kötnek le a felesleges feladatok, elvonva őket a stratégiai fontosságú területektől (vagy akár csak a napi – bevételt jelentő – feladatoktól). a túlzott bürokratikus terhek, mint a felesleges dokumentáció és a bonyolult folyamatok, szintén hozzájárulnak ehhez.

Működési hatékonyságcsökkenés is felléphet, mivel a túl sok ellenőrzési pont és adminisztráció lassíthatja az üzleti folyamatokat, gátolhatja az innovációt és az amúgy is divatos agilis működést. a túlzott kontroll és a felesleges feladatok akár az alkalmazotti elégedettséget is ronthatják. Versenypiaci hátrányt is eredményezhet a túlteljesítés, hiszen a többletköltségek rontják a versenyképességet, és a bonyolult biztonsági folyamatok rontják az ügyfélélményt. Végül, a fókusz elveszhet a kritikus területekről, ha a hangsúly kevésbé releváns, de „könnyen kipipálható” feladatokra tevődik át.

Az optimális megoldás: ésszerű és arányos megközelítés

A kockázatok minimalizálása érdekében elengedhetetlen a kockázat alapú megközelítés. Ez azt jelenti, hogy azonosítani kell a legkritikusabb területeket és folyamatokat, figyelembe véve az üzleti hatáselemzés (BIA) és az adatvagyon-felmérés eredményeit. a NIS 2 követelmények értelmezése és a szervezet méretének, komplexitásának megfelelő, testreszabott megoldások alkalmazása nélkülözhetetlen. a folyamatos felülvizsgálat és adaptáció biztosítja, hogy az intézkedések hatékonyak maradjanak a mindenkor változó környezetben. a vezetői elkötelezettség és a munkavállalók képzése szintén alapvető a sikeres megfeleléshez.

8.6. Helyettesítő védelmi intézkedések lehetőségei

A biztonsági osztályba sorolás alapján előírt védelmi intézkedések célja, hogy minden nyilvántartásba került EIR azonosítható és mérhető védelmi szinttel rendelkezzen. Ugyanakkor a gyakorlati megvalósítás során előfordulhat, hogy egy adott szervezet – akár technológiai korlátok, akár üzleti működési sajátosságok miatt – nem tud egy az egyben megfelelni minden előírt kontrollnak. Ilyenkor nyílik lehetőség jól dokumentált helyettesítő védelmi intézkedések alkalmazására, de kizárólag akkor, ha azok egyértelműen biztosítják az eredeti intézkedés céljának teljesülését.

Ez különösen fontos lehet olyan környezetekben, ahol az informatika (IT) és az ipari technológia (OT) együtt, ám egymástól eltérő működési logika mentén van jelen. Egy hagyományos IT rendszernél például egy biztonsági funkció szoftveres úton is megvalósítható, míg OT rendszerek esetén ugyanez csak fizikai hozzáférés-szabályozással vagy működési protokollok átszervezésével biztosítható. Lényeg, hogy az alternatív megoldás ne csak formai megfelelőséget

tükrözzön, hanem ténylegesen képes legyen csökkenteni a kockázatot, amire az eredeti kontroll irányult.

A helyettesítő intézkedések alkalmazása nem csak jog, hanem felelősség. Minden esetben kockázatalapú értékelésen, dokumentáción és felső vezetői jóváhagyáson kell alapulnia. a megfelelőséget nem a módszer, hanem az eredmény bizonyítja. Az audit során nem azt vizsgálják, hogy egy kontroll betű szerint teljesült-e, hanem azt, hogy a vizsgált szervezet képes volt-e az adott kockázatot igazoltan csökkenteni. Ebben segít az SZTFH rendelet 4. melléklete által előírt nyilvántartási sablon is, amely a szervezet és az auditor számára is átláthatóvá teszi a döntéseket és azok hátterét.

8.7. Eltérési lehetőségek kezelése

Az EIR-ek védelmi intézkedéseinek gyakorlati alkalmazása során a szervezetek számára lehetőség nyílik bizonyos eltérések engedélyezésére, amennyiben azok dokumentáltan és megalapozott módon biztosítják a rendszerrel szembeni biztonsági követelmények teljesülését. Az eltérések kezelése nem a megfelelőség megkerülését, hanem a kockázatalapú, adaptív védelem érvényesítését jelenti. a megfelelően dokumentált eltérés segíti a rugalmasságot, fenntarthatóságot és az erőforrások optimális felhasználását.

Egyedi eltérések típusai (kontrollszintű megközelítésben)

A védelmi intézkedések (kontrollok) alkalmazása során bizonyos esetekben a szervezet – dokumentált kockázatelemzés és megfelelő indokolás alapján – eltérhet egy-egy konkrét kontroll végrehajtásától. Az alábbiakban bemutatott típusok segítenek rendszerezni a gyakori eltérési helyzeteket.

- Kontroll nem releváns a működési környezetben:
  Amikor egy kontroll (pl.: vezeték nélküli hálózat titkosítása) nem alkalmazható, mert a rendszer egyáltalán nem tartalmaz vezeték nélküli kapcsolatot, az intézkedésre nincs szükség. Ebben az esetben a szervezet dokumentálja a kontroll inaktivitását azzal az indokkal, hogy az érintett technológia hiányzik a működési környezetből.
- Kontroll már meglévő más mechanizmussal biztosított:
  Bizonyos esetekben az előírt kontroll célját egy másik meglévő intézkedés már teljesíti. Például: ha a fizikai hozzáférés-ellenőrzést nem beléptetőrendszerrel, hanem állandó őrszolgálattal és kulcskezeléssel biztosítják, és az megfelel a kockázati szintnek. Az eltérés indoka: funkcionálisan egyenértékű alternatíva használata.
- Kontroll nem alkalmazható jogi vagy szervezeti okból:
  Előfordulhat, hogy egy kontroll nem alkalmazható adatvédelmi vagy munkaügyi szabályozás miatt. Ebben az esetben a szervezet az eltérést szabályozási megfelelésre hivatkozva dokumentálja, és az adatvédelmi kockázatok mérséklésére más intézkedést vezet be.
- Kontroll bevezetése csak fokozatosan lehetséges:
  Egy adott kontroll (pl.: többfaktoros hitelesítés) technikai vagy pénzügyi okokból nem vezethető be azonnal minden érintett rendszerre. a szervezet ekkor részletes bevezetési ütemtervet és kompenzációs intézkedéseket dolgoz ki. Az eltérés oka: fokozatos megfelelés és átmeneti állapot kezelése.
- Kontroll nem értelmezhető a rendszerfunkció szempontjából: Bizonyos intézkedések (pl.: erőteljes naplózás) nem

értelmezhetők egy statikus, publikus információkat tartalmazó weboldal esetén, ahol nincs bejelentkezés vagy interaktív adatkezelés. Az eltérés oka: a kontroll célja nem releváns a rendszer működéséhez viszonyítva.

- Kontroll kizárólag speciális rendszerelemekre vonatkozik: Egy komplex rendszer eltérő védelmi igényű komponensekből állhat. Ha például a belső adminisztrációs modul elszigetelt, külön hálózati zónában működik, a hozzáférés-szabályozási kontroll lehet szigorúbb, míg a nyilvános felület esetében enyhébb. Az eltérés oka: differenciált kontrollalkalmazás az architektúra mentén.
- Kontroll ideiglenesen nem megvalósítható: Egy intézkedés (pl.: rendszeres kockázatújraértékelés) technikai vagy humánerőforrás-hiány miatt ideiglenesen nem biztosítható. Az eltérés csak akkor elfogadható, ha van dokumentált kompenzációs mechanizmus, például manuális kontroll vagy gyakoribb monitoring. Az eltérés időtartama és felülvizsgálati terve rögzítendő.

Szükség esetén ezek a kategóriák kombinálhatók is: például egy kontroll egyszerre lehet jogilag nem alkalmazható, és technikailag is irreleváns. a kulcs az, hogy minden eltérésről készüljön:

- írásos indoklás,
- kockázatalapú elemzés,
- kompenzációs kontrollok meghatározása (ha szükséges),
- vezetői jóváhagyás és
- időszakos felülvizsgálati terv.

Az eltérések kezelése a követelményrendszerek gyakorlati alkalmazásának szerves része, és kulcsszerepet játszik abban, hogy a biztonság ne csupán formai megfelelés, hanem ténylegesen fenntartható és arányos védelmi gyakorlat legyen. a rugalmas, de jól dokumentált eltérési mechanizmus lehetőséget ad arra, hogy a szervezet erőforrásainak, működési sajátosságainak és technológiai realitásainak megfelelő védelmi szintet valósítson meg, miközben továbbra is megfelel a NIS 2 irányelv elvárásainak.

A siker kulcsa a transzparens indoklás, a rendszeres felülvizsgálat és a döntések vezetői szintű jóváhagyása. Az eltérések nem kiskapuk, hanem a tudatos és kockázatarányos védelem eszközei – ha szakszerűen alkalmazzuk őket.

09

Előkészítendő dokumentumok és nyilvántartások

Az információbiztonság nem csak technikai kérdés: alapja a megfelelő szabályozási és dokumentációs háttér. a NIS 2 irányelv és a hazai rendeletek előírják, hogy minden szervezetnek rendelkeznie kell szabályzatokkal, eljárásrendekkel és nyilvántartásokkal, amelyek rögzítik a biztonsági elveket, folyamatokat és felelősségeket. Ezek nem formális dokumentumok, hanem a kockázatkezelés, a védelmi intézkedések és a megfelelés nélkülözhetetlen elemei. Az információbiztonsági szabályzat (IBSZ) adja a keretet, a belső szabályozások az operatív működés részleteit, az eljárásrendek és protokollok a végrehajtás lépéseit, a nyilvántartások a nyomonkövethetőséget, a rendszerbiztonsági terv (RBT) pedig mindezt rendszer-szinten foglalja össze. Együtt biztosítják, hogy a szervezet a fenyegetések változása mellett is megőrizze az adatok és rendszerek bizalmasságát, sértetlenségét és rendelkezésre állását. Ezeket mutatjuk be ebben a fejezetben.

9. Előkészítendő dokumentumok és nyilvántartások

Írták: dr. Albert Ágota, Enyedi Alexandra, Sipos Zoltán

9.1. Az EIR-ek biztonsági és kockázatmenedzsment dokumentációi

Az MK rendelet meghatározza az EIR-ek biztonságával kapcsolatos követelményeket, részletesen taglalva azokat a dokumentációs kötelezettségeket, amelyeket a szervezetünknek a kockázatmenedzsment, a biztonsági intézkedések, valamint az ezekhez kapcsolódó belső szabályozók, eljárásrendek és nyilvántartások formájában el kell készítenie és karban kell tartania.

A kockázatmenedzsment dokumentációi

Az MK rendelet 1. melléklete írja le az EIR kockázatmenedzsmenttel kapcsolatos dokumentációs kötelezettségeinket. Ezek célja a szervezet kockázattudatosságának, valamint az információbiztonsági kontrollok tudatos és arányos kialakításának biztosítása.

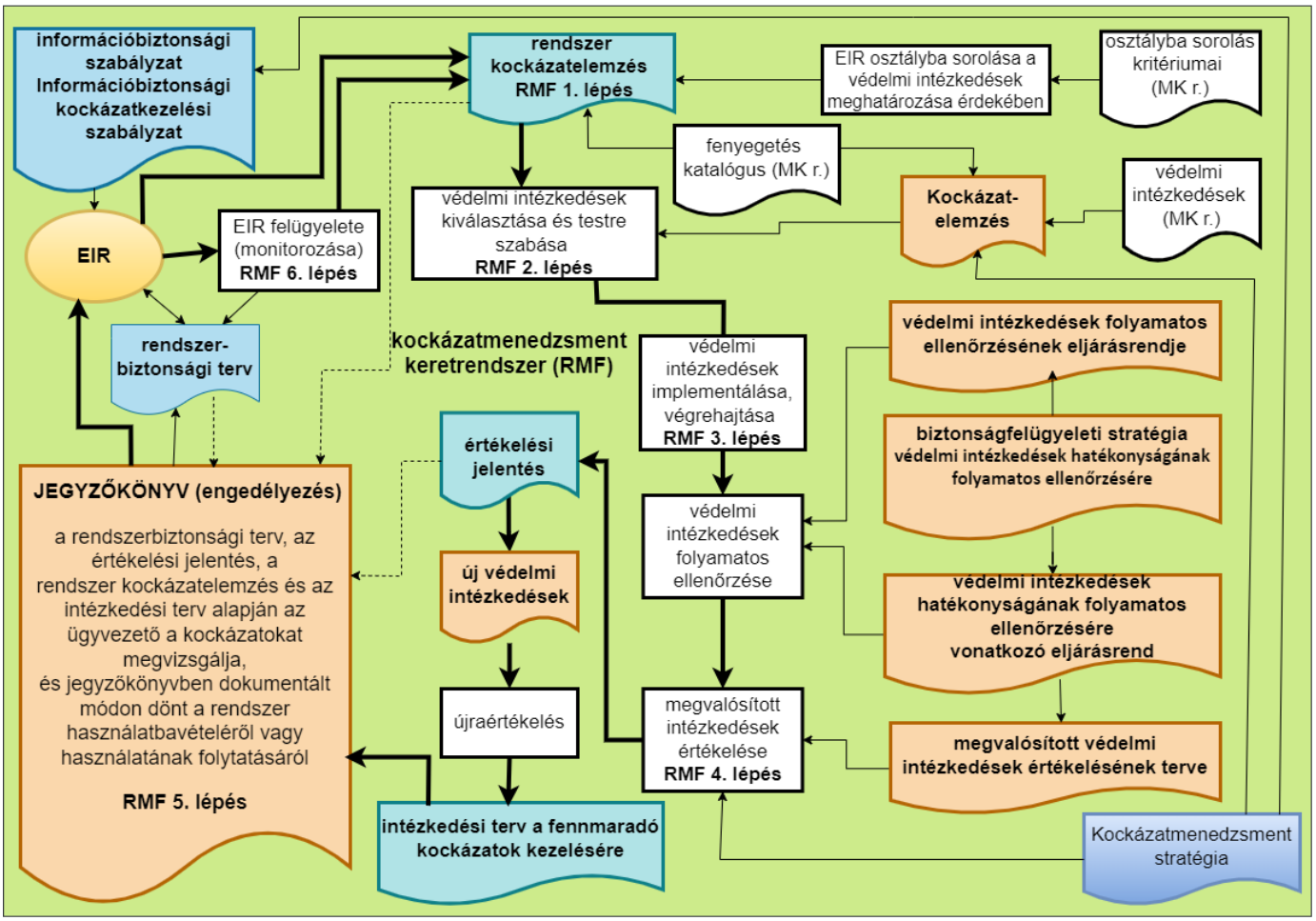
A kockázatmenedzsment keretrendszerünk alkalmazására felkészülésként meg kell határoznunk és dokumentumainkban rögzítenünk kell:

- az EIR-eink védelmével kapcsolatos szerepköröket, felelősségeiket, feladataikat és az ehhez szükséges hatásköröket,
- a kockázatmenedzsment stratégiánkat, amely leírja, hogy hogyan azonosítjuk, értékeljük, kezeljük és felügyeljük a biztonsági kockázatokat,
- a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiánkat, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységeink ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit.

Az EIR dokumentációi

Az EIR-ek tekintetében meg kell határoznunk és dokumentumainkban rögzítenünk kell:

- azokat az üzleti célokat, funkciókat és folyamatokat, amelyeket az EIR támogat,
- a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy szervezeteket,
- az érintett vagyonelemeket,
- az EIR szervezeti és technológiai határát,
- az EIR által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát, valamint az adatvédelmi architektúrát
- az EIR-rel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését
- az EIR helyét a szervezeti architektúrában, amennyiben mi rendelkezünk vele.



4. ábra, Kockázatmenedzsment dokumentumai – EIR szint

A biztonsági követelményeket a rendszerbiztonsági tervben dokumentáljuk.

A folyamatos felügyeleti stratégiával összhangban kidolgozzuk az EIR-re vonatkozó védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrendünket, majd rangsoroljuk és végrehajtjuk a kiválasztott és a rendszerbiztonsági tervben dokumentált intézkedéseket.

A megvalósított védelmi intézkedéseket értékelnünk kell a megvalósított védelmi intézkedések értékelésének tervében meghatározott értékelési eljárásrendünk alapján. Az értékelés dokumentálásaként elkészítjük az észrevételeket és javaslatokat tartalmazó értékelési jelentést.

Az értékelési jelentésben foglalt észrevételek és javaslatok alapján további intézkedéseket vezetünk be a követelmények teljesítése érdekében, majd újraértékeljük a védelmi intézkedéseket, valamint intézkedési tervet készítünk a fennmaradó kockázatok kezelésére.

Az EIR biztonsági állapotára vonatkozó dokumentumok (rendszerbiztonsági terv, értékelési jelentés, rendszer kockázatelemzés, intézkedési terv) alapján az üzembe helyezésére vagy üzemben tartására vonatkozó kockázatokat megvizsgáljuk, és a szervezet vezetője – más személyre át nem ruházható feladatkörében eljárva – jegyzőkönyvben dokumentált módon dönt a rendszer használatbavételéről vagy használatának folytatásáról.

A védelmi intézkedések folyamatos felügyeletével gondoskodunk arról, hogy a bekövetkezett szervezeti, technológiai és biztonsági környezet változása esetén a védelmi intézkedések a kockázatokkal arányosak maradjanak.

Ennek keretében:

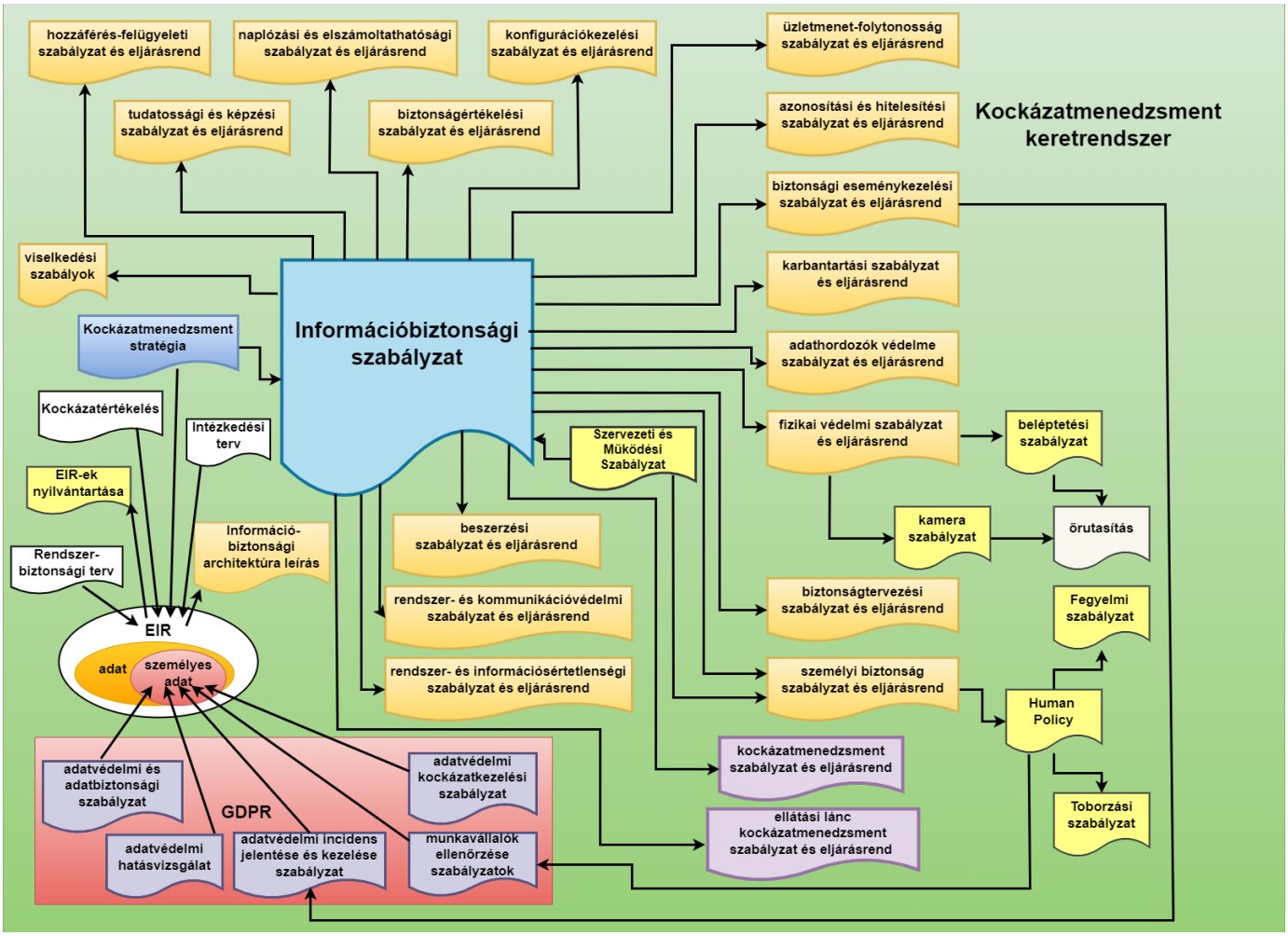
- figyelemmel kísérjük az EIR-ben vagy a működési környezetében bekövetkezett, a rendszer biztonsági helyzetét befolyásoló változásokat, és ennek alapján frissítjük a vonatkozó dokumentumainkat,
- a folyamatos felügyeleti stratégiánk alapján értékeljük az EIR-ben megvalósított védelmi intézkedéseinket, azok állapotát rendszeresen jelentjük a jogosult személyek felé,
- rendszeresen felülvizsgáljuk az EIR biztonsági állapotát, hogy megbizonyosodjunk arról, hogy az azonosított kockázatok elfogadhatók-e a szervezetünk számára,
- biztosítjuk, hogy az EIR élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket.

A szervezet dokumentációi

A 2. melléklet a védelmi intézkedések körét részletezi, melyek a bizalmasság, sértetlenség és rendelkezésre állás hármas célrendszeréhez illeszkedve az alábbi dokumentum kategóriákban jelennek meg:

- Szabályzatok: például információbiztonsági szabályzat (IBSZ), fizikai védelmi szabályzat, kockázatkezelési szabályzat, viselkedési szabályzat stb.
- Eljárásrendek: például incidenskezelési, jogosultságkezelési, mentési eljárásrendek.
- Protokollok: például kommunikációs protokollok, belépési folyamatleírások.
- Nyilvántartások: mint például eszköz-, hozzáférés-, incidens- és auditnapló-nyilvántartások.

5. ábra, Kockázatmenedzsment dokumentumai



9.2. Információbiztonsági szabályzat (IBSZ)

Az információbiztonsági szabályzat (IBSZ) a szervezetünk információbiztonsági irányítási rendszerének alapvető dokumentuma, melynek célja a szervezetünk elektronikus információs rendszereinek, adatvagyonának és működési folyamatainak védelme a kockázatokkal szemben, valamint az MK rendeletben és a NIS 2 irányelvben meghatározott megfelelés biztosítása.

IBSZ célja és szerepe

- Megalapozza az információbiztonsági kontrollokat és védelmi intézkedéseket.
- Rögzíti a biztonsági célkitűzéseket, az alkalmazandó szabályokat és a felelősségi köröket.
- Biztosítja az információs vagyon bizalmasságát, sértetlenségét és rendelkezésre állását.
- Meghatározza az információbiztonsági kockázatok kezelésének kereteit
- Támogatja a megfelelést a vonatkozó jogszabályoknak, így különösen a MK rendelet előírásainak és a NIS 2 elvárásainak.

Az IBSZ tartalmi követelményei

Az IBSZ elemi követelményeit az SZTFH rendelet 7. melléklete alapján, illetve más ISMS keretrendszerek alapján lehet meghatározni. Mire kell mindenképpen kitérnünk a szabályzatunkban?

Általános rendelkezések (a szabályzat célja, hatálya és jogszabályi hivatkozások, az érintett szervezeti egységek és rendszerek köre),

Biztonsági célkitűzések és alapelvek (kockázatarányos védelem elve, minimumkövetelmények a rendszerek és adatok védelmével kapcsolatosan, a szervezetünk biztonsági stratégiájának alapjai),

Szervezeti szerepek és felelősségek (IBF, DPO, vezetők, rendszeradminisztrátorok, felhasználók feladatai, kapcsolat a belső ellenőrzéssel és az IT-üzemeltetéssel),

Biztonsági területek szabályozása (hozzáférés-kezelés, fizikai biztonság, üzemeltetésbiztonság, titkosítás, incidenskezelés, hálózatbiztonság, harmadik felek kezelése, beszerzés, személyi védelem stb.),

Kapcsolódó dokumentumok listája (eljárásrendek, egyéb szabályzatok, nyilvántartások),

Felülvizsgálat és naprakészen tartás (rendszeres tervezett, illetve jelentős változás esetén kötelező felülvizsgálat, a változások dokumentálása és nyomon követése).

Az IBSZ tehát egy olyan szervezeti szintű dokumentum, amely leírja az egész szervezetünkre érvényes biztonsági szabályokat és követelményeket. Lehet egyetlen dokumentum vagy dokumentumok gyűjteménye.

A rendszerbiztonsági terveknek és az IBSZ-nek együtt kell teljes képet kell nyújtaniuk a szervezetünk biztonsági követelményeiről és a megvalósított védelmi intézkedéseinkről. Amennyiben szükséges, az IBSZ-ben hivatkozhatunk a különálló rendszerbiztonsági tervekre vagy eljárásrendekre, amelyek tartalmazzák az alacsonyabb szintű rendelkezéseket.

Az IBSZ frissítését kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban.

Az NKI álláspontja alapján[40] az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

40 Nemzeti Kiberbiztonsági Intézet: Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Programmenedzsment, Verzió 1.0 4.o.

Mikor rossz egy információbiztonsági szabályzat NIS2 szempontból?

- Ha nem NIS2-alapú szemléletű, például nem tükrözi a NIS2 kockázatalapú megközelítését, nem jelenik meg benne a vezetői felelősség, nem tartalmaz ellátási lánc / beszállítói kockázatkezelési elemeket, vagy nem kezeli az incidensbejelentési kötelezettségeket.
- Ha csak „ISO-másolat", helyi viszonyokra adaptálás nélkül, például általános ISO 27001 sablon, nincs hozzáigazítva a magyar végrehajtási rendeletekhez, nem veszi figyelembe a hazai hatósági gyakorlatot, esetleg az anyavállalati IBSZ fordítása, magyar sajátosságok nélkül.
- Ha nem hatókör-specifikus, azaz nem definiálja pontosan, hogy milyen rendszerekre, mely mely szervezeti egységekre, mely telephelyekre, mely beszállítókra vonatkozik, illetve nem különíti el az IT és OT környezetet (amennyiben a szervezet tevékenységi köre alapján az releváns).
- Ha nem kockázatelemzésre épül, például nincs kapcsolat a szervezet kockázatértékelésével, nem látszik, hogy az előírt kontrollok milyen kockázatot kezelnek, illetve nem arányos a szervezet méretével és kitettségével.
- Ha csak elvi deklarációkat tartalmaz, például „Biztosítjuk a megfelelő védelmet…", „Gondoskodunk az incidensek kezeléséről…", de nincs benne felelősségi mátrix, konkrét eljárás, mérhető kontroll, végrehajtási mechanizmus.
- Ha nem vezetői szintű dokumentum, azaz nem hagyta jóvá a felsővezetés, nem tartalmaz vezetői felelősségi és ellenőrzési kötelezettségeket.
- Ha nem kezeli megfelelően az incidenseket, például nem különíti el az információbiztonsági- és adatvédelmi incidenseket, nem szabályozza az eszkalációs utat, nem utal a bejelentési kötelezettségre, nem integrált a válságkezelési rendszerrel.
- Ha nem foglalkozik a beszállítókkal és kiszervezett feladatokkal, például nem ír elő beszállítói biztonsági minimumokat, nem tartalmaz szerződéses követelményeket, vagy nem ír elő rendszeres beszállítói felülvizsgálatot.
- Ha nincs összhangban más belső szabályzatokkal, például ellentmond az adatvédelmi szabályzatnak, más definíciókat használ (pl. „incidens"), nem kapcsolódik a rendszerbiztonsági tervhez, az üzletmenet-folytonossági tervhez, vagy éppen a HR-eljárásokhoz.
- Ha nem naprakész, például elavult technológiákra hivatkozik, nem tükrözi az aktuális architektúrát, nincs rendszeres felülvizsgálati ciklus, esetleg hiányzik a verziókövetés.
- Ha nem auditálható, például nem strukturált követelmény-alapú módon, nem lehet belőle ellenőrzési pontokat levezetni, illetve nem kapcsolódik mérőszámokhoz (KPI/KRI).
- Ha túl részletes technikai dokumentum, például konfigurációs paraméterek vannak benne, operatív utasításokat tartalmaz, nem szabályzat-szintű, hanem eljárás-szintű.
- Ha túl általános, például 4–5 oldalas „elvi" dokumentum, ha nem tér ki olyan kontrollokra, mint a hozzáférés-kezelés, a naplózás, a mentés, a hálózatbiztonság, a kriptográfia és a fizikai biztonság.
- Ha nem tartalmaz szerepkör-alapú felelősségi rendszert, így például nincs RACI-szemlélet, nem definiálja a rendszer tulajdonost, a biztonsági felelőst, az üzemeltetőt és az ellenőrző funkciót.

- Ha nem kezeli az OT sajátosságokat (ha releváns), például nem jelenik meg a gyártási környezet, nem szabályozza a beszállítói távoli hozzáférést, nem tér ki a hálózati szegmentáció elveire.
- Ha nem kapcsolódik oktatási programhoz, nincs előírva rendszeres tudatossági képzés, nem határozza meg a szerepkör-alapú oktatást, nem szabályozza a vezetői képzést.
- Ha nincs mögötte bizonyítási logika, például nem követhető, hogy az előírás hogyan jelenik meg a gyakorlatban.

9.3. Egyéb belső szabályozások

Az IBSZ mellett a szervezetnek specifikus belső szabályozásokat is ki kell alakítania, amelyek részletesebben szabályozzák az egyes biztonsági folyamatokat. Ezek célja a konkrét operatív és technikai tevékenységek részletes, végrehajtható szintű szabályozása.

Milyen belső szabályzatokat alkossunk?

A “Kockázatmenedzsment dokumentumai – szervezeti szint (5. ábra)” bemutatja az MK rendelet szabályozási elvárásait. Lényeges, hogy leszabályozzuk az összes olyan védelmi intézkedést, amelyet a jogszabály megkövetel tőlünk, illetve reagáljunk azokra a kockázatokra, amelyeket a kockázatelemzések feltártak. a szabályozásunk területei, többek között, de nem kizárólag:

- jelszókezelés (minimális hossz és összetettség, lejárati idő és ismétlődés kizárása, többtényezős hitelesítés használata stb.),
- adatmentés és visszaállítás (mentések gyakorisága, tesztelés rendje, helyszíni és távoli mentések, archiválási és törlési szabályok stb.),
- mobil eszközök és távoli hozzáférés (szervezeti és BYOD-eszközök használati feltételei, VPN és titkosított csatornák kötelező használata, elvesztés/ellopás esetén követendő lépések),
- szoftverhasználat (jogosulatlan szoftverhasználat tilalma, licenckezelés rendje, frissítési és patchelési protokoll stb.),
- fizikai és környezeti biztonság (hozzáférési zónák és jogosultságok, kamera- és beléptető rendszerek, áramellátás, hőmérséklet- és páratartalomkezelés, tűzvédelem stb.),
- távmunka és home office (használható eszközök és alkalmazások, titkosított adatkommunikáció előírása, felhasználói magatartás- és biztonságtudatossági elvárások stb.),
- sérülékenységkezelés és frissítés (szkennelési ciklusok, kritikus sebezhetőségek prioritáskezelése, verziókezelési gyakorlatok stb.),
- hozzáférési jogosultságok kezelése (új belépők jogosultsági eljárása, jogosultságmódosítások és megszüntetés, éves jogosultsági felülvizsgálat folyamata stb.),
- beszerzés (szerződések minimum tartalma, beszerzési kritériumok stb.),
- kockázatkezelés (EIR és ellátási lánc stb.),
- incidensmenedzsment stb.,
- személyi védelem (munkaköri leírások, viselkedési szabályok, hozzáférési megállapodások stb.).

Dokumentációs követelmények

A szabályzatok nem pusztán formális dokumentumok, hanem a szervezet működésének és biztonságának alapkövei. Az alábbi követelmények mentén javasolt őket kezelni:

- Minden szabályzatunk legyen naprakész és a szervezetünk egyedi működéséhez igazodó. a netről letöltött, illetve a fióknak

készülő “bármi legyen benne, csak legyen” verziók nem lesznek számunkra megfelelőek.

- A szabályzat:
    - reagáljon a kockázatelemzés által feltárt kockázatokra,
    - legyen összhangban a többi szabályzattal,
    - olyan nyelvezetet használjon, ami az érintettek számára ismert és befogadható,
    - tartalmazza a hatályt (“scope”)
    - nevezze meg a felelősöket és a felelősségi körüket,
    - szükség esetén helyezzen kilátásba szankciót.
- A szakterületek bevonása, a jóváhagyás, a verziókezelés és a felülvizsgálat kötelező, illetve az is, hogy a szabályzatot úgy hirdessük ki, hogy az érintettek azt megismerhessék.
- A munkavállalók számára elérhetővé kell tennünk, és oktatással is támogatnunk kell a szabályok megértését.
- Amennyiben a szabályzat tartalmazza a munkavállalók ellenőrzésének lehetőségét is, abban az esetben tartsunk tiszteletben az adatvédelmi követelményeket is (egyeztessünk az adatvédelmi tisztviselővel).

Minden szabályzat annyit ér, amennyit betartanak belőle. Gondoskodjunk tehát arról, hogy a szakterületek vezetői elkötelezettek legyenek a hatályban lévő szabályzatok betartása és betartatása iránt, és amennyiben a szabályzatok módosítására szükség van, illetve felmerül az igény új területek szabályozására, azt haladéktalanul jelezzék a vezetőség felé.

Tipikus hibák

A szabályzatok kialakításánál és kezelésénél számos olyan hiba fordul elő, amely csökkenti a dokumentum hatékonyságát, megnehezíti a betartását, vagy akár jogszabálysértéshez is vezethet. Tipikus hibák például:

- „Majd az IT lepapírozza” típusú hozzáállás,
- Másolt/letöltött, „generált” szabályzatok, amelyek nem tükrözik a valós működést, csak „word” dokumentumok maradnak,
- Nem megfelelő kockázatértékelés, vagy olyan kockázatértékelés, ami nem vezet intézkedéshez,
- Személyes adatokat kezelő EIR esetén a DPO kihagyása (az információbiztonság és a személyes adatvédelem ütközése),
- Nem megfelelően mért/ellenőrzött teljesítés, díszlet szabályzatok, eljárásrendek,
- Oktatás, tudatosítás hiánya,
- Felelősség hiánya (ki, miért, milyen mértékben). Aki nincs bevonva, az felelősséget sem érez, nem tolhatunk mindent csak az IT-ra,
- Elszámoltathatóság hiánya. a szabályzatot nemcsak megalkotnunk kell, hanem igazolható módon:
    - kihirdetnünk,
    - nyomon követhetően megismertetnünk,
    - a betartást megkövetelnünk és ellen-
      őriznünk és
    - szükség esetén a be nem tartást szankcionálnunk is kell.

9.4. Eljárásrendek és protokollok

A NIS 2 irányelv és annak magyarországi implementációja – különösen az MK rendelet és az SZTFH rendelet – jelentős hangsúlyt fektet a szervezetek biztonságtudatos működésére. Ennek részeként prioritást élvez a kulcsfontosságú eljárásrendek és protokollok dokumentálása, fenntartása és betartatása. Ezek biztosítják, hogy az informatikai rendszerekhez kapcsolódó működés ne ad hoc módon, hanem előre meghatározott, auditálható rend szerint történjen.

Az eljárásrend

Az eljárásrend egy olyan dokumentált folyamatleírás, amely meghatározza az egyes események, helyzetek kezelésének lépéseit, szereplőit, eszkalációs pontjait és határidőit. Az MK. rendelet alapján az eljárásrend az adott területet szabályozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A szabályzatoknak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell a szervezet kockázatkezelési stratégiájához. Amennyiben megfelelő minőségben és megfelelő szempontok mentén készítettük el szabályzatok és a kapcsolódó eljárásrendeket, abban az esetben nagy mértékben hozzájárultunk a szervezetünk biztonságának megőrzéséhez.

A Nemzeti Kiberbiztonsági Intézet útmutatói alapján[41] a szabályzatainknak és a kapcsolódó eljárásrendeknek összhangban kell lenniük nemcsak egymással, hanem az információbiztonsági környezetünkkel is. Az NKI álláspontja az[42], hogy a szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, mivel szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. Amennyiben a szervezetünk felépítése ezt indokolja, dönthetünk úgy is, hogy a szabályzati szinten megjelenő követelményeket szervezeti szintű szabályzat(ok)ba implementáljuk, míg a rendszer- és szerepköri követelményeket tartalmazó eljárásrend(ek)et beépíthetjük a rendszerbiztonsági tervünkbe.

Az eljárásrendeket nemcsak megalkotnunk, hanem frissítenünk is kell rendszeres időközönként, de a módosítást szükségessé tehetik értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban.

Az NKI nyomtatékosan többször is felhívja a figyelmet arra, hogy „az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek”.[43]

Az MK. rendelet számos eljárásrendet nevesít, például

- védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrend[44],
- értékelési tervben meghatározott értékelési eljárásrend[45],
- kockázatelemzési és kockázatkezelési eljárásrend[46],
- szabályzatokhoz kapcsolódó eljárásrendek (pl.: hozzáférés-felügyelet, tudatosság és képzés, biztonsági eseménykezelés, fizikai és környezeti védelem, személyi biztonság,

41 NKI EIR útmutató

42 pl.: Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Hozzáférés-felügyelet, Verzió 1.0. 9.-10 oldal

43 pl.: Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Hozzáférés-felügyelet, Verzió 1.0. 10 oldal

44 MK rendelet 1. melléklet 1.1.3. pont

45 MK rendelet 1. melléklet 1.1.5.3. pont

46 MK rendelet 1. melléklet 3.2.7. pont, 4.2.2. pont és 2. melléklet 15.1. pont

beszerzés, ellátási láncra vonatkozó kockázatelemzés és kockázatkezelés stb.).

Nemcsak arról kell gondoskodnunk, hogy egy adott szabályzat és a kapcsolódó eljárásrendek kidolgozásával dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatokkal egy felelős személy meg legyen bízva, hanem arról is meg kell bizonyosodnunk, hogy ezeket a szabályzatokat és eljárásrendeket az érintettek dokumentált módon meg is ismerjék, valamint az abban foglaltakat ténylegesen meg is valósítsák.

Minőségi kritériumok

Az eljárásrend legyen tömör, szerepkörökre lebontott, a napi működésbe illeszthető, nemcsak technikai, hanem szervezeti, adminisztratív és jogi szempontból is releváns. Dokumentálnunk kell az érvényességét, karbantartását, verzióját.

Nem megfelelő az adott eljárásrend, ha nem ismert az érintettek előtt vagy nem elérhető, túl technikai, túl bonyolult, nem életszerű, vagy nem értik azok, akiknek szánjuk. Az eljárásrenddel kapcsolatban – szükség esetén – oktatást kell tartanunk és időről időre ellenőriznünk kell, hogy az eljárásrendben foglaltak és a gyakorlat menynyiben tér el egymástól.

Protokoll

Protokoll alatt a szervezeti eljárásrendekhez kapcsolódó, jellemzően rövidebb, szituációspecifikus cselekvési terveket értjük. Míg az eljárásrend általános szabályokat, lépéseket és szerepeket rögzít, a protokoll célja egy adott típusú helyzet (pl.: biztonsági incidens, adatvesztés, válságkommunikációs esemény) gyors, összehangolt és ismételhető kezelésének támogatása.

A protokollok gyakran forgatókönyvszerűek, tartalmazzák az azonnali teendőket, felelősöket, kommunikációs lépéseket, és a külső bejelentési kötelezettségeket is (pl.: hatóság, érintett ügyfelek felé). Jó példa erre egy kiberbiztonsági incidens kezelési protokoll, amely akár óránkénti bontásban is meghatározhatja a szükséges teendőket.

Fontos, hogy a protokollok legyenek naprakészek, teszteltek (pl.: asztali gyakorlaton keresztül), és az érintett munkatársak számára elérhetőek és ismertek.

A protokollok nem önálló dokumentumként állnak a rendszerben, hanem az eljárásrendekhez szorosan kapcsolódó gyakorlati segédletek, amelyek biztosítják a szervezet gyors reagálóképességét, különösen a NIS 2 által előírt incidenskezelés, kommunikáció és visszaállítási kötelezettségek teljesítése során.”

9.5. Személyi biztonsággal kapcsolatos dokumentumok

A személyi védelmi intézkedések a kiberbiztonság egyik legkritikusabb, ugyanakkor leginkább alulértékelt területét jelentik. Ezek a kontrollok azt szabályozzák, hogy ki, milyen feltételekkel, milyen felelősség mellett és milyen tudatossággal férhet hozzá a szervezet elektronikus információs rendszereihez és az adataihoz, ideértve az üzleti titkokat és a személyes adatokat is.

A személyi biztonság célja nem az tehát, hogy a HR munkatársakat elárasszuk adminisztratív feladatokkal, hanem az, hogy átgondoltan, stratégiai megfontolások alapján csökkentsük humán kockázatainkat.

A NIS2 szemlélete szerint a vezető felel a megfelelő védelmi intézkedésekért, a személyi kontrollok elmulasztása pedig nem operatív hiányosság, hanem vezetői kockázatvállalás. Amennyiben egy adott EIR-hez hozzáféréssel rendelkező személyek tevékenységét nem szabályozzuk, és ezt a szabályozást nem érvényesítjük következetesen, a legfejlettebb technológiai védelem is sérülékeny lesz.

A személyi védelmi intézkedéseink nem lehetnek egysíkúak, az alkalmazott kontrollok

mélységének meghatározásakor minden esetben célszerű olyan körülményeket, kockázatot befolyásoló tényezőket figyelembe vennünk, mint például a szervezet biztonsági osztályba sorolása, az érintett EIR-ek kritikussága és az adott szerepkör kockázati profilja. Az arányosság hangsúlyozása az, ami segít elkerülni a túlzott adminisztrációt, optimalizálja a költségeinket és növeli az intézkedések szervezeti elfogadottságát.

A belső kockázat

A szervezetek többsége a külső támadókra készül fel, azonban a gyakorlat azt mutatja, hogy a súlyos incidensek jelentős része olyan humán tényezős belső okokra, mint például a túlzott jogosultságra, gondatlanságra, szerepkör-váltás utáni jogosultság-maradványra, illetve sértett, kontrollálatlan hozzáféréssel rendelkező munkavállalóra vezethető vissza.

Nem szabad azonban szem elől tévesztenünk azt, hogy a személyi védelmi intézkedések célja nem a bizalmatlanság kultúrájának meghonosítása, hanem a kockázatok strukturált kezelése és tudatos, jogi és etikai szempontból is megfelelő kezelése.

A személyi védelmi intézkedések három pillére

A személyi védelmi intézkedéseknél mindig figyelemmel kell lennünk arra, hogy az EIR-ekhez nemcsak munkavállalók, hanem alvállalkozók (adatfeldolgozók) munkavállalói, illetve azok képviselői is hozzáférhetnek. A személyi biztonsággal kapcsolatos kontrollokat éppen ezért – jogi státusztól függetlenül – minden felhasználó esetén érvényesíteni kell. Amennyiben a felhasználó az adatfeldolgozó munkavállalója, a védelmi intézkedések egy részével kapcsolatos követelmények érvényesítését (pl. háttérellenőrzés, munkaköri leírás stb.) vállalkozási/megbízási szerződéseinkben, illetve az adatfeldolgozásra/közös adatkezelésre vonatkozó megállapodásainkban kell rögzítenünk.

1. pillér: Megbízhatóság és felelősségvállalás

- Háttérellenőrzés a szükségesség és arányosság figyelembevételével:
- Különösen kritikus szerepkörökben (rendszergazdák, kulcsfontosságú üzemeltetési pozíciók) indokolt a végzettség és szakmai előélet ellenőrzése, a referenciák vizsgálata és a jogszabályok által megengedett módon végrehajtott háttérellenőrzés.
- Nem minden munkakör igényel azonos szintű vizsgálatot, ezért a védelmi intézkedéseket és azok mértékét a rendszerekhez való hozzáférés és a kockázati szint („munkakörök biztonsági szempontú besorolása”) alapján kell differenciálnunk.
- Írásos hozzáférési és titoktartási kötelezettség következetes érvényesítése: A hozzáférési szabályok magukban foglalják a titoktartási megállapodásokat, az elfogadható használati megállapodásokat és a viselkedési szabályokat is, a felhasználó által aláírt hozzáférési megállapodások pedig bizonyítékul szolgálnak arra, hogy mint az EIR-hez hozzáférő személy elolvasta, megértette és egyetért azzal, hogy betartja a korlátozásokat. A megállapodás célja a felelősségek tisztázása, illetve a szabályszegés következményeinek egyértelmű meghatározása és a felhasználóban tudatosítása.

2. pillér: Jogosultság menedzsment

A személyi biztonság egyik legfontosabb eleme az átgondolt és következetesen érvényesített jogosultság-menedzsment:

- Minden felhasználó csak azokhoz a rendszerekhez és adatokhoz férhessen hozzá, amelyek a feladata ellátásához feltétlenül szükségesek. Ez támogatja a

transzparenciát és jelentősen csökkenti a visszaélés lehetőségét.

- Mivel a rendszerhez hozzáférő személyek és a jogosultságok nem statikusak, követelmény a jogosultságok rendszeres és dokumentált felülvizsgálata, valamint a szervezeti és környezeti változásokhoz igazítása.

3. Pillér: A felhasználók személyi változásainak nyomonkövetése és kezelése

A személyi biztonság következetes érvényesítése dinamikus folyamat, amelyben le kell követnünk a munkavállalók és egyéb felhasználók szervezeti „életciklusát". Ez különféle kontrollokat követel meg, például:

- Belépők: háttérellenőrzés, a munkakörüknek megfelelő jogosultság biztosítása, viselkedési szabályok megismertetése, általános és szerepkör alapú biztonságtudatossági oktatásban részesítés, az EIR-hez hozzáférés előtt a hozzáférési megállapodás aláíratása.
- Szerepváltás (áthelyezés) esetén: jogosultságok felülvizsgálata, korábbi hozzáférések megszüntetése, az új munkakörhöz/szerepkörhöz igazodó jogosultságok biztosítása, szükség esetén szerepkörhöz igazodó biztonságtudatossági oktatás. Ide sorolhatjuk azokat a szervezeti intézkedéseket is, amely „kitilt" EIR-ekből felhasználókat, például a viselkedési szabályok megszüntetése miatt.
- Kilépők: azonnali hozzáférés-megszüntetés, szervezet által biztosított eszközök visszavétele, a távoli hozzáférések deaktiválása, figyelmeztetés arra, miszerint a felhasználó titoktartási kötelezettsége a munkaviszony megszűnése után is fennmarad. A felhasználó saját tulajdonú eszközéről is el kell távolítani a hozzáféréseket, illetve információkat.

A felhasználók nyomonkövetése jelentős szervezeti feladat, a szakterületek között folyamatos kommunikációt követel meg, és kimagasló az adminisztrációs igénye is. Azonban ezek a dokumentumok elengedhetetlenek ahhoz, hogy a szervezet megfeleljen az elszámoltathatóság elvének és biztosítsa az audit nyomvonalakat is.

Az auditok egyik leggyakoribb megállapítása például a kilépő munkatársak távozásuk után is aktív hozzáférése, ami tipikusan a HR és az IT közötti koordinációs hiányosságból ered.

Viselkedési normák és biztonsági kultúra

A személyi biztonság nem csak jogosultsági kérdés, hanem magatartási is, éppen ezért fontos, hogy konkrét és érthető viselkedési szabályokat biztosítsunk a felhasználók számára.

Minden felhasználóval – utólag bizonyítható módon – meg kell ismertetnünk az informatikai rendszerek és eszközök használatának szabályait, ideértve többek között az e-mail és internet használat kereteit, a jelszókezelési elveket és az incidensjelentési csatornákat. Azonban nemcsak ellenőrizhetjük, hanem bizonyos esetekben kötelesek is vagyunk ellenőrizni a felhasználók tevékenységét az EIR-jeinkben, éppen ezért nemcsak a használati, hanem a különféle ellenőrzések szabályait is előre meg kell határoznunk és ezekről tájékoztatnunk kell a felhasználókat is.

A szabályok azonban csak akkor hatékonyak, ha közérthetőek, elérhetőek és vezetői szinten is következetesen alkalmazottak. Amennyiben a szabályok változnak, erről minden esetben értesítenünk kell a felhasználókat is, szükség esetén pedig új hozzáférési megállapodást kell velük kötnünk.

Biztonságtudatossági oktatás

Az oktatás nem egy formális kipipálandó elem, hanem olyan szerepkör alapú biztonságtudatossági képzés, amelynek célja – többek között – az adathalász támadások és a social engineering felismerése, a jogosultságok felelős kezelése, a biztonsági szabályok betartása, a hibák/incidensek időbeni jelentése.

Mit jelent mindez ez a projektvezető számára?

A személyi védelmi intézkedések bevezetése szervezeti változást és koordinált csapatmunkát igényel, amely során a projektvezető feladata:

- A HR bevonása a háttérellenőrzési és felelősségi folyamatokba (kockázatelemzés, követelmények alapján a konkrét védelmi intézkedések kialakítása, bevezetése, érvényesítése),
- IT meggyőzése a jogosultsági fegyelem szükségességéről, illetve annak biztosítása, hogy az IT támogatja a HR-t a konkrét védelmi intézkedések meghatározásában, EIR-ekre szabásában,
- Vezetői támogatás biztosítása a szabályok következetes alkalmazásához, ellenőrzési és értékelési módszerek meghatározása és az ellenőrzési rendszer kialakítása,
- a kontrollok dokumentáltságának biztosítása.

Végül, de nem utolsó sorban

A NIS2 megfelelés nem pusztán technológiai érettségi kérdés, és ezt a személyi biztonsággal kapcsolatos védelmi intézkedések bizonyítják a legjobban. A három alapelv – a megbízhatóság, a jogosultsági fegyelem és a biztonsági kultúra – együttesen teremti meg azt az emberi kontrollréteget, amely nélkül a NIS2-nek való megfelelés nem tekinthető teljesnek.

9.6. Nyilvántartások és azok vezetése

A nyilvántartások szakszerű vezetése kulcsfontosságú az elektronikus információs rendszerek biztonságának fenntartásában.

Az MK rendelet előírja, hogy minden szervezetnek kockázatmenedzsment keretrendszert kell működtetnie, amelynek része a nyilvántartások naprakész vezetése. Ez magában foglalja az elektronikus információs rendszerek biztonsági osztályba sorolásához és a védelmi intézkedések bevezetéséhez szükséges dokumentációk, például a kockázatelemzések, fenyegetéskatalógusok és védelmi intézkedések nyilvántartását.

A védelmi intézkedések katalógusa, amely a rendelet 2. mellékletében található, részletesen meghatározza a nyilvántartásokkal kapcsolatos követelményeket. Ezek közé tartozik a hozzáférés-felügyelet, a naplózás és elszámoltathatóság, valamint a konfigurációkezelés. a szervezeteknek biztosítaniuk kell, hogy minden hozzáférési esemény és rendszerkonfiguráció változás megfelelően dokumentálva legyen, lehetővé téve az események visszakövethetőségét és az esetleges incidensek gyors azonosítását.

A nyilvántartások vezetésének további célja a kockázatok változásainak nyomon követése és a védelmi intézkedések hatékonyságának folyamatos értékelése. a szervezeteknek rendszeresen felül kell vizsgálniuk és frissíteniük kell a nyilvántartásaikat, különösen akkor, ha új fenyegetések jelennek meg vagy jelentős változások történnek az információs rendszerekben.

Nyilvántartások ellenőrzőlistája

Kockázatmenedzsment és biztonsági osztályba sorolás:

- Az elektronikus információs rendszerek biztonsági osztályba sorolásának dokumentálása az 1. melléklet szerint,

- Kockázatelemzések és -értékelések nyilvántartása,
- Fenyegetéskatalógus elemeinek vizsgálata és dokumentálása,
- Kockázatkezelési intézkedések és azok végrehajtásának nyomon követése.

Védelmi intézkedések katalógusa (2. melléklet) szerinti nyilvántartások:

- Programmenedzsment: biztonsági politikák, eljárások nyilvántartása,
- Hozzáférés-felügyelet: hozzáférési jogosultságok és azok változásainak nyilvántartása,
- Tudatosság és képzés: biztonságtudatossági képzések és azon résztvevők nyilvántartása,
- Naplózás és elszámoltathatóság: rendszeres naplózási tevékenységek és azok elemzésének, ellenőrzésének nyilvántartása,
- Értékelés, engedélyezés és monitorozás: rendszerértékelések és engedélyezési folyamatok dokumentálása, nyilvántartása,
- Konfigurációkezelés: rendszerkonfigurációk és azok változásainak nyilvántartása,
- Készenléti tervezés: üzletmenet-folytonossági és katasztrófa-helyreállítási tervek dokumentálása, azok tesztelésének nyilvántartása,
- Biztonsági események kezelése: incidensekről szóló nyilvántartás,
- Karbantartás: rendszerkarbantartási tevékenységek és ütemezések nyilvántartása,
- Adathordozók védelme: adathordozók kezelése és védelmi intézkedések dokumentálása,
- Fizikai és környezeti védelem: fizikai biztonsági ellenőrzések nyilvántartása,
- Személyi biztonság: alkalmazottak biztonsági átvilágítása és hozzáférési jogosultságok nyilvántartása,
- Kockázatkezelés: kockázatkezelési stratégiák és intézkedések dokumentálása,
- Rendszer- és szolgáltatásbeszerzés: beszerzési folyamatok és beszállítók nyilvántartása,
- Rendszer és adatintegritási intézkedések és ellenőrzések nyilvántartása,
- Ellátási lánc kockázatkezelése: beszállítók és harmadik felek biztonsági kockázatainak nyilvántartása.

9.6.1. Hogyan lehet ennyiféle nyilvántartást vezetni, karbantartani?

Integrált nyilvántartási rendszer használata

A legéletképesebb megközelítés egy központi, integrált nyilvántartási rendszer kialakítása, amely képes az összes felsorolt nyilvántartás struktúrált és naprakész kezelésére. Ilyen rendszer lehet például egy:

- GRC (Governance, Risk, Compliance) platform,
- ISMS (Information Security Management System) megoldás,
- Testreszabott dokumentumkezelő rendszer (pl.: SharePoint, Confluence + Power Automate, vagy Matrix42, ServiceNow).

Funkciók, amiket érdemes keresni:

- Verziókövetés,
- Jogosultságkezelés,
- Naplózás,
- Automatikus emlékeztetők frissítésekhez,
- Sablon alapú nyilvántartások (pl.: kockázatelemzéshez, konfigurációváltozásokhoz).

Felelősségi körök kiosztása és delegálás

Egy ekkora nyilvántartási kör nem vezethető egyetlen személy által. Ezért fontos:

- Felelősök kijelölése az egyes területekre (pl.: IT üzemeltetés, HR, beszerzés, fizikai biztonság stb.),
- Tisztázott tulajdonosi modell: minden nyilvántartásnak legyen „gazdája”,
- Rendszeres belső auditok segítségével biztosítható az adatminőség és aktualitás.

Automatizálás és integráció

Sok nyilvántartási típus (pl.: hozzáférés-változások, naplózás, konfigurációk) automatikusan gyűjthető és dokumentálható technikai eszközökkel:

- SIEM rendszerek (pl.: Sentinel, Splunk, QRadar): naplózás és eseményazonosítás,
- Identity & Access Management (IAM) rendszerek: jogosultságkezelés és naplózás,
- CMDB eszközök: konfigurációkezelés automatizáltan,
- Védelmi eszközök (EDR, NDR): események és válaszok nyilvántartása.

Sablonok és standardizált dokumentációs formák

Egyszerűsíti a fenntartást, ha minden nyilvántartásra előre definiált sablon áll rendelkezésre:

- Kockázatelemzési űrlap,
- Incidens bejelentő lap,
- Jogosultság-változás sablon,
- Tesztelési jegyzőkönyvek (pl.: katasztrófa-helyreállítás),
- Beszállítói értékelési táblázat.

Így gyorsabb, átláthatóbb és egységesebb az adminisztráció.

Rendszeres karbantartási ciklusok kialakítása

A karbantartás fenntarthatósága érdekében célszerű negyedéves, féléves frissítési ciklusokat kialakítani, például:

- Minden negyedévben: jogosultságok felülvizsgálata, naplózás auditálása,
- Félévente: kockázatelemzések, beszállítói kockázatfelmérések aktualizálása,
- Évente: rendszerkonfigurációk, védelmi tervek tesztelése és frissítése.

Ez kombinálható a belső ellenőrzési tervekkel és compliance felkészüléssel.

9.7. A rendszerbiztonsági terv

A rendszerbiztonsági terv (a továbbiakban: RBT)[47] célja, hogy dokumentált formában rögzítse az adott informatikai rendszer biztonsági állapotát, a meghozott védelmi intézkedéseket, valamint a szervezeti és technikai kontrollokat.

Az RBT-t a szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős szerepkört betöltő személy hagyja jóvá.[48] a rendszerbiztonsági terv magas szintű irányítási dokumentumok közé tartozik, ugyanúgy, mint az informatikai biztonsági stratégia, az informatikai biztonsági politika, valamint a kockázatértékelési, kockázatkezelési politika.[49]

A kiválasztott és a rendszerbiztonsági tervben dokumentált intézkedéseket rangsorolnunk kell, majd végrehajtanunk úgy, hogy a védelmi intézkedések tényleges megvalósítása, valamint a tervtől való esetleges eltérések alapján az RBT-t frissítjük.

47 MK rendelet 2. sz. melléklet 13.2. Rendszerbiztonsági terv védelmi intézkedés

48 MK rendelet 1. melléklet 1. pont

49 1/2025 (I.31) SZTFH rendelet 5. melléklet 1.2.1.2.1. pont

Az RBT a rendszer használatbavételével vagy használatának folytatásával kapcsolatos döntésről szóló jegyzőkönyv alapjául szolgáló dokumentum. Az audit során az RBT típusa „biztosító", értékelésből nem kizárható.

Milyen követelmények vannak az RBT-vel szemben?

Strukturális és tartalmi elvárások:

- legyen összhangban a szervezeti felépítéssel,
- határozza meg az EIR-t alkotó rendszerelemeket, az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait az ügymeneti és üzleti folyamatok szempontjából,
- azonosítsa azokat a személyeket, akik az EIR szerepeit és felelősségeit betöltik,
- határozza meg az EIR által feldolgozott, tárolt és továbbított információtípusokat,
- megfelelően alátámasztott módon határozza meg az EIR jogszabály szerinti biztonsági osztályát.

Biztonsági és operatív követelmények:

- sorolja fel az EIR-t érintő konkrét fenyegetéseket,
- határozza meg az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait, vagy azoktól való függőségeit,
- határozza meg és dokumentálja a rendszerre vonatkozó biztonsági alapkövetelményeket és szükség esetén az ezen felül alkalmazott kiegészítő védelmi intézkedéseket,
- határozza meg a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, intézkedésbővítéseket és azok indoklását,
- rögzítse azokat a biztonsági feladatokat, amelyek végrehajtása összehangolt munkát, koordinációt vagy tervezést kíván meg különböző szervezeti szerepkörök között.

Az RBT-t a jóváhagyó felelős:

- a végrehajtás előtt áttekinti és jóváhagyja,
- gondoskodik arról, hogy azt a meghatározott személyek és szerepkörök megismerjék (ideértve annak változásait is), valamint jogosulatlanok számára ne legyen megismerhető vagy módosítható,
- előre meghatározott gyakorisággal felülvizsgálja,
- frissíti az EIR-ben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

A védelmi intézkedések között számtalan olyat találunk, amely kötelező eleme az RBT-nek, pl.: 2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek. Jogszabály tartalmazza az RBT-vel kapcsolatos elemi követelményeket is.[50]

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet RBT sablonokat tett közzé mindhárom biztonsági osztályhoz (alap, jelentős, magas)[51], segítve az MK rendeletben foglaltak végrehajtását.

Hogyan álljunk neki az RBT kidolgozásának?

Célszerű interdiszciplináris csapattal nekifogni, bevonva olyan szakterületek képviselőit, mint az IT, az adatvédelem, a compliance, valamint a rendszert használó üzleti egységek.

Az NKI 2025. őszén módosította az RBT kötelező tartalmát, beemelve az adatvédelmi

50 1/2025 (I.31) SZTFH rendelet 7. melléklet K13.002 hivatkozási kód.

51 NKI az MK rendelet alapján aktualizált rendszerbiztonsági terv sablonok

kockázatelemzést a személyazonosításra alkalmas (PII) adatokat kezelő rendszerek tekintetében, illetve a biztonsági és adatvédelmi architektúra, valamint a tervezési döntések kockázatmeghatározását. Ez a kiegészítés egyelőre csak az NKI dokumentumaiban jelenik meg, a vonatkozó jogszabályokban még nem.

A sablonokat lehetőleg testre szabva, a szervezeti kontextushoz igazítva alkalmazzuk, valós, rendszerre szabott kockázatelemzésre alapozva. Amennyiben az RBT elavult, nem frissített rendszerleírás, abban sablonszöveget használunk, a verziók követését nem dokumentáljuk, az érintettek vonatkozásában elhanyagoljuk a kapcsolódó oktatásokat, az RBT elveszti gyakorlati értékét, és nem tölti be irányítási szerepét.

Mikor rossz egy rendszerbiztonsági terv NIS2 szempontból?

- Ha jogszabály-független, „sablonos” dokumentum, például nem hivatkozik a hazai NIS2 végrehajtási rendeletekre, nem tükrözi a magyar felügyeleti gyakorlat (pl. hatósági ellenőrzési szempontok) elvárásait, vagy éppen a külföldi anyavállalati template egyszerű fordítása, helyi adaptáció nélkül.
- Ha nem konkrét EIR-re készült, például általános IT-biztonsági szabályzatként működik, nem rendszerspecifikus (nincs pontos rendszerleírás, hatókör, adatáramlás, interfészek), vagy nem különíti el az IT és az OT környezetet, ahol ez releváns.
- Ha nincs kockázatelemzésre alapozva, például nem kapcsolódik dokumentált kockázatelemzéshez, nem látható, hogy az intézkedések milyen azonosított kockázatot kezelnek, vagy a kockázati szintek és a védelmi intézkedések között nincs arányosság.
- Ha nem bizonyítható az intézkedések tényleges megvalósulása, például a terv csak deklarál (“alkalmazzuk”, “biztosítjuk”), de nincs meghatározva felelős, szükség esetén határidő, kontrollmechanizmus, mérhetőség, valamint nincs összekötve üzemeltetési bizonyítékokkal (logok, jegyzőkönyvek, riportok).
- Ha hiányos az incidenskezelési rész, például nem tartalmaz konkrét bejelentési folyamatot, nem szabályozza az észlelés–minősítés–eszkaláció lépéseit, nem veszi figyelembe a NIS2 szerinti rövid bejelentési határidőket, vagy éppen nincs összhangban a szervezet válságkezelési struktúrájával.
- Ha nem kezeli a beszállítói és ellátási lánc kockázatokat, például nem tér ki a külső szolgáltatókra, nincs beszállítói minősítési vagy felügyeleti mechanizmus, vagy a felhőszolgáltatók, IT támogatással kapcsolatos szolgáltatások nincsenek beemelve.
- Ha nem kezeli külön az OT / ipari rendszereket (amennyiben a szervezet tevékenysége szempontjából az releváns), például nem különíti el az üzembiztonsági és információbiztonsági követelményeket, nem tartalmaz hálózati szegmentációs elveket vagy éppen nem tér ki a gyártói hozzáférések kontrolljára.
- Ha nincs vezetői felelősségi szintű dokumentum, például nincs kijelölt felelős vezető, nem nyomonkövethető a vezetői felelősség.
- Ha nem naprakész, például hiányzik a verziószám, a dátum, vagy a felülvizsgálati ciklus, nem tükrözi az aktuális architektúrát és nem tartalmaz változáskezelési nyomvonalat.

- Ha nincs összhangban a szervezet szabályzataival, például ellentmond az adatvédelmi szabályzatnak, nem az IBSZ-nek megfelelően definiál incidenseket, jogosultsági szinteket, nincs kapcsolata az üzletmenet-folytonossági tervvel, a katasztrófa-helyreállítási tervvel, illetve az incidenskezelési eljárásrendekkel.
- Ha túl technikai, vagy épp túl jogias, például csak jogszabályi hivatkozásokból áll, vagy ellenkezőleg, kizárólag technikai leírás, jogszabályi kontextus nélkül, netalán nem értelmezhető az auditor számára.
- Ha nem auditálható, például nem ellenőrizhető objektív bizonyíték alapján, nincsenek kontrollpontok, nem megfelelően strukturált a megfelelőségi követelmények mentén.
- Ha nem arányos, például nem kockázatarányosak a kontrollok, vagy nem tükrözi a szervezet méretét, tevékenységét, kitettségét.
- Ha nem tartalmaz tudatossági és oktatási elemet, például nem kapcsolódik képzési programhoz, vagy nem szabályozza a szerepkör-alapú biztonsági felelősséget.

10

Auditálási folyamat

Mint minden auditra, itt sem szabad az utolsó pillanatban felkészülni, hiszen, mint látjuk a jogszabályokból, van tétje (bírság, új auditra kötelezés, vezetői eltiltás). a siker kulcsa a szervezett, ütemterv alapú és tételes felkészülés. Önmagában a szabályzatok, eljárásrendek megléte még nem elegendő az audit sikeres teljesítéséhez; szükség van olyan evidenciákra és bizonyítékokra is, amelyek igazolják, hogy a leírtak a gyakorlatban is megvalósultak. Minden intézkedéshez intézkedési tervet kell készteni, határidőkkel, felelőssel és pénzügyi tervezéssel. Ha egy intézkedés pénzügyi vagy időbeli okokból még nem valósult meg, célszerű a részletes intézkedési tervben módosítani a határidőt és a pénzügyi adatokat, amely már a reális, ésszerű határidőket tartalmazza, és biztosítja a feladatok végrehajtását a rendelkezésre álló erőforrásokon keresztül. Ezen elvek mentén a fejezetben részletesen bemutatjuk az auditálási folyamat lépéseit, a szükséges dokumentumokat, bizonyítékokat és a felkészülés bevált módszereit.

10. Auditálási folyamat

Írták: Arató György, Enyedi Alexandra, Koppány Géza, Mészáros Csaba, dr. Novák Anett, Mandrik Edina, Dr. Váczi Dániel

10.1. Evidenciák előkészítése, összegyűjtése

Az auditálást megelőzően az evidenciák előkészítése, összegyűjtése, rendszerezése döntő fontosságú az audit sikeressége szempontjából. Az evidenciák előkészítése, összegyűjtése és rendszerezése során, különösen azon bizonyítékok esetén, amely valamely technológiai megfelelőséget hivatottak megmutatni, felbukkanhatnak olyan nemmegfelelőségek is, amelyeket a belső audit vagy a GAP elemzés valamely okból nem tárt fel vagy nem evidencia mélységig vizsgált meg.

Ha az auditra való felkészülést a szervezet az SZTFH rendelet 7. melléklete szerinti mélységig végzi el, még az auditot megelőzően lehetősége van arra, hogy az ilyen módon is feltárt hiányosságokra időben meghozza a szükséges védelmi intézkedéseket, vagy pótoljon olyan technológiai beállításokat, amelyek hiánya ezt a nemmegfelelősséget okozza.

Az evidenciákat javasolt a már fent említett melléklet alapján kategorizálni és az egyes követelményekhez rögzítetten összegyűjteni és tárolni, hogy az auditon már célzottan, ennek birtokában tudja a szervezet képviselni és igazolni a megfelelőséget.

A kategorizálást javasolt az SZTFH rendelet 6. melléklete alapján elvégezni, és azokkal az evidenciákkal mindenképp előkészülni, összegyűjteni, amelyet a melléklet kötelező tesztre vagy dokumentumelemzésre jelöl ki.

A dokumentum elemzéshez kapcsolódó evidenciák a szervezet IBIR szabályozói környezetét érintik elsősorban, és mindazon üzemeltetési és fejlesztési dokumentációt, amely kapcsolódik az információbiztonsághoz. Ebből következően, ha egy jól felépített és dokumentált IBIR-rel már rendelkezik a szervezet, ezen evidenciák összegyűjtése nem fog problémát okozni. Javasolt a szabályozói környezet esetén az egyes evidenciákat úgy jelölni, hogy az könnyen visszakeresheto legyen, pl.: az IBSZ esetén oldalszám(ok), fejezetszámok, bekezdések jelölésével.

A tesztre kijelölt kontrollok esetén több esetben is olyan technológiai ellenőrzésre kerülhet sor, amely pl.: a határvédelmi megoldásokat teszteli. Ezekhez jellemzően az alkalmazott megoldás, technológia dokumentációja szolgáltatja az evidencia egyik lábát, míg a másik lábát a működést igazoló képernyőképek adják jellemzően. Evidencia lehet még egy-egy olyan log is, amely szintén az elvárt működést igazolja.

Mind a dokumentumelemzésre, mind a tesztre kijelölt kontrollok esetén az evidenciákat javasolt úgy tárolni, hogy az visszavezethető legyen az adott kontrollpontra – pl.: névkonvencióval jelölve, vagy Excel táblában jelölve az egyes evidenciák fájlneveit stb.

10.2. Auditálásba bevont személyek felkészítése

Az SZTFH rendelet 6. melléklete alapján “Kötelező interjú” jelölésű kontrollok esetén várható, hogy az auditor a szervezet egyes szerepköreivel interjút fog készíteni. Az interjú során az auditor a szervezet IBIR szabályozói környezetében meghatározott védelmi intézkedések gyakorlati megvalósulását fogja ellenőrizni, éppen ezért az audit sikeressége szempontjából sok múlhat a megszólított kolléga válaszainak magabiztosságán, szakszerűségén és teljeskörűségén, így az ő felkészítésükre is javasolt időt fordítani az audit felkészülése során.

A felkészítés során a következő szempontokat javasolt szem előtt tartani:

- az auditor az interjúk keretében elsősorban a gyakorlati megvalósulását fogja vizsgálni a szabályzatokban, eljárásrendekben, egyéb dokumentációkban megtalálható szervezeti, technológiai kontrolloknak;
- az interjúra kijelölt kollégák esetén a szakterületéhez kapcsolódó folyamatokat és a folyamatokban érintett egyes IT megoldások ismerete éppen ezért elengedhetetlen ez a gyakorlati vetülete a megfelelőségnek;
- ugyanígy az interjúra kijelölt kollégák esetén a szakterületéhez kapcsolódó szabályzatokat, eljárásokat és munkautasításokat is érdemben ismernie szükséges;
- az interjún a szabályzati, eljárásrendi kontrollok érvényesülését a kollégának meg kell tudnia mutatni a gyakorlatban is, amennyiben ezt az auditor kéri, így a felkészítés során a gyakorlatot az elmélettel – azaz a szabályozásokkal – javasolt legalább egyszer áttekinteni az auditot megelőzően.

Összegezve, a kijelölt kollégáknak az alábbi ismeretekkel mindenképpen rendelkeznie szükséges az auditot megelőzően:

- a szakterületéhez kapcsolódó szabályzatok, eljárásrendek, egyéb dokumentációkban megtalálható szervezeti, technológiai kontrollok;
- a szakterületének üzleti folyamatai;
- az üzleti folyamatot támogató IT megoldások;
- valamint e három halmaz metszete: az üzleti folyamat hogyan kapcsolódik az IT megoldásokhoz és szabályzatokhoz.

Az interjú sikerességét jelentősen befolyásolja az interjúalany kommunikációs és viselkedési stílusa is. Az interjú alanyok belső felkészítése, kiválasztása során érdemes hangsúlyt fektetni az alábbi soft skillek meglétére, a figyelem felhívására:

- magabiztos, de nem túlzottan domináns kommunikáció;
- pontos és tömör, de ne legyen szűkszavú válaszadás, a kérdésekre célzottan reagálva;
- nyugodt viselkedés, stresszhelyzetek kezelése gyakorlással;
- aktív figyelem, a kérdések teljes meghallgatása és csak ezután történő válaszadás;
- őszinteség abban az esetben is, ha valamire nincs pontos információ, konstruktív megfogalmazással;
- nonverbális jelzések tudatos használata, mint szemkontaktus, nyitott testtartás, nyugodt mozdulatok;
- a válaszok relevanciájának megőrzése, a kommunikációt a témán tartva, kerülve a szükségtelen kitérőket vagy mellékszálakat, mellyel felhívhatjuk a hiányosságokra feleslegesen a figyelmet.

10.3. Pontozási rendszer értelmezése és bemutatása gyakorlati példán keresztül

A NIS 2 szerinti magyar auditálási eljárás egyik fontos újítása, hogy nem kizárólag bináris (igen/nem) alapon vizsgálja a kontrollokat, hanem minőségi és strukturált módon értékeli azok meglétét, működését és hatásosságát. A módszertan az SZTFH rendelet 5. mellékletében szereplő Auditori módszertanon alapul, mely a NIST 800-53A Rev. 5 értékelési logikájára épít. Az értékelés célja, hogy ne csak az derüljön ki, hogy létezik-e egy szabály vagy eljárás, hanem az is, mennyire működik hatékonyan a gyakorlatban. Az auditor az egyes elemi

követelmények esetében általában három dimenzió mentén végez értékelést:

- Dokumentáltság: Van-e dokumentált szabályozás, eljárásrend, szerződés vagy utasítás? – Például: a szervezet rendelkezik írásban rögzített hozzáférés-kezelési szabályzattal, amely meghatározza a jogosultságkezelés folyamatát.
- Működés: a dokumentumban foglaltak ténylegesen alkalmazásra kerülnek-e, működnek-e a gyakorlatban? – Például: a szabályzatnak megfelelően történik a jogosultságok kiosztása, de az eltávolítás és időszakos felülvizsgálat nem minden rendszerre terjed ki, vagy nincs automatizált támogatás.
- Hatékonyság: a kontrollok elérik-e a kívánt célt? Csökkentik-e a kockázatot, megelőzik-e a hibákat vagy incidenseket? – Például: a belső auditok során nem találtak kritikus jogosultsági problémát, de egy korábbi incidensnél manuális visszavonás okozott késedelmet.

Az auditor a követelménycsoportok vizsgálata során először szétválasztja azokat aszerint, hogy azok szervezeti szintű (SZ) vagy elektronikus információs rendszerenkénti (EIR) értékelést igényelnek. Ez az információ nem értékelési döntés kérdése, hanem előre meghatározott, és a 6. melléklet táblázatában minden követelménycsoporthoz rögzített.

- Az SZ típusú követelmények esetén az auditor egyszer vizsgál a teljes szervezetre vonatkozóan.
- Az EIR típusú követelményeket minden egyes vizsgálatba bevont információs rendszerre külön-külön kell értékelnie.

Ezt követően az auditor értékeli a követelménycsoport alkalmazhatóságát is. Ha egy adott követelmény, például valamilyen technológiai vagy működési sajátosság miatt, nem releváns az adott szervezet vagy rendszer szempontjából, akkor „nem alkalmazható” minősítést kap, és nem képezi az audit tárgyát. Fontos, hogy a 6. melléklet rögzít olyan követelménycsoportokat, amelyet nem lehet figyelmen kívül hagyni. Ezesetben nem kaphatják meg ezt a minősítést. Kiemelendő, hogy az auditált szervezet feladata ismernie a saját rendszereit és egyértelműen, dokumentált formában rögzíteni az egyes követelmények alkalmazhatóságát vagy kizárását. Ennek elmaradása hibapontot és nemmegfelelőséget eredményezhet.

A következő lépésben az auditor kiválasztja a vizsgálati módszereket. a 6. mellékletben táblázatosan rögzítették, hogy egyes követelmények esetén kötelező-e alkalmazni dokumentumvizsgálatot, interjút vagy tesztelést. Jellemzően ezek kombinációja van előirányozva.

Ezután az auditor áttér annak vizsgálatára, hogy a 6. mellékletben szereplő követelménycsoportokhoz milyen konkrét elemi követelmények tartoznak a 7. melléklet alapján. Mivel egy-egy csoport több ilyen elemből áll, ezek teljesülését külön-külön értékeli, de az összesített minősítést már követelménycsoport szinten adja meg, amely háromféle lehet:

- **NA (nem alkalmazható)**: a követelmény a konkrét környezetben nem értelmezhető.
- **NM (nem megfelelt)**: nincs elérhető bizonyíték vagy a szervezet nem teljesíti a követelményt.
- **M (megfelelt)**: az auditor rendelkezésére állnak a megfelelő bizonyítékok, és a követelmény igazolhatóan teljesül.

Amennyiben minden elemi követelmény „megfelelt” vagy „nem alkalmazható” értékelést kap, úgy az adott követelménycsoport minősítése megfelelt lesz. Amennyiben legalább egy elemi követelmény „nem megfelelt”, akkor az auditor köteles az eltérés súlyosságát megállapítani. a minősített eltérések számszerűsítésre kerülnek, hogy kiszámítható legyen az adott

információs rendszer védelmi megfelelési indexe (VMI). Ez az érték azt mutatja meg, mennyire tér el az adott EIR a rendelet szerinti elvárásoktól. a követelménycsoportokhoz a következő pontszámokat rendelik hozzá az eltérés súlyossága alapján:

Minősítés	Értelmezés	Érték
Megfelelt	Minden elemi követelmény teljesül vagy nem alkalmazható	0
Elhanyagolható mértékű eltérés	Az eltérés nem befolyásolja érdemben az EIR biztonságát.	1
Kis mértékű eltérés	Az intézkedés részben működik, de célját lényegében teljesíti.	4
Kiemelt mértékű eltérés	Az intézkedés lényegében nem működik.	10
Kritikus mértékű eltérés	Jelentős kockázatot jelent, akár adatvédemi, üzleti vagy működési szempontból.	1000

A VMI számítás a következő képlet alapján történik:

Értelmezve a képletet:

$$VMI = 100 - 100 * \frac{\left(2 * \sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j\right)}{(20n + 10m)}$$

- A követelmények nem egyformán fontosak. Minden vizsgált követelménycsoport egy előre meghatározott típusba tartozik. a “Biztosító” típusúak az alapkövetelmények. Ha ezek nem teljesülnek, az az EIR működésének alapjait veszélyeztetheti. Ilyenek például a szabályzatok megléte, a felelősségi körök kijelölése vagy a kritikus beállítások. a “Támogató” típusúak szintén fontosak, de inkább kiegészítő jellegűek. a biztosító intézkedések működését segítik, de önmagukban kevésbé kritikusak.
- Minden problémás követelményhez egy úgynevezett eltérési érték tartozik, amely azt mutatja meg, mennyire súlyos az adott hiányosság. Ezeket a korábban bemutatott táblázat tartalmazza: 0, 1, 4, 10 vagy akár 1000 pont.
- A rendszer tehát nem egyszerűen a hibák számát nézi, hanem figyelembe veszi, hogy milyen típusú követelmény sérült, és milyen súlyossággal. a „biztosító” eltérések kétszer olyan fontosak, mint a „támogatók”. Ezt a képlet úgy éri el, hogy a biztosítók pontszámát kétszerezve számolja be, a támogatókét egyszeresen, majd az egészet egy olyan nevezővel osztja el, amely figyelembe veszi a vizsgált követelmények súlyát is (20 pont minden biztosító, 10 pont minden támogató után).
- A képlet eredménye egy százalékos értékhez hasonló szám, amely azt mutatja meg, mennyire teljesíti az adott rendszer a megfelelési elvárásokat. Az értelmezés a következő:

VMI érték	Megfelelés minősítése
≥ 95	Megfelel
90–94	alacsony kockázattal megfelel
80–89	jelentős kockázattal megfelel
70–79	magas kockázattal megfelel
< 70	nem felel meg

Vegyünk egy konkrét példát a „Rendszer- és szolgáltatásbeszerzés” követelménycsaládból, amely tartalmaz szervezeti szintű (SZ) és elektronikus információs rendszerenkénti (EIR) követelményeket is. Most nézzük meg az egyik SZ típusú követelményt: a 16.1-es csoportot. Ez a követelménycsoport ún. P (paraméter) elemeket és O (operatív) elemi követelményeket tartalmaz. a P típusú elemeket a szervezetnek kell meghatároznia, míg az O típusúakat azok alapján kell működtetni, behelyettesítve az adott paramétert. (A lenti példa táblázatban nem soroljuk fel az összes sort, amit a 7. melléklet definiál.)

Az auditor tehát egyenként értékeli az egyes P és O követelmények teljesülését. Ebben az esetben talált olyan pontot, amely nem teljesült, ezért a teljes követelménycsoportra „nem megfelelt” (NM) minősítést ad. a probléma súlyosságát kis mértékű eltérésként értékeli, így a csoporthoz 4-es pontszámot rendel.

Mivel ez egy SZ típusú követelmény, elegendő egyszer, szervezeti szinten értékelni, viszont minden EIR VMI-számításába beleszámít. Emellett „Támogató” típusú követelmény, így a számítás során egyszeres súllyal kerül beszámításra. a példa:

16.1. Szabályzat és eljárásrendek		**Sz**	**Támogató**	**M**	**4**
K16.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a beszerzési szabályzatot meg kell ismertetni	Meghatározta a paramétert			
K16.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a beszerzési eljárásokat meg kell ismertetni	Nem határozta meg a paramétert			
.					
K16.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a beszerzési eljárásokat felül kell vizsgálni és aktualizálni kell	Megtörtént			
K16.001_O_16.1.1.(a)	beszerzési szabályzatot dolgoztak ki és dokumentáltak	Megtörtént			
K16.001_O_16.1.1.(b)	a beszerzési szabályzatot megismertették a K16.001_P[1] által meghatározott személyekkel vagy szerepkörökkel	Nem a paramétertől eltérő a gyakorlat			
.					
K16.001_O_16.1.1.1.2.	a beszerzési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal	Összhangban van			

A következő követelménycsoport példa a 16.66, mely EIR szintű, így az auditornak annyiszor kell elvégezni az értékelést, ahány EIR-t auditál. Ráadásul Biztosító típusú, így a fenti képletben sokkal nagyobb mértékben számít bele. Mivel azonban minden elemi követelmény szinten megfelel, így 0-s értékelést kap.

16.66. Fejlesztői biztonsági tesztelés		EIR	Biztosító	M	O
K16.001_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {egység-, integrációs-, rendszer-, illetve regressziós tesztelés}	Meghatározta a paramétert			
K16.001_P[2]	meghatározták a tesztelés, illetve értékelés elvégzésének gyakoriságát	Meghatározta a paramétert			
K16.066_P[3]	a K16.066_P[1] szerinti teszttípus mélysége és lefedettsége meghatározásra kerül	Meghatározta a paramétert			
K16.001_O_16.1.1.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában tervet dolgozzon ki a folyamatos biztonsági értékelésekre	Megtörtént			
K16.001_O_16.1.1.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában hajtsa végre a tervet a folyamatos biztonsági értékelésekre	Megtörtént			
.					
K16.066_O.16.66.5	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában javítsa ki a tesztelés és értékelés során azonosított hibákat	Megtörtént			

Így értékel minden követelmény csoportot az auditor és határozza meg EIR-enként a VMI indexet.

A SZEKI (szervezet ellenálló-képességi index) megmutatja, összességében milyen állapotban van a szervezet információs rendszereinek biztonsága. a jogszabályban megadott képlet a következő:

$$SZEKI = \frac{\left(\sum_{i=1}^{n} VMI_i\right)}{n}$$

Ez a gyakorlatban egy egyszerű átlagolást jelent. Össze kell adni az összes EIR VMI értékét, majd el kell osztani a rendszerek számával. Például ha van 3 rendszer, és a VMI értékek: 95, 87, 72, akkor a SZEKI=(95+87+72)/3=84.67.

A SZEKI értékelését az alábbi táblázat foglalja össze:

SZEKI	Minősítés	Eredmény
≥ 95	elhanyagolható kockázattal megfelel	megfelel
90–94	alacsony kockázattal megfelel	auditált
80–89	közepes kockázattal megfelel	
70–79	magas kockázattal megfelel	
< 70	kritikus kockázattal nem felel meg	nem felelt meg

10.4. Szubjektív tényezők szerepe az auditban

Az információbiztonsági auditok célja annak értékelése, hogy egy szervezet mennyire felel meg a vonatkozó szabályozásoknak, sztenderdeknek és saját belső követelményeinek. Az SZTFH rendelet rögzíti, hogy az értékelési módszertan a NIST SP 800-53A Revision 5 szabványon alapul. Ez a keretrendszer strukturált, célorientált és objektív értékelést biztosít az információbiztonsági és adatvédelmi kontrollok tekintetében, az ún. determination statement struktúra mentén. Ennek ellenére az auditfolyamatban továbbra is meghatározó szerepet töltenek be a szubjektív tényezők, ezen tényezők általánosan elfogadottak, és minden audit sajátja.

A szubjektivitás természetes jelenléte az auditban

Noha a NIST SP 800-53A elviekben objektív megközelítést kínál, az audit gyakorlatában az alábbi szubjektív elemek elkerülhetetlenek:

- Az auditor szakmai megítélése: Az, hogy egy bizonyíték elegendő-e, vagy egy kontroll milyen mértékben teljesül, gyakran az auditor tapasztalatától és szakértelmétől függ.
- A szervezet kockázattűrési kultúrája: Ugyanazon technikai kontroll különböző szervezeti környezetben más-más súlyt kaphat.
- Tailoring lehetősége: a szabvány testreszabása hasznos rugalmasságot biztosít, ugyanakkor fokozza az értelmezési különbségek lehetőségét.

E tényezők miatt az audit következetessége és objektivitása kihívások elé néz, különösen az értelmezési és minősítési szakaszokban.

OSCAL: az objektivitás támogatása

A SZTFH előírta az OSCAL (Open Security Controls Assessment Language) formátum alkalmazását, amely gépi feldolgozásra alkalmas struktúrát kínál a kontrollok dokumentálására, értékelésére és megosztására. Az OSCAL célja az egységesítés, az átláthatóság és a visszakövethetőség biztosítása. Az audit trail OSCAL-formátumban történő vezetése csökkenti a szubjektív értelmezésből eredő torzulásokat, és lehetőséget nyújt a későbbi validálásra is.

Az alábbi módszerek alkalmazása segíthet a szubjektivitás negatív hatásainak csökkentésében:

- Többszintű szakmai review: Különböző auditorok vagy szakterületi szakértők bevonása az értékelésbe.
- Standardizált értékelési sablonok: Az értékelés formátumának egységesítése az interpretációs szabadság csökkentésére.
- OSCAL-alapú audit trail: a döntések strukturált és visszakereshető dokumentálása.
- Automatizált kontroll-ellenőrzések: Műszaki kontrollok automatikus validációja objektív eszközökkel.

- Bias-tudatosság fejlesztése: a szakemberek képzése és tudatosságuk növelése a kognitív torzítások felismerése érdekében.

Következtetés

Az auditfolyamatból a szubjektív tényezők teljes mértékben nem zárhatók ki, azonban megfelelő módszertani és technikai eszközökkel kontrollálhatók. a kulcs az átláthatóság, a dokumentálás és a közös értelmezési keret kialakítása. Az alábbi ajánlások betartása javíthatja az audit eredmények megbízhatóságát és összehasonlíthatóságát:

- Fókuszáljunk a kontrollok pontos megfogalmazására és a kapcsolódó elvárások világos rögzítésére.
- Vonjunk be több nézőpontot, több szakértőt – „több szem, többet lát”.
- Dokumentáljunk minden döntést és értelmezést – ez az egyik legjobb védelem audit során.

A professzionális audit sikerének záloga a strukturáltság, a konzisztencia és az emberi tényezők tudatos kezelése.

Audit megismételhetősége

Alapkövetelmény minden audit során, hogy megismételhető legyen, amely biztosítja, hogy ismételt auditálás során ugyanarra az eredményre jusson az audit. Ezt az elvet minden auditon alkalmazni szükséges.

10.5. Módszertani eltérések auditorok között

Az információbiztonsági kontrollok értékelésére vonatkozó szabályozási környezet az elmúlt években jelentős fejlődésen ment keresztül. Az SZTFH rendelet, valamint az általa hivatkozott NIST SP 800-53A Revision 5 egyaránt strukturált, célorientált keretrendszert biztosít a biztonsági kontrollok értékeléséhez. Ugyanakkor a gyakorlati megvalósítás során továbbra is jelentős módszertani eltérések tapasztalhatók az egyes auditorok között.

Az eltérések forrásai

A különbségek nem pusztán az auditorok egyéni stílusából fakadnak, hanem mélyebb tényezőkre vezethetők vissza, mint például:

- Szakmai tapasztalat és háttér – Egy technikai mélységben jártas auditor eltérő szempontokat vizsgál, mint egy irányítási rendszerre fókuszáló kolléga.
- Kockázati érzékenység – a szervezet kockázati kultúrájához való viszonyulás jelentősen befolyásolhatja az értékelést.
- Értelmezési gyakorlat – Azonos helyzetekben más-más minősítés is születhet az eltérő auditorlogikák következtében.

Egy gyakorlati példa: míg az egyik auditor a bizonyítékok részletes technikai elemzésére (például logfájlok validálására) összpontosít, addig egy másik auditor elsősorban a dokumentáció konzisztenciájára és folyamatok koherenciájára helyezi a hangsúlyt. a megoldás valahol kettő közötti egyensúly lesz.

Kritikus területek, ahol a módszertani különbségek megjelennek

A tapasztalatok alapján az eltérések leginkább a következő aspektusokban jelentkeznek:

- Bizonyíték elegendőségének és megfelelőségének megítélése,
- Részben teljesült kontrollok értékelése és súlyozása,
- Eltérések súlyosságának meghatározása a kockázat szerint,
- Jogszabályban előírt értékelési pont struktúrától való eltérés,

- Mintavételezés alkalmazása helyett vagy mellett minden egyes EIR-re és alrendszerre kiterjedő, teljes körű megfelelőség-bemutatás elvárása,
- Tailoring alkalmazása a szervezet sajátos kontextusához igazítva.

Ezek az eltérések különösen problémásak lehetnek nagyobb szervezetek esetén, ahol több auditor vagy auditáló szervezet dolgozik párhuzamosan, illetve idősoros értékeléseknél, ahol a korábbi auditokkal való következetes összehasonlíthatóság alapvető fontosságú. Az előzőekben említettek alapján tehát a szervezeti és az EIR szintű vizsgálatok esetén eltérések lehetnek a mélyebb megértésben.

A módszertani eltérések kezelési lehetőségei

Az értékelések következetességének és összehasonlíthatóságának fenntartása érdekében az alábbi módszertani és szervezeti eszközök alkalmazása javasolt:

- Belső benchmarkok és referenciaértékek kialakítása: Segít a szervezet-specifikus követelmények egységes értelmezésében.
- Minősítési kritériumok standardizálása: Az értékelési logika egységesítésével mérsékelhetők a személyes értelmezésekből fakadó eltérések.
- Peer-review és szerepkör-rotáció: a több szemlélet bevonása révén csökkenthető az egyéni torzítás.
- OSCAL-formátum alkalmazása (Hatóság által kötelezően elvárt): Az egységes dokumentáció elősegíti a transzparenciát és lehetővé teszi az auditértékelések utólagos elemzését és összehasonlítását.
- Megismételhetőség elvének fenntartása az auditok során.
- Auditor szervezet minőségbiztosítása az audit során.

Összegzés

Az auditorok közötti módszertani különbségek természetesek, de szabályozott keretek között hatékonyan kezelhetők. a strukturált értékelési modell, a sztenderdek következetes alkalmazása és a technikai eszközök (pl.: OSCAL) integrációja kulcsfontosságú az objektív, összehasonlítható és megbízható auditfolyamat megvalósításához.

A jövőbeni auditfolyamatokat támogató szervezeteknek törekedniük kell a folyamatos módszertani fejlődésre és a tapasztalatok intézményesített megosztására. Különös figyelmet kell fordítaniuk a megismételhetőség elvére, ezzel is stabil alapot biztosítani a módszertani megvalósításhoz.

10.6. Behatolás tesztelés (Pentesztekre) való felkészülés

Az audit részeként az auditor cég behatolás tesztelés (penteszt) elvégzését rendelheti el a szervezettől a magas biztonsági osztályba sorolt elektronikus információs rendszer esetében. Az auditor az ilyen tesztekre egy meghatározott időintervallumot jelöl meg, amelyen belül a vizsgálat bármikor elvégezhető, az előre egyeztetett paraméterek (pl.: érintett személyek, szervezeti egységek, technikai tartományok, eszközök) figyelembevételével. a pentesztekre a következő felkészülési lépések megtétele javasolt:

- Az auditor meghatározza, hogy melyik rendszereken végeznék el a vizsgálatot. Ezután a rendszer felelősével és IT üzemeltetőjével kell egyeztetnünk, hogy mikor végezhető el a vizsgálat – történhet e nap közben, vagy csak munkaidőn kívül, esetleg csak hétvégén. Megjegyzendő, hogy idő intervallumot határozhat meg az auditor, az intervallum alatt bármikor végezhetik a teszteket, az előre leadott

módokon (személy, sík, technikai tartomány, eszközök).

- Gyűjtsük össze a felelősök elérhetőségeit és azokat osszuk meg a tesztet végző etikus hackerrel. Ezekre akkor lehet szükség, ha kritikus sérülékenységet találnak. Ebben az esetben kérjük meg őket, hogy azonnal értesítsenek minket.
- A legbiztosabb megoldás a jogszabály és a jógyakorlat alapján, ha a rendszer rendelkezik UAT vagy DEV vagy TESZT környezettel – mely az éles környezet tükörképe, csak élő adatok nélkül – és megkérjük a pentesztert, hogy ezen a rendszeren végezze el a vizsgálatot. Fontos kiemelni, hogy a penetration tesztet végző személy a meghatározott kereteken belül végzi el a tesztelést, így megfelelően kell meghatározni a kereteket.
- Szükség lehet különböző szintű felhasználói fiókok létrehozására és biztosítására a tesztelők számára. Általában felhasználói szintenként 2-2 fiókot szoktak kérni (tehát pl.: 2 admin, 2 sima user).
- Amennyiben intraneten keresztül elérhető alkalmazásról beszélünk szükség lehet a VPN beállítások megosztására is, hogy a külső tesztelő elérje a belső hálózatot. Figyelni kell arra, hogy a vonatkozó szabályzóknak megfelelően kell kezelni ezt a jogosultság adást is így a jóváhagyásoknak végig kell menniük a szabályozott módon.
- Bizonyos biztonsági eszközök megkövetelhetik azok külső IP címjeik whitelist-re történő beregisztrálását, úgyhogy ilyen kérés is érkezhet a tesztet végzők részéről.
- A felkészülés részeként azt is egyeztessük le a rendszer felelőseivel, hogy a talált sérülékenységek javításához tervezzenek be fejlesztési időt – és a javításokat dokumentálják le, szabályozott változás követési folyamatot kell alkalmazni a javítási folyamat során. a legtöbb penteszter cég visszaellenőrzi a talált sérülékenységeket a javításuk után, amennyiben ez nem szerepelne a megállapodásban, akkor érdemes a javítások után visszaellenőrzést (aka. retest) kérni a penteszter cégtől, akik a korábban talált sérülékenységeket próbálják meg reprodukálni, és ha nem sikerül akkor biztosan kimondható, hogy sikerült megoldanunk őket. Fontos megjegyezni, hogy a javítási folyamat során előfordulhat, hogy újabb sérülékenységet viszünk be a rendszerbe, ezért mindenképpen ellenőrízni kell a rendszert.

10.7. Összeférhetetlenség

Az összeférhetetlenségről általánosságban

E jogintézmény mind a közjog, mind a magánjog által ismert fogalom, és alapvetően azt szolgálja, hogy bizonyos szerepkörökben, pozíciókban ne sérüljön a közbizalom és ne következzen be érdekösszeütközés. Lényege az, hogy egy szerepkörben lévő személy ne tölthessen be egyidejűleg több, egymással nem összeegyeztethető pozíciót.

Az összeférhetetlenség a közjogban is markánsan jelen van, pl.: az országgyűlési képviselő egyidejűleg nem lehet polgármester vagy gazdasági társaság tisztségviselője.

Az összeférhetetlenséget a magánjog is szabályozza az egyes eljárásjogokban, az ún. kizárás keretében.[52] a kizárás célja eljárásjogi értelemben, hogy megakadályozza az elfogultságot, vagyis olyan személy a döntéshozatalban ne vehessen részt, aki korábban már eljárt az ügyben, avagy más eljárásjogi pozícióban vett részt az eljárásban.

52 A polgári perrendtartásról szóló 2016. évi CXXX. törvény (a továbbiakban: Pp.) 12.§

Fontos, hogy az összeférhetetlenség tényét az érintettnek fel kell ismernie, és határidőben be kell jelenteni. Amennyiben erre nem, vagy nem határidőben kerül sor, a döntései hatálytalanok lesznek, továbbá köteles az összeférhetetlenséget elhárítani (pl.: tisztségről lemondani). Amennyiben az összeférhetetlenség megszüntetésére nem kerül sor, egy jogsértő állapot áll be, melyhez egyéb szankciók, jogkövetkezmények is társulhatnak (pl.: büntető-vagy fegyelmi eljárás, tisztség megszűnése stb.). Az hogy pontosan mik a jogkövetkezmények, azt az adott jogági szabályozás dönti el.

Az összeférhetetlenség, mint kritérium

Az auditorok összeférhetetlenségére kógens szabályok vonatkoznak, s több nemzetközi szabvány kifejezetten tartalmazza ezt a feltételt.

Az ISO/IEC 17021 szabvány megemlíti, hogy a tanúsító testületnek pártatlannak és függetlennek kell lenni, különösen attól a szervezettől, amit tanúsít. Ennek keretében nem nyújthat tanácsadást s kapcsolódó szolgáltatást, azon szervezetnek, amit auditál.

Ehhez hasonlóan az ISO 19011:2018 szabvány az audit módszertanok között rögzíti a függetlenséget, valamint a konfliktuskezelést (az auditor nem lehet az ellenőrzött rendszer tervezője, bevezetője, vagy működtetője). Az ISO/IEC 27006 megköveteli a független auditcsoportot, valamint a lehetséges érdekellentétek kizárását. Ezen nemzetközi példák is alátámasztják az auditori pozícióhoz kapcsolódó szigorú követelményeket: pártatlanság, függetlenség, objektivitás.

A függetlenség elemei

A függetlenség fogalma jogilag az alábbiakban ragadható meg: szervezeti, pénzügyi, szakmai függetlenség.

- A szervezeti függetlenség lényege, hogy az auditor nem függ a vizsgálat szervezettől, tehát attól szervezetileg elkülönült.
- A pénzügyi függetlenség lényege, hogy az auditornak nincs közvetlen anyagi érdekeltsége az auditált szervezet vonatkozásában.
- A szakmai függetlenség pedig azt jelenti, hogy az auditor a jogszabály által előírt metodikával, módszertannal dolgozik, és saját döntése alapján határozza meg a vizsgálat menetét.

NIS 2 és a függetlenség

A NIS 2 esetében az auditorokkal összefüggésben szinten felmerülhet a fenti dilemma. E körben a Kiberbiztonsági tv. 4. § 10. pontja kimondja: *„auditor: az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet.”* a definíció kifejezetten előírja a függetlenséget, mint alapvető kritériumot, és hangsúlyozza, hogy az auditor szervezet kell legyen, tehát magánszeméllyel az audit elvégzésére nem köthető szerződés.

Ehhez képest az auditorokkal kapcsolatos SZTFH rendeletek további részletszabályokat nem rögzítenek, vagyis a fenti dilemmára expressis verbis nem írnak elő egzakt jogi megoldást.

Az SZTFH rendelet [5] Preambulumbekezdése tartalmazza, mely szerint: *„A kiberbiztonsági audit célja, hogy egy független auditor vizsgálja meg azt, hogy az audittal érintett szervezetek elektronikus információs rendszerei mennyire ellenállóak a kiberbiztonsági fenyegetésekkel szemben.”*

Az SZTFH rendeletben több helyen felbukkan a „független” szó, azonban ennek részleteit nem fejti ki (pl.: függetlenség ellenőrzése, függetlenség megsértésének jogkövetkezményei stb.).

A 2/2025. (01.31.) SZTFH rendelet a felügyeleti díjakkal és az auditorok díjazásával foglalkozik, itt az auditorok jogállásáról nincs említés.

A 3/2025.(04.17.) SZTFH rendelet a kiberbiztonsági felügyeleti tevékenységhez kapcsolódó feladatellátás, valamint a hatósági ellenőrzés szabályait tartalmazza, tehát szintén nem tér ki az auditorok jogállására.

A dilemma

Mindezeket követően jogosan merül fel a dilemma: a NIS 2 auditorok esetében nem érvényesül az összeférhetetlenség elve?

A rövid válasz: nem. a vonatkozó jogszabályok ugyanis az összeférhetetlenségre vonatkozóan semmilyen részletszabályt, kizárást, szankciót jelenleg nem tartalmaznak. Ez azt jelenti, hogy a NIS 2 auditra kötelezett szervezet által felkért és leszerződött auditor tekintetében semmilyen összeférhetetlenségi kizáró ok nincs. Vagyis a választott auditor akár a szervezet NIS 2 felkészítését is elláthatja (itt a szervezet adott biztonsági osztálya szerinti auditjának elvégzésére jogosult auditorról van szó). a szakmai elvárások és az ISO szabványok egyaránt előírják, hogy ugyanaz a személy nem vehet részt mindkét folyamatban, ezért alapesetben a feladatot csak akkor lehet (illik) így ellátni, ha a szervezet megfelelő számú, felkészült szakemberrel rendelkezik.

A felek a szerződéses szabadság keretében szabadon rendelkezhetnek a megbízási szerződésükben a feltételekről, illetve az auditori megbízólevélben a részletekről, azonban a jogszabály a megállapodás részleteit a felek döntésére bízza.

Többekben felmerülhet a kérdés: ez mennyiben etikus, mennyiben kivitelezhető megoldás? Hiszen a felkészítést végző auditor nyilvánvalóan jól ismeri az auditált szervezet gyengeségeit, dokumentációját, amely egyrészről pozitív, hiszen az audit gyorsabb és eredményesebb lehet. Másrészről viszont mennyiben kerül veszélybe a pártatlanság és függetlenség elve, a szakmaiság, vagy esetlegesen az a cél, amely miatt a NIS 2 mint joganyag létrejött?

Ez egyelőre nyitott kérdés, megválaszolása a NIS 2 auditok lebonyolítását követően aktuális. Célszerű lenne azonban az ISO szabványcsalád alapján kialakított auditori függetlenségi modell bevezetése a NIS 2 auditok esetében is. Emellett hasznos javaslat lehet a jogalkotó irányában az összeférhetetlenség intézményének egyértelmű megfogalmazása is.

A gyakorlat és a szakmai elvárások

A kiberbiztonsági szabályozás egyik kulcseleme az auditori függetlenség kérdése 2026-ban is. A NIS 2 fontos alapelve ugyanis az információbiztonságban betöltött funkciók szétválasztása, vagyis a tevékenységek funkcionális elkülönítése. Ennek megfelelően az auditor nem ellenőrizheti saját tevékenységét, és nem lehet olyan szervezeti vagy üzleti kapcsolatban a vizsgált szervezettel, amely befolyásolhatja az objektív értékelést.

A gyakorlatban ez azt jelenti, hogy a felkészítést végző tanácsadó és az auditot végző szervezet szerepe elválik, valamint az auditor nem lehet az adott IT-biztonsági kontrollok kialakításában vagy üzemeltetésében érintett fél. Ez klasszikus összeférhetetlenségi helyzet, mivel az auditor saját munkáját értékelné.

Hasonló konfliktus merül fel akkor is, ha egy IT-biztonsági szolgáltató (például SOC vagy menedzselt biztonsági szolgáltató) az általa működtetett kontrollok megfelelőségét auditálná.

További kérdés, hogy a nagy tanácsadó- vagy audit hálózatok esetében mennyire tekinthető valódi függetlenségnek, ha a felkészítést és az auditot külön jogi személyek, de ugyanazon cégcsoport tagjai végzik. Ez a gyakorlat több országban – így Magyarországon is – jelenleg még szürke zónának számít, azonban várható az ezzel kapcsolatos jogértelmezés pontosítása, tekintettel arra, hogy a hatályos magyar jogszabályok az auditori összeférhetetlenségre nem tartalmaznak rendelkezést. Ennélfogva ezzel kapcsolatos joggyakorlat sem alakult még ki.

Az eddigi tapasztalatok alapján a legelfogadottabb megoldás, ha a felkészítést végző tanácsadó, az esetleges előauditot végző szakértő és a hivatalos auditot végző auditor külön, egymástól független szereplők. Ez biztosíthatja, hogy a kiberbiztonsági megfelelés értékelése objektív és hiteles legyen mind a szervezetek, mind az auditot felügyelő hatóság számára.

10.8. Audit riport értelmezése (JSON)

Az SZTFH a kiberbiztonsági auditok lezárását követően nemcsak a hagyományos, szöveges auditjelentés megküldését várja el az auditoroktól, hanem annak gépi feldolgozásra alkalmas, strukturált változatát is.[53] Ennek célja az, hogy az auditjelentések egységes szerkezetben, összehasonlítható módon, automatizáltan is feldolgozhatók legyenek a hatósági oldalon. Fontos hangsúlyozni, hogy ez a formátum elsődlegesen nem az auditált szervezetek számára készül, hanem az auditorok adatszolgáltatási feladatának része. Ugyanakkor a szervezetek a gyakorlatban találkozhatnak ezzel a struktúrával, megkaphatják azt, vagy ellenőrzési, egyeztetési, illetve dokumentációs célból betekinthetnek abba. Éppen ezért indokolt röviden, de szakmailag pontosan bemutatni, hogy mit tartalmaz ez a JSON-formátum, milyen logika szerint épül fel, és hogyan kapcsolódik a tényleges auditjelentéshez.

A jelentés specifikációjának alapja az OSCAL, azaz az Open Security Controls Assessment Language nevű nyílt szabványú leíró nyelv, amelyet kifejezetten arra alakítottak ki, hogy a követelmények, az értékelések, a megállapítások és a kapcsolódó bizonyítékok egységes, strukturált és automatizáltan feldolgozható formában legyenek rögzíthetők.

Az OSCAL[54] több, egymáshoz kapcsolódó sémából áll, amelyek a megfelelőség és az audit különböző szintjeit fedik le. A Catalog a kontrollok katalógusát tartalmazza, vagyis azt, hogy milyen követelményeknek kell megfelelni. A Profile ennek testreszabott változata, amely az adott szabályozási vagy szervezeti környezetben releváns kontrollokat emeli ki. A System Security Plan a rendszer biztonsági felépítését és kontrolljait írja le. Az Assessment Plan az audit vagy értékelés tervét rögzíti. Az Assessment Results az audit során keletkező tényleges eredményeket foglalja strukturált egységbe. A Plan of Action and Milestones pedig az azonosított hiányosságok kezelésére szolgáló intézkedéseket és ütemezést tartalmazza.

Az Assessment Results kiemelt jelentősége abban áll, hogy az auditori megállapításokat nem pusztán szöveges beszámolóként, hanem egységes adatmodellként rendezi össze. Ez biztosítja, hogy a különböző auditorok által készített jelentések összehasonlíthatók legyenek, a vizsgálatok logikája visszakövethető maradjon, és a hatóság az adatokat ne kizárólag egyedi dokumentumokként, hanem strukturált adathalmazként is értelmezni tudja. Az Assessment Results formátum tipikusan tartalmazza az auditban érintett elektronikus információs rendszerek jellemzőit, a dokumentumvizsgálat, interjú és tesztelés eredményeit, az észlelt kockázatokat, a követelmények teljesülési állapotát, valamint mindazon bizonyítékokat, amelyek az auditjelentésben szereplő értékelést alátámasztják. Az SZTFH számára ez azért bír jelentőséggel, mert ugyanazon logika mentén épülnek fel az egyes jelentések, így az auditok tartalma, terjedelme, minősítése és eredményrendszere sokkal könnyebben összevethető.

Az alábbiakban bemutatásra kerül egy JSON-példa, ami ezt a logikát követi. A legfelső szinten az assessment-results objektum foglalja

53 https://sztfh.hu/downloads/kiberbiztonsag/kiberbiztonsagi_auditjelentes_gepi_feldolgozasra_alkalmas_formatuma_sztfh.pdf [Letöltve: 2026. 04. 02.]

54 https://pages.nist.gov/OSCAL/

össze az auditjelentés egészét, vagyis ez a gyűjtőelem tartalmazza a metaadatokat, a konkrét audit-eredményeket és a háttéranyagokat. Már ezen a szinten is látható, hogy a formátum nem egyszerű melléklet, hanem egy önálló adatszerkezet, amely az audit folyamati, szervezeti és szakmai összetevőit is egyetlen egységes modellbe rendezi. Az itt szereplő egyedi azonosító (uuid, például: 26a53d2c-4249-4e0c-9939-410590f3ae9e) azt biztosítja, hogy az adott auditfájl önállóan azonosítható és nyomon követhető legyen.

A metadata rész az auditjelentés alapadatait írja le. Ide tartozik a cím (title, például: „[Szervezet neve] 7/2024. (VI. 24.) MK rendelet audit jelentés"), a létrehozás és módosítás időpontja (published, last-modified, például: 2024-09-24T02:24:00Z), a dokumentumverzió (version, például: 1.0) és az alkalmazott OSCAL-verzió (oscal-version, például: 1.1.3). Ezek a mezők azt a célt szolgálják, hogy a jelentés adminisztratív és technikai értelemben is beazonosítható, veriózható és időrendben követhető legyen. A metadata.props mezőben olyan további tulajdonságok is megjelennek, amelyek a hazai specifikációhoz kapcsolódnak, például a jelentés típusa (type, például: 7/2024. (VI. 24.) MK rendelet) vagy az audit egyedi azonosítója (id, például: [Szervezet neve] 2025 audit).

A metadata részen belül a roles blokk az audit során értelmezett funkcionális szerepköröket sorolja fel. Itt nem konkrét személyek vagy szervezetek jelennek meg első körben, hanem olyan szerepek, mint a felügyeleti hatóság (*authority*), az auditor szervezet (*assessor*), az auditorcsapat (*assessment-team*), az auditvezető (*assessment-lead*), a sérülékenységvizsgálati csapat (*vulnerability-test-team*), a sérülékenységvizsgálat vezetője (*vulnerability-test-lead*), az auditált szervezet (*organization*) vagy a szervezet auditfelelősei (*organization-team*). Ennek az a jelentősége, hogy a JSON különválasztja a szerepkört attól, hogy azt konkrétan ki tölti be. Ez később lehetővé teszi, hogy a szerepkörökhöz külön lehessen hozzárendelni a szervezeteket és személyeket.

A *locations* tömb a releváns fizikai helyszíneket tartalmazza. Ilyen lehet az auditor telephelye, a szervezet telephelye vagy az EIR mögött álló adatközpont (például: „Auditor telephelye", „A szervezet telephelye", „Adatközpont"). A helyszínek strukturált címadatokkal szerepelnek, és további tulajdonságokkal is kiegészíthetők, például megadható, hogy általános irodai helyszínről vagy elsődleges adatközpontról van szó (type: office, illetve value: data-center, class: primary). Ez azért fontos, mert a későbbi audit megfigyelések már közvetlenül hivatkozhatnak ezekre a helyszínekre, például egy fizikai helyszíni vizsgálat esetében.

A parties blokk a konkrét szereplőket tartalmazza, vagyis azokat a szervezeteket és személyeket, akik az auditban valamilyen módon részt vesznek. Itt külön elemként jelenik meg az auditor szervezet (például: „[Az auditor cég hosszú neve]"), az auditált szervezet (például: „[A szervezet hosszú neve]"), maga a hatóság („Szabályozott Tevékenységek Felügyelete"), továbbá az auditorok és a szervezet részéről közreműködő személyek is (például: „[Auditor 1] neve", „[A szervezet 2. munkatársának] neve"). Minden ilyen szereplő saját egyedi azonosítót kap, megadható a típusa (organization vagy person), kapcsolati adatai, telephelye, valamint személyek esetében az is, hogy mely szervezet tagjai. A props mezőkben itt jelenik meg például a munkakör is (job-title, például: auditor, pentester, biztonsági tisztviselő). Ez teszi lehetővé, hogy a jelentés ne csak szervezeti, hanem személyi szinten is visszakövethető legyen.

A responsible-parties blokk kapcsolja össze a korábban definiált szerepköröket a konkrét szervezetekkel és személyekkel. Itt válik láthatóvá, hogy ki tölti be az egyes funkciókat, vagyis például melyik szervezet a felügyeleti hatóság, melyik cég az auditor, kik alkotják az

auditorcsapatot, ki az auditvezető, kik vettek részt a sérülékenységvizsgálatban, illetve kik a szervezet kijelölt auditfelelősei. Például az assessment-lead szerepkörhöz a minta szerint az egyik auditor személye van hozzárendelve, míg az organization-team szerepkör alatt a szervezet két munkatársa jelenik meg. Ez a szerkezet jól mutatja, hogy a JSON alapvetően relációs szemléletű, azaz a szereplők és a szerepek külön léteznek, és hivatkozásokon keresztül kapcsolódnak egymáshoz.

Az import-ap mező arra utal, hogy az eredmény egy korábban definiált audit- vagy értékelési tervhez kapcsolódik. Ez azt jelzi, hogy az auditjelentés nem önmagában áll, hanem egy előzetesen meghatározott auditkeret vagy auditálási terv alapján jött létre. A gyakorlatban ez azt támogatja, hogy az eredmények összevethetők legyenek azzal, amit eredetileg az audit céljaként, tárgyaként vagy módszertanaként meghatároztak.

A tényleges audit-eredmények a results tömbben jelennek meg. Egy ilyen elem már a konkrét auditfutás szakmai tartalmát hordozza, azaz saját azonosítója, címe, rövid leírása, valamint időintervalluma van (title, description, start, end; például: „2025 NIS2 audit jelentés”, „Az audit jelentés rövid leírása”, 2025-03-01T00:00:00Z – 2025-03-12T00:00:00Z). Ez a blokk tehát már nem az adminisztratív keretet, hanem az audit gyakorlati eredményeit rögzíti.

A results részen belül a local-definitions blokk az audit során használt, lokálisan definiált vizsgálati objektumokat tartalmazza. Ennek egyik legfontosabb eleme a components tömb, amelyben a vizsgált elektronikus információs rendszerek vagy rendszerelemek szerepelnek (például:”EIR 1 név” és „EIR 2 név”. Mindkettő EIR külön azonosítóval, leírással, típussal és működési állapottal rendelkezik (type: system, status.state: operational). A hozzájuk kapcsolt tulajdonságok különösen fontosak. Itt adható meg a biztonsági vagy kockázati szint (risk-level: alap, jelentős, illetve magas), az alkalmazott kontrollkatalógus és profil, az üzleti cél, valamint a besorolási indoklás (business-domain, reasoning). A kritériumszintű indoklások (2.2.2.1.reasoning, 2.2.3.5.reasoning stb.) azt a célt szolgálják, hogy ne csak maga a besorolás, hanem annak konkrét szakmai megalapozása is dokumentált legyen az MK rendeletben foglalt elvárások mentén.

A local-definitions másik fontos eleme az inventory-items tömb, amely a komponensekhez kapcsolódó konkrét technikai vagy nyilvántartási elemeket tartalmazza. Ilyen lehet egy külső IP-cím, egy adatbázis-kezelő hoszt vagy egy szerver (például: „A szervezet külső IP címe”, „A szervezet MSSQL adatbázis kezelője”, „A szervezet Windows 2019 servere”). A komponensek és az inventárium-elemek közötti különbség lényeges. A komponens jellemzően egy magasabb szintű audit objektum, míg az inventárium-elem annak konkrét technikai megjelenése vagy erőforrása. Ez a szétválasztás azért hasznos, mert így az auditmegfigyelések és a bizonyítékok pontosabban hozzárendelhetők a megfelelő szinthez.

A reviewed-controls blokk mutatja meg, hogy az auditor mely követelményeket és kontrollcélokat vizsgálta az egyes komponensek esetében. A control-selections részben például lehetséges, hogy az egyik EIR-re minden követelmény alkalmazandó, kivéve két kizárt követelménycsoportot (például: 2.2. és 4.1.), amelyekhez az auditor indokolást is rögzíthet (például: „A 2.2. követelménycsoport kizárható, mivel…”). Ha egy EIR esetében nem történt kizárás, ott minden követelmény része a vizsgálatnak. Ez a blokk tehát nemcsak a vizsgálati kört írja le, hanem annak határait és az esetleges kizárások szakmai indokait is. A control-objective-selections rész ugyanennek a logikának a részletesebb, kontrollcél-szintű leképezése.

Az attestations blokk az auditból származó összesített értékeléseket tartalmazza. A mintában ezen belül szerepelnek a pontszámok, például a szervezet egészére vonatkozó SZEKI

érték (score: 90), valamint az egyes EIR-ekhez kapcsolódó VMI értékek (score: 92, illetve 88). E pontszámok nem önálló számokként jelennek meg, hanem mindig valamilyen szervezethez vagy komponenshez kapcsoltan, ami biztosítja, hogy az értékelés kontextusa egyértelmű maradjon. Ez a rész jól mutatja, hogy a JSON nemcsak kvalitatív megállapításokat, hanem számszerűsített audit-eredményeket is kezelni tud.

Az assessment-log az auditfolyamat időbeli lenyomata. Olyan lépések jelennek meg benne, mint az audit terv elkészítése, a terv felülvizsgálata, dokumentáció-áttekintés, interjúk lefolytatása, technikai tesztelés, sérülékenységvizsgálat, kockázati táblázat összeállítása vagy a jelentés tervezetének és végleges változatának elkészítése. Ez a blokk biztosítja, hogy az audit nemcsak eredményoldalról, hanem folyamatoldalról is rekonstruálható, vagyis látható, milyen fő lépések mentén zajlott le az értékelés.

Az observations blokk az audit során keletkezett konkrét megfigyelések, vizsgálati tapasztalatok és bizonyítási pontok nyilvántartására szolgál. Itt szerepelhet dokumentum-átvizsgálás, interjú, sérülékenységvizsgálat, helyszíni audit vagy technikai script-futtatás eredménye. Például készülnie kell külön observation az EIR-besorolás felülvizsgálatáról, illetve a vizsgálati típusonként külön-külön observation a szabályzatok átvizsgálásáról, az interjúról, az automata sérülékenységvizsgálati jelentésről, a fizikai auditról vagy az audit script eredményeiről. Minden observation tartalmazhat címet, leírást, módszert (EXAMINE, INTERVIEW, TEST), típust, eredetet, érintett tárgyakat és kapcsolódó bizonyítékokat. Ez a réteg azért különösen fontos, mert az audit szakmai állításai nem közvetlenül a végső megállapításból születnek meg, hanem először valamilyen megfigyelés vagy vizsgálati cselekmény történik, és az abból levont következtetés jelenik meg a későbbi megállapításokban.

Az observations belső szerkezete jól mutatja a JSON erősségét. Egy dokumentumvizsgálati observation hivatkozhat például egy szabályzatra mint bizonyítékra (IBSZ), miközben a vizsgálat tárgya maga a komponens vagy a szervezeti működés egy része. Egy interjú-observation konkrét személyekhez kapcsolható (subject-uuid), és interjújegyzőkönyvre mint bizonyítékra hivatkozhat. Egy technikai observation egyszerre érinthet inventárium-elemet és komponenst is, vagyis pontosan megmutatható, hogy egy adott IP-címen, szerveren vagy adatbázis-kezelőn végrehajtott teszt mely rendszerkörnyezethez kapcsolódott. Ez a modell a bizonyítékok és a megfigyelések közötti kapcsolatot átláthatóan és visszakereshetően rögzíti.

A risks blokk az audit során azonosított kockázatokat tartalmazza. Ezek a kockázatok már nem puszta technikai észrevételek, hanem olyan értékelt objektumok, amelyek leírják, hogy egy adott hiányosság vagy követelmény-nemteljesülés milyen hatással van a vizsgált rendszerre.

A findings blokk az audit végső szakmai megállapításait jeleníti meg. Ezek a megállapítások egy adott követelménycsoportra vagy egy konkrét kontrollcélra vonatkoznak, és azt mondják ki, hogy az adott elem teljesült-e vagy sem. A target rész határozza meg, hogy a megállapítás pontosan mire vonatkozik, a status.state pedig azt, hogy az eredmény megfelelő (satisfied) vagy nem megfelelő (not-satisfied).

Különösen fontos, hogy a findings elemek nem önmagukban állnak, hanem visszahivatkoznak az őket alátámasztó megfigyelésekre (related-observations) és – ahol releváns – a kapcsolódó kockázatokra (related-risks). Ez biztosítja a teljes auditnyomvonal visszakövethetőségét. A hatóság és az érintett szervezet számára így nemcsak a végkövetkeztetés látható, hanem annak bizonyítási lánca is (milyen megfigyelésből, milyen módszerrel, milyen bizonyíték alapján és milyen kockázati kontextusban született meg az adott minősítés).

A back-matter blokk a hivatkozott erőforrásokat és evidenciákat foglalja össze. Ide

tartozhatnak a vonatkozó jogszabályok, szabályzatok, interjú jegyzőkönyvek, képernyőképek, technikai vizsgálatok eredménye vagy más bizonyítékok. Egy átlagos kicsit érettebb szervezet JSON-jében külön erőforrásként szerepel a 7/2024. (VI. 24.) MK rendelet, az 1/2025. (I. 31.) SZTFH rendelet, az Interjú jegyzőkönyv, fizikai biztonsági szemle eredménye, az IBSZ és más szabályzatok, eljárásrendek, képernyőképek, esetleg script- és sérülékenységvizsgálati riportok. Ezekhez az auditor típust, osztályt, verziót, közzétételi időpontot, médiaformátumot és hash-értéket is rendelhet, hogy a bizonyítékok nemcsak tartalmilag, hanem formai és integritási szempontból is nyomon követhetők maradnak.

Összességében a hatóság által elvárt JSON nem egyszerűen egy technikai fájlformátum, hanem a teljes auditfolyamat strukturált reprezentációja. Egyszerre szolgál adminisztratív, szakmai, bizonyítási és feldolgozhatósági célokat. Az auditorok számára azért kötelező ennek alkalmazása, mert ez teszi lehetővé az egységes riportkészítést, a jelentések összehasonlíthatóságát, a gépi feldolgozhatóságot, a verziókövetést és a dokumentumok későbbi ellenőrizhetőségét. A szervezeteknek ugyan nem ez az elsődleges munkadokumentumuk, mégis hasznos megérteniük a szerkezetét, mert ebből pontosan látható, hogy a hatósági szempontból releváns auditjelentés milyen információkból, milyen logika szerint és milyen bizonyítási lánccal épül fel.

Fontos megjegyezni, hogy a JSON akkor töltheti be igazán az összehasonlítási, trendelemzési funkcióját, ha az auditorok közel azonos pontossággal, lelkiismerettel, hozzáállással hajtják végre az auditokat. Ez az első auditálási ciklusban a tapasztalatok alapján nem teljesen valósult meg. Ennek ellenére a formátum egy jó keretet ad a fejlődésre, éppen ezért érdemes az érintett szervezeteknek is megismerni a sajátjuk tartalmát, amennyiben erre van lehetőségük.

10.9. Eddigi audittapasztalatok

Minden egyes felkészítő cég a saját tudása, tapasztalata alapján javasol valamilyen felkészülési módszert, amivel igyekszik rávezetni az érintett céget a megfelelő szabályozásra és a működés bizonyítására. A két legszélsőségesebb eset az, amikor az adott kontrollcsoport összességére vonatkozó kidolgozandó megvalósítás jelentkezik igényként, míg a másik szerint az elemi követelmények szintjén kell megfelelő bizonyítékot mutatni az adott kontrollcsoport elvárásaira. Míg az előbbi egy “beszédes” mikrokörnyezet leírását kéri, az utóbbi a “szőrszálhasogatás” mezejére csúszik át.

A kérdés: mi fogja az eredményt megmutatni? Sajnos – vagy szerencsére – az utóbbi. Az auditornak nincs – vagy nem szabadna legyen – döntési bizonytalansága, ha egy egyértelmű kérdés elhangzik és arra egyértelmű válasz érkezik. Mi a leggyakoribb hiba? A szabályzat vagy a megvalósulási nyilatkozat megfogalmazása. Akár sablon alapján készül a dokumentáció, akár saját erőforrásból, AI segítségével, a következő elvárás-válasz párosítás nem fog megfelelni az elvárásoknak:

- Elemi követelmény: meghatározták az adott szabályzat felülvizsgálatáért felelős személyt – név és beosztás – vagy szerepkört.
- Megvalósulás: Szervezetünk a NIS 2 előírásai alapján kijelölte és meghatározta azt a személyt illetve szerepkört, amely felelős az érintett szabályzat felülvizsgálatáért.
- Szabályzat: A Szervezetben az IBF a felelős az adott szabályzat felülvizsgálatáért felelős személy vagy szerepkör meghatározásáért.

Ha netán van egy újabb hivatkozás egy olyan bekezdésre, dokumentumra, rendszerre vagy akár egy RACI mátrixra, ahol egyértelműen azonosítható az adott személy vagy szerepkör, akkor ezzel nincs is probléma, de rendszerint se hivatkozás, se meghatározás nem található. Így ez a rekord, ez az elemi követelmény nem teljesült. Általában ez a P1 jelölésű követelmények (kulcsok) egyike.

Ebből adódóan, ha három sorral alább az az elemi követelmény, hogy "a P1 szerint meghatározott személy vagy szerepkör felülvizsgálta a P2 szerinti gyakoriság szerint a szabályzatot", eleve nem teljesíthető, hiába van becsatolva bizonyítékként egy felülvizsgálati jegyzőkönyv, ha nem azonosítható a jóváhagyó személyének jogosultsága.

Mi lett volna a helyes szabályozás: A szabályzatot az IBF köteles minimum évente egyszer felülvizsgálni.

A megfelelő szabályzatok megléte önmagában nem elegendő. Valódi, gyakorlati teszt-bizonyítékok benyújtása is szükséges. A következő esetek a gyakorlatban rendszeresen előfordulnak:

- Hiányzó bizonyíték. A jelenlegi formában ez nem értékelhető, így egyértelműen nem felelt meg. Előfordulhat azonban, hogy a bizonyíték feltöltésre került, csak a fájlban hiányzik a rá mutató hivatkozás. Amennyiben az auditor ezt azonosítani tudja, vagy egyéb, korábbi vagy későbbi, releváns bizonyítékot talál, az elfogadhatóvá válhat.
- Egy darab, a követelmény szempontjából teljes mértékben irreleváns bizonyíték került benyújtásra, amely így szintén nem felelt meg. Előfordulhat, hogy az auditor időt fordít annak értelmezésére, hogy a szervezet milyen megfontolás alapján nyújtotta be az adott bizonyítékot, azonban amennyiben ez nem állapítható meg, vagy a bizonyíték nyilvánvalóan nem kapcsolódik a követelményhez, az adott pont nem fogadható el.
- Egyetlen, 70+ oldalas jegyzőkönyv vagy kimutatás kerül benyújtásra, amely gyakran nem kereshető, szkennelt formátumban áll csak rendelkezésre. Ez jelentősen megnehezíti az értékelést, mivel az auditornak a teljes dokumentumot át kell tekintenie annak megállapításához, hogy tartalmaz-e releváns információt például annak igazolására, hogy az alkalmazott tűzérzékelő rendszereket független energiaforrás támogatja. Ehhez nem feltétlenül megfelelő egy Tűzvédelmi Szabályzat, amennyiben az erre vonatkozóan nem tartalmaz konkrét utalást. Ez a hiányosság azonban jellemzően csak a dokumentum részletes átvizsgálása során derül ki.
- Egy darab, megfelelő bizonyíték került benyújtásra. Például, ha az elvárás az, hogy a főelzáró csapok megközelíthetőek legyenek, egy akadályoktól mentes csapot ábrázoló fénykép elegendő igazolásnak minősül. Ez az eset egyértelműen megfeleltnek tekinthető, és ellenőrzése ideális körülmények között legfeljebb néhány másodpercet vesz igénybe.
- Több (például 10) bizonyíték került benyújtásra, amelyek közül kilenc irreleváns, és mindössze egy tekinthető megfelelőnek. A fájlok elnevezése az elemi követelmények hivatkozási számai alapján történt, azonban ezek megnyitásig nem teszik egyértelművé a tartalmukat. Ez különösen problémás lehet nagy méretű (például 200 MB-ot meghaladó) fájlok esetén, ahol a releváns bizonyíték azonosítása jelentős időráfordítást igényel, és hosszabb távon az auditor számára is frusztrálóvá válhat. Figyelembe véve, hogy az audit során közel 100 szervezeti, valamint EIR-enként további mintegy 200 teszt-bizonyíték áttekintése

szükséges, az ilyen jellegű benyújtás jelentősen növeli a feldolgozási időt. Bár az auditor feladata a releváns bizonyítékok kiválasztása, a túlzott mennyiségű, nem megfelelően strukturált dokumentáció kedvezőtlenül befolyásolhatja az értékelés hatékonyságát. Egy-egy ilyen eset akár több percet is igénybe vehet rekordonként, ami összességében számottevő időveszteséget eredményezhet és az auditor szubjektív értékelése ilyenkor negatívan befolyásolhatja az értékelés eredményét.

- Több bizonyíték került benyújtásra, azonban egyik sem tekinthető megfelelőnek. Előfordulhat, hogy egyes fájlhivatkozások tévesen kerülnek hozzárendelésre, ami jellemzően adminisztrációs hibára vezethető vissza. Ilyen esetekben az auditor megkísérelheti a feltöltött dokumentumok között a releváns bizonyíték azonosítását, azonban ez ismételt időráfordítást igényel, különösen, ha többszöri próbálkozás sem vezet eredményre. Tapasztalható továbbá olyan helyzet is, amikor következetesen nem megfelelő bizonyítékok kerülnek benyújtásra, mintha egyetlen jegyzőkönyv – annak tényleges tartalmától függetlenül – egy teljes kontrollcsoport lefedésére alkalmas lenne. Ez a megközelítés nem megalapozott, így az adott követelmény nem tekinthető teljesítettnek. Az utóbbi esetek jellemzően akkor fordulnak elő, ha a szervezet nem rendelkezik megfelelő tudással és tapasztalattal az auditbizonyítékok előkészítéséhez, illetve nem vesz igénybe külső szakértői támogatást vagy felkészítést.

A fentiek alapján egyértelműen kirajzolódik, hogy milyen jellemzőkkel bír az ideális bizonyíték-szolgáltatás:

- Szabályzó dokumentum esetén elegendő a szabályzat neve vagy azonosítója, valamint az érintett fejezet, bekezdés (szükség esetén oldalszám) pontos megjelölése. Amennyiben az adott kérdésre a válasz egyértelműen megtalálható a hivatkozott részben, nem indokolt további szabályzatok, fejezetek vagy bekezdések megadása pusztán azért, mert azok logikailag kapcsolódnak az adott kontrollhoz. Például, ha a kérdés arra vonatkozik, hogy ki jogosult a rendszerelemek telephelyről történő elszállításának engedélyezésére, elegendő az erre vonatkozó IBSZ-fejezet megjelölése; nem szükséges külön feltüntetni a Fizikai Biztonsági Szabályzat kapcsolódó részeit is.
- Írásbeli interjú (amennyiben rendelkezésre áll) esetén, azon túl, hogy egy-egy kiemelt kontrollcsoporthoz kapcsolódó kérdések megválaszolásra kerülnek, a dokumentum lehetőséget biztosít kiegészítő magyarázatok rögzítésére is. Ez különösen hasznos olyan esetekben, amikor egy adott kontroll teljesülését olyan körülményre vonatkozóan kellene igazolni, amely a gyakorlatban még nem következett be. Ilyen lehet például, ha a rendszeres felülvizsgálati időszak a bevezetés óta még nem telt le, vagy nem történt olyan esemény, illetve körülményváltozás, amely soron kívüli felülvizsgálatot indokolt volna. Ezekben az esetekben a helyzet részletesen kifejthető az írásbeli interjú keretében, amelyet az auditor figyelembe vesz. Amikor az adott elemi követelmény értékelésére kerül sor, az auditor elfogadhatja, hogy az adott körülmények miatt nem áll rendelkezésre konkrét bizonyíték.
- Tesztbizonyítékok esetén célszerű a lehető legkevesebb, kizárólag az adott elemi követelmény teljesítéséhez szükséges és releváns bizonyítékot benyújtani. Amennyiben a bizonyításhoz terjedelmes dokumentum (például többoldalas anyag), nagy méretű strukturált fájl (például több

száz soros XML), vagy mély szakmai tartalom (például hálózati eszköz konfigurációját bemutató képernyőkép) szükséges, javasolt egyértelműen megjelölni a releváns részeket. Ez történhet kommentekkel vagy vizuális kiemeléssel annak érdekében, hogy az auditor gyorsan és egyértelműen azonosítani tudja a szükséges információt.

- Paraméterérték esetén az elemi követelmény meghatározza, hogy egy vagy több opció közül szükséges választani (adott esetben egy másik elemi követelményben definiált eset vagy eszköz alapján). Lényeges, hogy a szabályozás minden esetben a ténylegesen választott paraméterhez igazodjon. Például előfordulhat, hogy OT környezetben a túlzott erőforrás-terhelés vagy a magas számú fals pozitív riasztás miatt az aláírás alapú vírusellenőrzés szándékosan ki van kapcsolva. Ilyen esetben a választott paraméter a nem aláírás alapú vizsgálati módszer, amelynek megfelelően ennek kell megjelennie a szabályozásban is. Fontos továbbá, hogy az ilyen döntések minden esetben alátámasztásra kerüljenek megfelelő kockázatelemzéssel és/vagy kompenzáló kontrollok alkalmazásával.

A megfelelő szint (SZEKI) eléréséhez elengedhetetlen, hogy a szervezet minden egyes elemi követelményt megértsen és megfelelően megválaszoljon. Rengeteg, tényleg rengeteg az adminisztráció, de jelen helyzetben ez elengedhetetlen.

11

Ellátási lánc biztonsága

A digitális tér egyre bővülő összefonódásával az ellátási láncok is összetettebbé és sérülékenyebbé váltak különösen a kritikus ágazatokban. a NIS 2 irányelv egyik fontos újítása, hogy az ellátási lánc biztonságát nem csupán kiegészítő szempontként, hanem a kiberreziliencia központi elemként kezeli. a cél világos, a szervezet biztonsági szintjét nem veszélyeztethetik a külső kapcsolatok sem, legyen szó beszállítókról, szolgáltatókról, alvállalkozókról vagy egyéb partnerekről. Számos korábbi kibertámadás bizonyította, hogy a támadók gyakran nem közvetlenül a célpontot, hanem annak kiszolgáltatott partnereit támadják, így szerezve hozzáférést érzékeny rendszerekhez vagy adatokhoz. Ezek az ún. „supply chain” vagy „third-party” támadások sok esetben nehezen észlelhetők, feltárásuk és elhárításuk komoly reputációs és pénzügyi károkat okozhat. Ez a fejezet azt mutatja be, hogyan lehet a fentiek fényében szerződéses, kockázatkezelési és operatív szempontból megfelelően kezelni az ellátási lánc biztonságát, és miként válhat mindez az üzleti stabilitás és az ügyfélbizalom egyik kulcsfontosságú tényezőjévé.

11. Ellátási lánc biztonsága

Írták: dr. Albert Ágota, Cseh Patrik, Cserháti Vencel, dr. Jeney Andrea, Major Róbert, Máté Márk, Végh András

11.1. Meglévő szerződések felülvizsgálata

A NIS 2 kockázatalapú megközelítése nemcsak az új szerződéseink kötelező védelmi intézkedésekhez "igazítását" követeli meg, hanem a már meglévő szerződéseink felülvizsgálatát is.

Szerződések információbiztonsági követelményei

A meglévő szerződéseink felülvizsgálatának első lépése, hogy minden dokumentumban egyértelműen szerepeljenek az információbiztonsági követelmények, különösen, ha a beszállító /üzleti partner EIR-hez fér hozzá, illetve személyes adatokat kezel. a felülvizsgálat során ellenőriznünk szükséges, hogy a szerződések tartalmazzák-e:

- a biztonsági intézkedések minimum szintjét
- a hozzáférés-felügyelet szabályait
- a titoktartási kötelezettségeket
- a naplózásra, monitoringra vonatkozó elvárásokat
- az adatvédelmi megfelelést a GDPR, illetve nemzeti szabályozások alapján.

Az MK rendelet 16.7. védelmi intézkedése tartalmazza, a beszerzési folyamataink során – beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is – a szerződéseinkben egységes nyelvezetet kell alkalmaznunk, továbbá a szerződésekbe konkrétan milyen követelményeket kell rögzítenünk.

Alvállalkozókra vonatkozó szabályok

Az ellátási lánc biztonságának kulcseleme, hogy ne csak a közvetlen szerződött partnerekre, hanem azok alvállalkozóira is kiterjedjenek a biztonsági követelmények. Ennek során át kell tekintenünk:

- van-e az adott szerződésben tiltás vagy korlátozás alvállalkozók igénybevételére;
- van-e kötelezettség az alvállalkozók írásos előzetes bejelentésére és jóváhagyására;
- az alvállalkozóknak ugyanazon biztonsági és adatvédelmi követelményeket kell-e teljesíteniük, mint a közvetlen beszállítónak;
- kötelezőek-e back-to-back (visszavonatkoztatott) szerződéses kötelezettségvállalások;
- van-e kötelezettség arra, hogy a közvetlen közreműködő harmadik fél bevonása esetén erről előzetesen értesítse a megrendelőt;
- biztosított-e, hogy a bevont harmadik fél is teljesíti a közvetlen közreműködőre vonatkozó, előírt biztonsági és technológiai követelményeket (például hálózatbiztonság, hozzáférés-kezelés, adatvédelem).

Az MK rendelet 16. védelmi intézkedéscsoportjában megtaláljuk azokat a követelményeket, amelyeket a beszerzéseink során érvényesítenünk kell attól függően, mely osztályba soroltuk az adott EIR-t, így például meg kell követelnünk

- a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását („alap", 16.8.);
- a szolgáltatási szerződés alapján igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezetünk elektronikus információbiztonsági követelményeinek, és a szervezetünk által meghatározott védelmi intézkedéseket alkalmazzák („alap", 16.49.);

- az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási információkat a védelmi intézkedésekhez. Ezek az információk tartalmazzák a biztonsági szempontból releváns külső rendszerinterfészeket, a magas szintű rendszertervet, az alacsony szintű rendszertervet, a forráskódot vagy a hardversémákat, valamint a szervezet által meghatározott részletes tervezési és megvalósítási információkat („jelentős”, 16.9.);
- a fejlesztőtől, szállítótól, hogy határozza meg a használatra tervezett funkciókat, portokat, protokollokat és szolgáltatásokat („jelentős”, 16.13.) stb.

Az alvállalkozók esetében is fontos kiemelni, amennyiben azok személyes adatokat is kezelnek, a GDPR 28. cikke előírja, hogy az adatfeldolgozó (a szerződött partnerünk) az adatkezelő (azaz a mi) előzetesen írásban tett eseti vagy általános felhatalmazásunk nélkül további adatfeldolgozót (alvállalkozót) nem vehet igénybe.

Tanulság NIS 2 szempontból:

- az ellátási lánccal kapcsolatos kockázat nem áll meg az első szerződött partnernél. a további adatfeldolgozó (al-adatfeldolgozó) is kockázatot jelenthet, különösen akkor, ha további alvállalkozókat von be a megbízó tudta nélkül;
- a NIS 2 megköveteli, hogy szervezetek átláthatóan kezeljék a beszállítói láncukat, ideértve az adatfeldolgozókat és azok alvállalkozóit is;

Egy spanyol energiapiaci szereplő (adatkezelő) megbízta az ALBOR ENERGÍA S.L. tanácsadó céget, hogy potenciális ügyfeleket keressen. a megbízott engedély nélkül két további alvállalkozót is bevont, egy marketingcéget (mint al-adatfeldolgozót), amely továbbadta a munkát egy call centernek (al-al-adatfeldolgozó), amely a szolgáltató nevében ügyfeleket keresett meg szerződésmódosítás ürügyén. Mivel a tanácsadó adatfeldolgozónak minősül, aki csak az adatkezelő utasításai szerint járhat el, és a további alvállalkozók bevonása jelen esetben az adatkezelő engedélye nélkül történt, a spanyol adatvédelmi hatóság 12 ezer eurós bírságot szabott ki a tanácsadó cégre.[55]

- kulcsfontosságú a szerződéses kontroll és rendszeres audit, hogy ne történjen jogosulatlan adat-, illetve rendszerhozzáférés;
- egyetlen láncszem hibája (pl.: call center) komoly kiberbiztonsági vagy adatvédelmi incidenst okozhat.

Amennyiben általános írásbeli felhatalmazást adunk alvállalkozó bevonására, a szerződéses partnerünknek tájékoztatni kell minket minden olyan tervezett változásról, amely további alvállalkozók (adatfeldolgozók) igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget arra, hogy ezekkel a változtatásokkal szemben kifogást emelhessünk. a GDPR alapján erre az alvállalkozóra (további adatfeldolgozóra) is ugyanazok az adatvédelmi kötelezettségeket kell telepítenünk, mint amelyek köztünk és a szerződéses partnerünk között létrejött szerződésben szerepelnek. Ugyanez az egyenszilárdságú védelem kialakítására vonatkozó kötelezettség jelenik meg abban a NIS 2 védelmi intézkedésben (19.7.), mely szerint gondoskodnunk kell arról, hogy az EIR-rel összefüggő szerződésekben

55 Agencia Española de Protección de Dato: Nº: EXP202504911.

szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.

Szerződéses auditálhatóság, megfelelőség

A meglévő szerződések felülvizsgálata során kritikus, hogy rendelkezünk-e auditálási joggal, amely lehetővé teszi a beszállító és alvállalkozói tevékenységének ellenőrzését, beleértve:

- a helyszíni audit lehetőségét,
- dokumentumellenőrzést (pl.: naplók, jelentések),
- a szabálytalanságok feltárását követő intézkedési kötelezettségeket,
- audit-ütemezések és költségek szabályozását.

Az MK rendelet kifejezetten előírja, hogy folyamatosan monitorozzuk és értékeljük a rendszereinket, illetve a védelmi intézkedések megvalósulását, és ez vonatkozik a beszállítói kapcsolatokra is. Az is követelmény felénk, hogy meghatározott gyakorisággal értékeljük és felülvizsgáljuk a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat. Ezt csak abban az esetben tudjuk megvalósítani, ha a vállalkozókkal az együttműködésünk kontrollált és nemcsak megvan a lehetőségünk az ellenőrzésre, de élünk is ezzel a lehetőséggel.

> A lengyel adatvédelmi hatóság rámutatott, hogy amennyiben szerződést kötünk, amely keretében az üzleti partnerünk a nevünkben személyes adatot kezel (azaz adatfeldolgozónk), kizárólag olyan adatfeldolgozókat vehetünk igénybe, amelyek a GDPR által megkövetelt garanciák nyújtására képesek. a felek olyan hosszú távú együttműködése, amelyet nem támasztanak alá rendszeres és szisztematikus auditok vagy ellenőrzések, nem garantálja, hogy az adatfeldolgozó megfelelően ellátja szerződéses kötelezettségeit. a múltban pozitívan értékelt együttműködés csak kiindulópont lehet annak ellenőrzésénél, hogy a szerződő partnerünk elegendő garanciát nyújt-e a megfelelő technikai és szervezési intézkedések végrehajtására annak érdekében. Az adatfeldolgozási megállapodás puszta aláírásával még nem teljesítjük azt a kötelezettségünket, amely szerint a szerződő partnerünknek a GDPR követelményeinek való megfelelését ellenőriznünk kell.[56]

11.2. Új szerződéskötések szempontjai

Az új szerződések esetében az információbiztonsági, illetve az adatvédelmi szempontokat már a beszerzési folyamat során érvényesítenünk kell, ideértve a piackutatást, ajánlati felhívást, az ajánlatok értékelését, a szerződéstervezetek összeállítását, valamint a leendő szerződéses partnerekkel kapcsolatos kockázatértékelést is.

Beszerzési szabályzat

Az új szerződéskötések során elengedhetetlen, hogy a szervezetünk rendelkezzen olyan beszerzési szabályzattal, amely kiterjed az ellátási lánc biztonsági elvárásaira is. a szabályzatban célszerű rögzítenünk:

- a beszállítók és szolgáltatók előminősítési követelményeit,
- az információbiztonsági és adatvédelmi, valamint adatbiztonsági feltételeket,
- az általunk megkövetelt kötelező tanúsítványokat (pl.: ISO 27001, TISAX, SOC2),
- a kockázatalapú értékelés szempontjait,

56 DKN.5130.2215.2020,

- a szerződésben rögzítendő incidenskezelési és jelentési kötelezettségeket,
- a szerződéses partner auditálhatóságára vonatkozó kikötéseket.

A beszerzési szabályzatnak tartalmaznia kell a szervezeten belüli együttműködés módjait, a felelősségi köröket és azt is, kinek a feladata a szükséges kockázatelemzések elvégzése. Javasolt, hogy a beszerzési szabályzat ne csak a beszerzés szempontú kockázatelemzés meglétét követelje meg a megkötendő szerződés előfeltételéül, hanem az információbiztonsági és adatvédelmi kockázatelemzés meglétét is oly módon, hogy a szerződésben foglalt kikötések reflektáljanak az adott partner kockázati besorolására (pl.: felelősségbiztosítás megkövetelése, kötbér kikötése, azonnali szerződésfelmondás esetei stb.).

Fontos, hogy a beszerzési szabályzatot a szervezetünk működéséhez, ágazati sajátosságaihoz és az EIR-ek kockázati besorolásához igazítsuk, elkerülve a sablonszerű, általános megfogalmazásokat.

Az MK rendelet külön védelmi intézkedési csoportban írja elő a beszerzési folyamatainkra, illetve az ellátólánccal kapcsolatos kockázatkezelésre vonatkozó követelményeket, azonban ezek konkrét tartalommal feltöltése és megvalósítása már a szervezet feladata.

Beszállítói átvilágítás

A NIS 2 irányelv 21. cikke kötelezővé teszi a szervezetek számára, hogy proaktívan kezeljék a teljes beszállítói láncukból eredő kiberbiztonsági kockázatokat. Ez a kötelezettség a hardver, szoftver és szolgáltatás beszállítókra egyaránt kiterjed, beleértve a közvetlen és közvetett (al-) szolgáltatókat is. a megfeleléshez bizonyítanunk kell, hogy azonosítjuk, értékeljük és folyamatosan csökkentjük ezeket a kockázatokat. a hatékony beszállítói átvilágítás egy kockázatalapú, a beszállító teljes életciklusát lefedő folyamat.

A beszállítói átvilágítás mélységét és komplexitását a szervezet méretéhez és kockázati kitettségéhez kell igazítanunk. Erre egy kétlépcsős modell nyújthat praktikus megoldást, ami alap és fejlett metódusra osztható fel. Míg az előbbit KKV fókusszal javasolt használni, addig az utóbbi nagyvállalati környezetben ad megoldást.

A kisebb és közepes vállalatok számára a cél a pragmatikus, kockázatarányos védekezés, amely a legjelentősebb fenyegetésekre koncentrál, elkerülve a túlzott bürokráciát. Ez az alap modell.

Beszállítói kategorizálás: a folyamat a beszállítók azonosításával és rangsorolásával kezdődik, a rangsor alapja a beszállító üzletmenetre gyakorolt hatása. Az átvilágítást a kritikus (akik nélkül a cég működése leállna) és a fontos (akik kiesése jelentős fennakadást okoz) beszállítókra kell összpontosítanunk.

Egyszerűsített átvilágítási folyamat: a kiválasztott beszállítók esetében egy egyszerűsített, kérdőíves felmérés a leghatékonyabb eszköz. a kérdőívünk fókuszáljon a NIS 2 által is elvárt alapvető területekre

- Alapvető kiberhigiénia: Vírusvédelem, tűzfalak, rendszeres szoftverfrissítések.
- Adatkezelési gyakorlatok: Hogyan kezelik és védik az ügyfeleik adatait?
- Incidenskezelési képesség: Van-e tervük egy biztonsági incidens esetére?
- Fizikai biztonság: Megfelelő védelemmel rendelkeznek-e a fizikai eszközeik?

A nagyvállalatok komplex ellátási láncai, a beszállítók nagy száma és a magasabb kockázati szint egy jóval strukturáltabb, mélyebb és folyamatosan menedzselt átvilágítási rendszert követel meg.

Többszintű, kockázatalapú átvilágítás: a beszállítók szegmentálása itt is alapvető, de részletesebb szempontok alapján történik, mint például az adathozzáférés mértéke, a rendszerintegráció mélysége, a helyettesíthetőség és

a kritikalitás. a magas kockázatú beszállítók átvilágítása több, egymásra épülő elemből áll:

- Részletes kérdőívek: Szabványos keretrendszerekre (pl.: ISO 27002, CSA CAIQ, SIG-Full, SOC2) épülő, a technikai és szervezeti kontrollok széles körét lefedő kérdőívek.
- Többrétegű ellenőrzések: Dokumentációk (biztonsági szabályzatok, incidenskezelési tervek), külső audit riportok (pl.: penetrációs tesztek) bekérése és elemzése.
- Helyszíni vagy távoli auditok: a dokumentumokban és kérdőívekben foglaltak validálása interjúk és technikai vizsgálatok segítségével.
- Folyamatos monitorozás: Külső kiberbiztonsági minősítő szolgáltatások (Security Rating Services) alkalmazása a beszállító digitális lábnyomának folyamatos figyelésére.

A releváns tanúsítványok megléte alapelvárás a kritikus partnereknél. Ezek például az alábbiak lehetnek:

- ISO/IEC 27001: Gyakorlatilag elengedhetetlen a magas kockázatú beszállítóknál.
- Iparági tanúsítványok: Pl.: PCI DSS (pénzügy), SOC 2 vagy CSA STAR (felhőszolgáltatók), ISO 27017, ISO 27018.
- NIS 2 megfelelőségi nyilatkozat/audit: Ennek megkövetelése szintén kulcsfontosságúvá válik a jövőben.

Mérhetőség és folyamatos fejlesztés

Az átvilágítási folyamat hatékonyságát mérnünk kell, a három kulcsfontosságú teljesítménymutató (KPI):

- Átvilágított beszállítók aránya (%),
- Beszállítók tanúsítottsági lefedettsége (%),
- Kritikus sérülékenységek átlagos javítási ideje a beszállítóknál (nap).

Fontos megjegyezni, az átvilágítás nem egyszeri projekt, hanem egy folyamatos, a szervezet kockázatkezelésébe integrált tevékenység. a teljes ellátási lánc kiberrezilienciája csak a beszállítói kockázatok szisztematikus és proaktív kezelésével valósítható meg.

A szerződésben részletesen és számonkérhető módon kell meghatároznunk azokat a biztonsági követelményeket, amelyek nemcsak a szolgáltatások biztonságos működését és az adatok védelmét biztosítják, hanem garantálják az üzletmenet folytonosságát és a jogszabályi megfelelést is.

A szerződéses elvárások meghatározásakor elsődleges szempont a bizalmasság, a sértetlenség és a rendelkezésre állás (Confidentiality, Integrity, Availability – azaz a CIA-elv) biztosítása:

Bizalmasság: Rögzítenünk kell a hozzáférés-szabályozás, az adatkezelés és -tárolás, valamint a titkosítás követelményeit. Az adatokhoz kizárólag az férhet hozzá, akinek erre jogosultsága van.
Sértetlenség: Az adatok és rendszerek pontosságát, megbízhatóságát folyamatosan fenn kell tartanunk. Az adatintegritást ellenőriznünk és naplóznunk szükséges, a változásokat pedig szabályozott módon kell kezelnünk.
Rendelkezésre állás: a szerződéseinknek ki kell térnie a szolgáltatások folyamatos elérhetőségét biztosító intézkedésekre, például a redundanciára, a rendszeres mentésekre, a helyreállítási idők meghatározására vagy a kimaradások kezelésére.
A C.I.A elvet ki lehet egészíteni a hitelesítéssel és a visszautasíthatatlansággal, amely biztosítja, hogy egy tranzakcióban vagy kommunikációban részt vevő fél ne tagadhassa meg cselekedeteit, aláírásának vagy üzeneteinek hitelességét. Bizonyítja a származást és a kézbesítést, így lehetetlenné téve, hogy valaki hamisan tagadja részvételét vagy az adatok integritását.

Minden biztonsági elváráshoz célszerű konkrét, mérhető követelményeket rendelnünk, amelyek értékeléséhez teljesítménymutatók (Key Performance Indicator – KPI) alkalmazása javasolt. Ilyen elvárás lehet például a rendelkezésre állás százalékos aránya, válaszidők, helyreállítási célértékek (RTO, RPO), vagy az adatbiztonság technikai paraméterei, mint például a titkosítási szabványok vagy a hozzáférés-kezelési protokollok. a teljesítmény folyamatos mérését érdemes automatikus monitorozással, rendszeres riportokkal és auditokkal biztosítanunk, hogy mindkét fél számára átlátható legyen, teljesülnek-e a szolgáltatási szintek.

A szerződésben ki kell térnünk arra is, hogy a beszállító köteles a szerződéses biztonsági követelményeket saját alvállalkozóira is kiterjeszteni, ezzel biztosítva a teljes ellátási lánc védelmét.

Szolgáltatási szintű megállapodás (Service Level Agreement, azaz SLA)

Az SLA a NIS 2 hatálya alá tartozó szervezet (megrendelő) és a szolgáltató – jelen témakörben beszállító – között létrejövő szerződés vagy annak melléklete. Ebben a felek részletesen rögzítik a vállalt szolgáltatások körét, a minőségi és mennyiségi elvárásokat, ezek mérésének és ellenőrzésének módját, valamint a hibás vagy nemteljesítés esetén alkalmazandó eljárásokat.

A szerződésnek lehetőséget kell adnia arra, hogy a biztonsági követelmények módosíthatók legyenek, ha változnak a jogszabályok, a fenyegetettségi környezet vagy a szervezet igényei.

A megállapodásban ki kell térnünk arra is, hogy milyen következményekkel jár a biztonsági követelmények vagy szolgáltatási szintek nem teljesítése. a gyakorlatban ez lehet kötbér, díjcsökkentés, a szolgáltatás felfüggesztése vagy akár a szerződés felmondása is.

A szankciók pontos feltételeit és mértékét előre, egyértelműen kell meghatároznunk, hogy mindkét fél számára világos legyen, milyen következményekkel jár a biztonsági követelmények vagy szolgáltatási szintek megsértése. Emellett indokolt előírnunk, hogy a beszállító rendelkezzen megfelelő felelősségbiztosítással, amely fedezetet nyújt az SLA-ban és a biztonsági követelményekben vállalt kötelezettségek megszegése miatt keletkező károkra.

Incidenskezelési és jelentési kötelezettségek

Az új szerződéseinkbe kötelezően bele kell foglalnunk az incidenskezelési kötelezettségeket, amelyek biztosítják:

- az események időben történő bejelentését (tekintettel jogszabályi feltételek fennállása esetén a kiberbiztonsági incidens 24 órás, adatvédelmi incidens 72

órás felügyeleti hatósághoz bejelentési kötelezettségére),
- a közös incidenskezelési folyamatot,
- a vizsgálat során való együttműködést,
- a hatóságok felé történő jelentési kötelezettségek betartását.

Az incidenskezeléssel kapcsolatos szerződéses kikötések esetében ki kell térnünk mind a kiberbiztonsági incidensek kezelésére és jelentési kötelezettségére, mind az adatvédelmi incidensek kezelésére is, különös tekintettel a vonatkozó jogszabályok által kilátásba helyezett szankciókra.

Jogszabályi és szabályozási megfelelés

Az új szerződéseinknek biztosítaniuk kell, hogy a beszállítók és partnerek teljes mértékben megfeleljenek:

- a NIS 2 irányelvnek,
- a GDPR-nak,
- a hazai adatvédelmi és információbiztonsági előírásoknak (például az őrző-védő szolgáltatásokkal kapcsolatos speciális követelmények stb.),
- az iparági standardoknak (ISO stb.).

Már a beszerzési folyamatban, például az ajánlatok bekérésekor célszerű nyilatkozatokat kérnünk a megfelelőségről, és a szerződésekben rögzíteni kell azokat a kikötéseket, amelyek arra a helyzetre vonatkoznak, ha a szerződéses partnerünk nem tesz eleget a megfelelőségi kötelezettségeinek.

11.3. Kockázatelemzés az ellátási lánc mentén

A NIS 2 irányelv megköveteli, hogy a szervezetek ne csupán felismerjék, hanem aktívan kezeljék is az ellátási láncukból fakadó kiberbiztonsági kockázatokat. Ez egy strukturált, folyamatos és dokumentált kockázatkezelési folyamatot tesz szükségessé, amely azonosítja a gyenge pontokat, felméri azok lehetséges hatását, és megfelelő intézkedéseket rendel hozzájuk. a cél nem a kockázatok teljes megszüntetése – ami lehetetlen –, hanem azok tudatos, üzleti alapon történő kezelése és az elfogadható szintre csökkentése.

A kockázatelemzést a Whitepaper 5.7. fejezete alapján érdemes elvégezni, azonban a speciális szempontokat érdemes figyelembe venni a kockázatcsökkentő intézkedések során, hiszen a teljes ellátási láncot le kell fedniük.

Szerződéses és jogi intézkedések

A beszállítói szerződéseknek kiberbiztonsági és adatkezelési záradékot kell tartalmazniuk, meghatározva a technikai és szervezeti követelménylistát, auditálási jogot, és incidensjelentési kötelezettséget.

Technológiai intézkedések

A beszállítói lánc felől érkező fenyegetésekből eredő károkat, olyan intézkedésekkel lehet csökkenteni, mint az alábbiak:

- Hozzáférés-kezelés: a jogosultságok minimalizálása (Least Privilege) és többfaktoros hitelesítés (MFA) megkövetelése.
- Biztonságos kapcsolat: Írjuk elő titkosított kommunikációs csatornák (pl.: VPN, HTTPS) kötelező használatát.
- Hálózati szegmentáció: Izoláljuk el a beszállítók által elért rendszereket a belső hálózatunk kritikus részeitől, hogy egy esetleges kompromittálódás ne terjedhessen tovább.
- Szoftverintegritás: a „Security by Design” elvének alkalmazása. Szoftver-összetevők jegyzékének (SBOM) használata a nyomonkövethetőség és a gyors sebezhetőség-azonosítás érdekében.

Szervezeti és folyamati intézkedések

A technológiai intézkedések mellett a jól kialakított folyamatok is segítenek, úgy mint:

- Beszállítói átvilágítás: a 11.2. pontban részletezett folyamat következetes alkalmazása a szerződéskötés előtt.
- Bennfentes fenyegetések kezelése: a munkatársak, alvállalkozók és beszállítók tudatosságának növelése oktatással.
- Nemzetközi szabványok alkalmazása: Az olyan ismert szabványoknak való megfelelés, mint az ISO 27001 vagy az IEC 62443, közös nyelvet és keretrendszert teremt a biztonság értékeléséhez.
- Közös incidenskezelési gyakorlatok: a kritikus beszállítókkal érdemes lehet közösen tesztelni az incidensreagálási terveket, hogy vészhelyzetben olajozott legyen az együttműködés.
- Végponttól végpontig tartó nyomonkövethetőség: Minden alkatrész és szoftverkomponens életútját célszerű követni a forrástól a végfelhasználóig. Ez lehetővé teszi, hogy egy hiba forrását akár órákon belül azonosítani lehessen.

Jogi megfelelőség biztosítása, mint kockázatcsökkentő intézkedés

Mind a NIS2, mind a GDPR számos követelményt tartalmaz, amelyeket szerződéses szinten kell rendeznünk, ideértve például a szerződő partner munkavállalóival/megbízottjaival kapcsolatos elvárásokat, az EIR-ekkel kapcsolatos viselkedési szabályokat és azok kikényszerítésének módját, a kötelezően megkötendő hozzáférési megállapodások tartalmát, valamint a háttérellenőrzések lefolytatásának kötelezettségét.

Ezeknek a szerződéses követelmények rögzítésének célja nemcsak az, hogy megfeleljünk a jogszabályi követelményeknek, hanem az is, hogy az ellátólánccal kapcsolatos kockázatainkat tudatosan csökkentsük. Éppen ezért az ellátólánccal kockázatkezelésnek ki kell térnie az adatvédelmi, az adatbiztonsági és a humán erőforrással kapcsolatos kockázatokra is.

Folyamatos monitoring és kockázatkezelési folyamatok

A beszállítói kockázatok kezelése egy folyamatos, iteratív ciklus, nem egyszeri projekt. Ennek kulcselemei:

- Rendszeres újraértékelés: a kritikus beszállítók éves auditálása.
- Fenyegetettségi hírszerzés (Threat Intelligence): a beszállítóinkat vagy az általuk használt technológiákat érintő új támadási típusokról, sérülékenységekről szóló jelentések figyelése.
- Teljesítmény- és incidensnaplók elemzése: a beszállítókkal kapcsolatos hozzáférési naplók és az esetleges biztonsági incidensek rendszeres elemzése.

A monitoring során szerzett információkat (pl.: új sebezhetőség) vissza kell csatornáznunk a kockázatkezelési folyamatunkba. Ezzel újrakezdjük az azonosítási, értékelési és kezelési lépéseket, biztosítva a szervezet folyamatos alkalmazkodását a változó fenyegetettségi környezethez.

11.4. Milyen információkat kérjünk be a beszállítóktól?

Támogatva a szerződéskötési folyamatot, továbbá az ellátási lánc szerepét a kockázat és biztonsági esemény kezelésben, az alábbi információkat szükséges bekérnünk és szervezetünk által meghatározott gyakorisággal megújíttatnunk:

- beszállító szervezeti- és személyi alapadatai, kapcsolattartók (kiemelten a szerződésben rögzítendő incidenskezelési és jelentési kötelezettségek vonatkozásában),

az általunk megkövetelt tanúsítványok, minősítések;

- a beszállítók és szolgáltatók előminősítési követelményei alapján meghatározott elvárt kiberbiztonsági védelmi intézkedések és az információbiztonsági érettségi szintjére vonatkozó információk, pl.: önértékelési kérdőív formájában;
- az ellátási lánc – a beszállító, szolgáltató és alvállalkozóik – kockázatainak felmérése a releváns EIR-k, rendszerelemek és rendszerszolgáltatások vonatkozásában, pl.: kiberbiztonsági követelményeket tartalmazó kérdőíven a megfelelés igazoló adatok.

Beszállítók és partnerek biztonsági követelményei

Az adminisztratív, fizikai és logikai kiberbiztonsági követelményeket a releváns EIR-k, rendszerelemek és rendszerszolgáltatások vonatkozásában az ellátási láncra is meg kell határoznunk a közreműködés szintje és jellege alapján.[57]

Incidenskezelés az ellátási láncban

A NIS 2 irányelv beszállítói láncra vonatkozó incidenskezelési elvárásai a teljes szállítói ökoszisztémát érintik, ezért a proaktív kiberbiztonsági működés a szervezetek számára stratégiai kérdéssé vált. Egyetlen beszállítói incidens dominóhatást indíthat el, amely végigsöpör az értékláncon, így a partnerek megfelelősége és üzleti folytonossága nagymértékben függ attól, mennyire felkészültek a beszállítók.[58]

E környezetben a kockázatkezelésnek túl kell lépnie a hagyományos IT-biztonsági kereteken: a saját, valamint a harmadik és negyedik felek által alkotott alvállalkozói hálót is folyamatosan vizsgálnunk kell. a felkészültség részét képezi a nap 24 órájában működő biztonsági megfigyelés, amely valós idejű fenyegetés-észlelést, partneri anomáliák azonosítását és automatizált riasztást foglal magában.

A jelentési kötelezettségek szigorúak. Az ellátási lánc szereplőinek indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül egy első bejelentést, indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, és zárójelentést – legkésőbb az eseménybejelentés benyújtását követő egy hónapon belül – kell tenniük. Amennyiben a fő kommunikációs csatorna nem elérhető, alternatív megoldásként nyilvános közlemények vagy szakmai szervezeteken keresztül történő értesítés is alkalmazható.

Amennyiben az incidens személyes adatokat is érint, az adatvédelmi incidens jelentésére vonatkozó követelményeknek kell megfelelnünk, az ezzel kapcsolatos határidőket és feladatokat célszerű a szállítóval kötött adatfeldolgozási megállapodásban rögzítenünk.

Az incidensek súlyosság szempontjából kategórizálhatók, és célszerű, hogy az észlelés pillanatában életbe lépő protokollunk előírja az érintett rendszerek izolálását, a károk felmérését, a kommunikációs terv aktiválását, valamint a belső és külső szakértők mozgósítását.

A hatékony helyreállítás érdekében üzleti partnereinkkel közösen gyakorlatokat szervezhetünk és folyamatosan megoszthatjuk egymással a releváns információkat, összehangolva a helyreállítási lépéseket, majd a tapasztalatok alapján finomítva a folyamatainkat. a helyreállítás során kiemelt szerep jut a kritikus szolgáltatások folytonosságának biztosításának, az adatintegritás visszaállításának, az alkalmazott kontrollok megerősítésének és az eredmények utánkövetésének.

---

57 Lásd még : MK rendelet 16. védelmi intézkedéscsoport, a 16.2.1 fejezet

58 ENISA: GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY. June 2023. doi:10.2824/805268 TP-03-23-145-EN-N.

Fontos, hogy a kommunikációnk többszintű, biztonságos infrastruktúrára épüljön. Az elsődleges titkosított vonalak mellett kell, hogy rendelkezésünkre álljanak tartalék csatornák, vészhelyzeti protokollok és szükség esetén nyilvános platformok. Az érzékeny adatok továbbítása végponttól végpontig titkosítva, többfaktoros hitelesítés mellett és auditált naplózással történjen.

Gondoskodnunk kell róla, hogy a felelősségi körök átláthatóak legyenek. Célszerű, hogy dedikált incidenskezelő irányítsa a folyamatot, egyértelmű eszkalációs útvonalak segítsék a döntéshozást, a különböző szakterületek képviselői közösen dolgozzanak, miközben igény esetén külső tanácsadók is bekapcsolódhatnak. a szerződéseink részletesen rögzítsék a bejelentési határidőket, a felelősségi és kártérítési kereteket, az audit-jogokat és a lehetséges szankciókat mind információbiztonsági, mind adatvédelmi vonatkozásban.

A folyamatos fejlődés biztosítása érdekében a személyzetünk részesüljön rendszeres képzésekben, szükség esetén vezessünk be új technológiákat a védelmi képességeink növelésére. a megfelelőséget folyamatosan monitorozzuk a hiányosságainak a lehető legrövidebb határidővel szüntessük meg és naprakész iparági ajánlásokat alkalmazzunk.[59] Az információbiztonsági stratégiai szemléletű beruházások hosszú távon költségmegtakarítást, magasabb ügyfélelégedettséget, szabályozói előnyöket és kedvezőbb biztosítási feltételeket is eredményezhetnek.

A NIS 2 a technológiai korszerűsítést is ösztönzi[60]: mesterséges intelligencián alapuló fenyegetés-észlelés, automatizált válaszrendszerek, felhőalapú biztonsági szolgáltatások és integrált platformok válnak a szállítói környezet részévé. Azok a vállalatok, amelyek képesek összhangban működtetni a felderítést, a reagálást, a kommunikációt és a felelősségvállalást, megbízható partnerekké lépnek elő, és versenyelőnyhöz jutnak a biztonságtudatos digitális gazdaságban.

Folyamatos megfelelőség és audit

Előre meghatározott rendszerességgel az ellátási láncban ellenőrzéseket, információbiztonsági és adatvédelmi auditokat kell végrehajtanunk, akár helyszíni vagy adatbekérés formában a megfelelőség igazolására. Az ellenőrzéseket és azok kiértékelését javasolt módszertan kidolgozásával formalizálnunk, a megfelelés igazolásához alátámasztó bizonyítékokat bekérnünk, támogatva a kiberbiztonsági audit megfelelést. a beszállító részére az audit tervet át kell adnunk.[61]

Oktatás, tudatosság és tréning

Az ellátási lánc szereplőinek képzése, a tudatosság növelése fontos tényező a beszállítói kockázatok csökkentése szempontjából. Ennek keretében átadhatjuk a vonatkozó szabályzatainkat, a vészhelyzeti intézkedési terveinket és azokat gyakorolhatjuk is, valamint közzétehetünk kiberbiztonsági ismertetőket is.

Vészhelyzeti tervezés és helyreállítás

Meg kell határoznunk az üzletmenet-folytonosság szempontból kritikus beszállítóinkat, szolgáltatóinkat és azok alvállalkozóit, és a vonatkozó terveinkben meg kell határoznunk a szerepüket. a kockázatelemzésben figyelembe kell vennünk a szolgáltatás megszűnéséből eredő kockázatokat, redundanciákat vagy alternatívákat biztosítva a folytonosság fenntartására.

59 pl.: ENISA: CYBERSECURITY ROLES AND SKILLS FOR NIS 2 ESSENTIAL AND IMPORTANT ENTITIES – Mapping NIS 2 obligations to ECSF. June 2025. doi: 10.2824/8870995.

60 pl.: ENISA: TECHNICAL IMPLEMENTATION GUIDANCE. June 2025, version 1.0. doi:10.2824/2702548.

61 Lásd még: 11.1.3. Szerződéses auditálhatóság, megfelelőség

11.5. Mit adjunk át beszállítóként?

A NIS 2 szabályozás értelmében beszállítóként információt kell szolgáltatnunk partnereinknek a saját információbiztonsági érettségi szintünkről annak érdekében, hogy partnereink felmérhessék a kockázatokat az ellátási láncaikban. Ez a transzparencia egyik pillére a NIS 2-es megfeleléshez és az információbiztonsági rendszer biztonságos működtetéséhez.

Milyen információkat adjunk át?

Az átadandó adatok körét a szolgáltatás jellege és a partner igényei határozzák meg. Általánosságban az alábbiakat érdemes – szerződéstől függően pedig kötelező – megosztanunk:

- Információ szervezeti szintű biztonsági intézkedéseinkről:
  - Információbiztonsági irányítási rendszerünk (IBIR): nyilatkozzunk IBIR meglétéről (pl.: ISO 27001 tanúsítvány), vagy adjunk át magas szintű összefoglalót (amennyiben rendelkezünk ilyen rendszerrel).
  - Biztonsági események kezelése: adjunk tájékoztatást a belső incidenskezelési folyamatainkról és protokollokjainkról, határidőkről, értesítési láncokról. Erre az adatfeldolgozási megállapodásaink is kitérnek.
  - Kockázatkezelési megközelítés: röviden ismertessük, hogyan azonosítjuk és kezeljük a biztonsági kockázatokat.
  - Technikai védelem: magas szintű leírás a releváns védelmi rétegekről (pl.: tűzfalak, végpont-, vírusvédelem, fizikai biztonság).
  - Adatmentés és helyreállítás: információk az üzletmenet folytonossági és katasztrófa-helyreállítási tervünkről.
- Szerződéshez specifikusan kapcsolódó biztonsági garanciák:
  - Szolgáltatási szintű megállapodások (SLA): adjuk át a biztonsággal kapcsolatos vállalásokat tartalmazó SLA-kat, technikai és szervezési intézkedéseink leírása (TOM, GDPR 32. cikk).
  - Auditálhatóság, ellenőrzési jogok: részletezzük a szerződésben rögzített auditálhatósági jogokat (beszállítóként ügyeljünk arra, hogy egyes partnereink túlzott elvárásokat támaszthatnak velünk szemben).
- Adatkezelési és adatvédelmi megfelelőség:
  - GDPR megfelelőség: nyilatkozat az adatvédelmi és adatbiztonsági megfelelőségünkről és adatfeldolgozást is tartalmazó tevékenység esetén adatfeldolgozási megállapodás megkötése (GDPR 28. cikk).
  - Adatlokalizáció: tájékoztatás az adatok tárolási helyéről. a régió / joghatóság megjelölése szükséges lehet az adatvédelmi követelmények miatt is.

Mely információk adhatók át biztonságosan, és melyeket tilos átadnunk?

- Biztonságosan átadhatók: nyilvános adatok, magas szintű összefoglalók és politikák (bizalmas technikai részletek nélkül), megfelelőségi nyilatkozatok (pl.: tanúsítványok), kijelölt kapcsolattartók adatai, bejelentési felületek elérhetősége.
- Nem, vagy csak szigorú feltételek mellett adhatók át: érzékeny műszaki konfigurációs adatok (pl.: hálózati topológia, titkosítási kulcsok, hozzáférési adatok), belső sebezhetőségi felmérések és penetrációs tesztek részletes eredményei (helyette nyilatkozat a rendszeres vizsgálatról), személyes adatok (csak megfelelő jogalappal és garanciák biztosítása mellett), üzleti titkok és szellemi tulajdon. Amennyiben a partner olyan dokumentumot kér, amely nem szükséges ahhoz, hogy a biztonságunk szintjét megítélje, alkalmazzuk a fokozatosság elvét, osszuk meg a fedőlapot, a kivonatot,

a tartalomjegyzéket, adott esetben biztosítsunk helyszíni betekintési lehetőséget.

Hogyan döntsük el, mit adhatunk át?

- Szükségesség és arányosság: csak a feltétlenül szükséges információkat osszuk meg, amely ténylegesen szükséges annak igazolásához, hogy egy adott védelmi intézkedést, biztonsági megoldást leszabályoztunk, és az a gyakorlatban is működik.
- Kockázatelemzés: minden információátadás előtt mérjük fel a kockázatokat és a szükséges védelmi intézkedéseket (pl.: titkosított kommunikáció).
- Személyes adatok átadása: amennyiben nem jogszabály kötelez minket az adatok átadására, körültekintően állapítsuk meg a hivatkozott jogalapot és jogos érdekre hivatkozás esetén végezzünk érdekmérlegelési tesztet.
- Titoktartási megállapodás (NDA): Érzékeny adatok esetén ragaszkodjunk NDA megkötéséhez, illetve adatfeldolgozási megállapodás esetén ne terjeszkedjünk túl az abban foglaltakon.
- Szerződéses kötelezettségek: Tartsuk szem előtt a szerződésben rögzített kötelezettségeket annak fennállása idején (pl.: tanúsítvány fenntartása, incidensbejelentő űrlap elérhetősége, érintetti jogok érvényesülésének támogatása stb.).
- Kommunikáció: nyíltan kommunikáljunk a partnereinkkel az esetleges aggályainkról és szükség esetén keressünk alternatív megoldásokat.

Beszállítóként fontos a proaktív együttműködés, azonban mindig a „zero trust”, illetve a “need to know” elvét szem előtt tartva osszunk meg információkat. a cél a transzparencia, de nem a sebezhetőségünk, valamint egyéb kockázataink növelése.

12

Használható eszközök és automatizálási lehetőségek

A NIS 2-nek való megfelelés egyik legnagyobb kihívása nem pusztán a szabályozói elvárások értelmezése, hanem azok mindennapi működésbe való beépítése. Ehhez a szervezeteknek olyan eszközökre és automatizálási lehetőségekre van szükségük, amelyek támogatják a kockázatok átlátható kezelését, az auditálhatóság biztosítását, valamint a vezetői döntések megalapozását. Az Exceltől kezdve a komplex GRC rendszereken át egészen a mesterséges intelligencián alapuló megoldásokig számos út áll rendelkezésre, melyek más-más szervezeti érettségi szinthez és erőforrásigényhez illeszkednek. a fejezet célja, hogy bemutassa a leggyakrabban alkalmazott megoldásokat, és segítsen kiválasztani a szervezet méretéhez és céljaihoz leginkább illeszkedő eszközt.

12. Használható eszközök és automatizálási lehetőségek

Írták: Dr. Váczi Dániel, Csarnai Gergő, Mészáros Csaba

12.1. Excel-alapú megoldások

Az Excel az egyik legelterjedtebb és legegyszerűbben hozzáférhető eszköz, amelyet sok szervezet használ kiberbiztonsági és megfelelőségi feladatok nyilvántartására, kezelésére és riportolására. Előnye, hogy könnyen testre szabható, gyorsan létrehozhatók benne táblázatok, kimutatások és diagramok, és a felhasználók többsége alapvető szinten már rendelkezik a használatához szükséges ismeretekkel. Támogatja az adatok rendezését, szűrését, valamint a különféle képletek és függvények alkalmazását, így jól használható kockázatelemzéshez, feladatnyilvántartáshoz vagy ellenőrzési tervek összeállításához. Rugalmas formátuma lehetővé teszi, hogy a szervezet saját folyamataira és igényeire szabja a dokumentumokat anélkül, hogy komoly fejlesztési erőforrásokat kellene bevonnia.

Azonban az MK rendeletek alapján egyre komplexebb követelménystruktúra alakult ki, amelyet bár alapvető szinten lehet Excelben kezelni, a részletes és folyamatos megfelelés biztosítása már nehézkes. Különösen igaz ez olyan szervezeteknél, amelyek nagy számú EIR-rel rendelkeznek, hiszen ilyenkor a táblázatok karbantartása, az adatok frissítése és a kapcsolódó bizonyítékok rendszerezése jelentős erőforrást igényel. Cégcsoportok esetében a követhetőség és a számosság miatt ez a probléma hatványozódik. a különböző leányvállalatok vagy szervezeti egységek adatainak egységes kezelése, konszolidálása és nyomon követése Excelben gyakran bonyolult, időigényes, ráadásul a hibázási esély is magas.

A legtöbb szervezet ennek ellenére mégis megpróbálta a komplex követelményeket Excelben megvalósítani. Emiatt számos eltérő megközelítés, táblázattípus alakult ki, ami az audit során is nehézséget okozhat, különösen, ha a táblázatok felépítése, adatstruktúrája vagy jelölésrendszere nem egységes. a következetlen formátum és tartalom nemcsak a belső nyomon követést, hanem az auditorok munkáját is megnehezíti. Éppen ezért célszerű lehet az NKI OVI űrlapot[62] vagy a védelmi intézkedés katalógust[63] alkalmazni alapként. Bár ez önmagában nem biztosít olyan komplex, integrált megoldást, amely teljes körűen lefedi a NIS 2 követelményrendszerét, jó kiindulási pontot adhat a megfelelőségi munka strukturálásához, és segíthet egységes keretet teremteni a dokumentáláshoz.

Ezek mellett az Excel használatának további korlátai és kockázatai is figyelmet érdemelnek. Az egyik legnagyobb hátrány a verziókezelés nehézsége, különösen akkor, ha a fájlokat e-mailben vagy megosztott hálózati mappában kezelik. Ez könnyen vezethet több, eltérő verzió párhuzamos használatához, ami adatkonzisztencia-problémákat okozhat. Bár a felhőalapú tárhelyek részben megoldják ezt a gondot, ott is gondoskodni kell a jogosultságkezelés megfelelő beállításáról.

Biztonsági szempontból kockázatot jelent, hogy az Excel-fájlok könnyen másolhatók és továbbíthatók, a beépített jelszóvédelem pedig viszonylag gyenge, így önmagában nem elegendő érzékeny adatok biztonságos tárolására. Az Excel nem biztosít beépített, részletes audit-nyomvonalat sem, ezért nehéz pontosan nyomon követni, ki, mikor és mit módosított. Ez megfelelőségi vizsgálatoknál hátrányt jelenthet.

62 NKI Űrlapok

63 NKI EIR útmutató

Funkcionális korlát, hogy a szerepkör-alapú hozzáférés és a komplex jogosultságkezelés nem támogatott, így nem lehet hatékonyan elkülöníteni a felhasználói jogosultságokat. Nagy adatállomány vagy bonyolult számítások esetén a teljesítmény romolhat, a dokumentum instabillá válhat. Az automatizálási lehetőségek, például makrók és VBA-szkriptek, bár hasznosak lehetnek, nem érik el a dedikált GRC- vagy menedzsmentrendszerek által nyújtott integrációs és workflow-kezelési szintet.

Az Excel jó választás lehet ugyan kisebb szervezetek vagy átmeneti megoldások esetén, illetve olyan feladatokra, ahol gyors, rugalmas és költséghatékony eszközre van szükség. Hosszú távon, komplex folyamatok, nagymennyiségű adat és szigorú megfelelőségi követelmények esetén azonban célszerű dedikált információbiztonsági vagy GRC és menedzsment eszközök megoldásra váltani, amely hatékonyabb verziókezelést, auditálhatóságot és biztonságot kínál.

12.2. GRC és menedzsment eszközök

A NIS 2-nek való megfelelés nem csupán egy jogi vagy technikai feladat, hanem sokkal inkább egy olyan komplex, folyamatalapú átalakulás, amely a szervezet egészére hatással van. Az irányelv előírásai olyan információbiztonsági irányítási rendszert igényelnek, amelyben az információk következetesen, naprakészen és transzparensen elérhetők. Ebben kulcsszerep jut a GRC[64] és egyéb specifikus menedzsment eszközöknek.

A közepes szervezetek, de gyakran a nagyvállalatok is gyakran Excel táblázatokkal, Word dokumentumokkal, fájlmegosztó mappákkal és e-mailekkel próbálják elvégezni azt a komplex munkát, ami a megfeleléshez és az auditáláshoz szükséges. Ez ideiglenesen működhet, de egy többfunkciós, kockázatvezérelt rendszer nélkül rendkívül nehéz átlátni a teljes komplex NIS 2 alapú IBIR-t. a magyar jogszabályok mentén, ráadásul az érintett szervezetek nem csak az MK rendeletben szereplő követelményrendszert kell figyelembe venni, hanem az sikeres audit felkészülés érdekében célszerű az ezt tovább bontó SZTFH rendeletben szereplő elemi követelményeket és további információkat is figyelembe venni. Ráadásul ez a kettő nem teljesen feleltethető meg egymásból, mivel az audit módszertan nem csak olyan követelményeket bont alá, amelynek nincs gyereke (pl.: 1.1.1.1), de magasabb szintűeket is, úgy mint az 1.1.1. Ráadásul a második szinten (pl.: 1.1) paramétereket is definiál. Ezt Excelben megvalósítani nem könnyű és biztos nem kényelmes. De ez csak egy része a nehézségeknek. Át kell látni és az auditor számára egyértelműen át is kell adni a felelősségi köröket, összekapcsolni a kockázatokat és az ellenintézkedéseket, biztosítani az audit során a folyamatos információátadást.

A NIS 2 új dimenziója, hogy nem elegendő a „papíralapú” megfelelés. a hatóságok és auditorok egyre inkább folyamatalapú, dinamikus bizonyítékokat keresnek arra, hogy egy szervezet valóban képes időben reagálni fenyegetésekre, kezelni a kockázatokat és dokumentálni az incidenseket.

A GRC rendszerek célja, hogy összefogják azokat a területeket, amelyek különböző emberekhez, csapatokhoz és folyamatokhoz kötődnek. Egy jól működő GRC vagy NIS 2 menedzsment eszköz nemcsak technikai checklistákat kínál, hanem lehetőséget ad a folyamatok, EIR-ek nyomon követésére, a dokumentumverziók és a döntések kezelésére, a kockázatok rögzítésére és értékelésére, a feladatkiosztásra és határidőmenedzsmentre, valamint incidensek regisztrálására és kivizsgálására.

A piacon különböző szintű eszközök találhatók: egyesek a pénzügyi vagy IT kockázatokra

64 GRC: Governance, Risk, Compliance angol szavak anagrammája. Magyarul irányítás, kockázat, megfelelést jelent.

optimalizálták funkcióikat, mások kifejezetten a kibervédelem vagy a compliance oldalról közelítenek. a NIS 2 esetében kulcsfontosságú, hogy az eszköz ne csak technikai megfelelőségi szempontokat tudjon kezelni, hanem a teljes szervezeti működést le tudja képezni a vezetői döntéstámogatástól a végrehajtási szintekig.

Egy jól kiválasztott menedzsment eszköz már a bevezetés első szakaszában segíthet rendszert vinni az egyébként széttöredezett felkészülési folyamatba. Az automatizált értesítések, a vizuális státusztérképek, a dashboardokon keresztüli átláthatóság mind olyan eszközök, amelyek elősegítik a vezetői felelősség teljesítését is, ami a NIS 2 egyik legfontosabb eleme.

Ezen kívül ezek az eszközök segítenek: az auditálhatóság biztosításában (minden döntés, határidő és tevékenység nyomon követhető), az érettség és megfelelés felmérésében és fejlesztésében (strukturált kérdőívek, felületek alapján), a tudásmegosztásban és belső együttműködésben, mivel egy platformon dolgoznak a különböző csapatok (pl.: IT, jog, compliance, vezetés) és végső soron a kockázati gondolkodás integrálásában a szervezet napi működésébe.

A NIS 2 bevezetésével véget ért az az időszak, amikor egy szervezet „túlélhette" a szabályozói megfelelést ad hoc Excel-listákkal és e-mailes egyeztetésekkel. a felügyeleti hatóságok már nemcsak a meglévő szabályzatokra kíváncsiak, hanem arra is, hogyan működnek a folyamatok a valóságban, hogyan reagál a szervezet incidens esetén, és hogyan kezelik ténylegesen a kockázatokat.

Egy jól integrált GRC vagy menedzsment rendszer lehetővé teszi, hogy a szervezet proaktív legyen, ne csak reagáljon a követelményekre, hanem képes legyen saját működését is mérni, javítani, tanulni belőle.

A megfelelő eszköz kiválasztása nem pusztán funkcionalitás és, lássuk be, pénz, kérdése. Sokkal inkább arról szól, milyen érettségi szinten áll a szervezet, milyen mértékben kíván hosszú távon belső kontrollokat kiépíteni, és mennyire fontos számára, hogy a megfelelés ne (csak) teher legyen, hanem versenyelőny is. a piacon számos nemzetközi megoldás érhető el, azonban az elmúlt években több magyar fejlesztés is megjelent, amelyek kisebb-nagyobb mértékben beépítették a hazai jogszabályi és iparági sajátosságokat. Ezek különösen előnyösek lehetnek, ha a szervezet a NIS 2 követelményeit a magyar szabályozási környezethez igazodva kívánja megvalósítani.

A jövő azoké a szervezeteké, amelyek képesek nemcsak megfelelni a NIS 2-nek, hanem azt integrálni is tudják a napi működésbe, ehhez pedig elengedhetetlen egy jól átgondolt, testreszabott menedzsment támogatás.

12.3. AI alkalmazási lehetőségei

Ugyan az AI Act nincs a whitepaper scope-jában, érdemes megemlíteni, hogy azok a szervezetek, amelyek AI rendszereket kezdenek használni (esetleg fejleszteni) a NIS 2 megfelelés céljából, azoknak az AI Act követelményeinek is meg kell felelniük: mérlegelendő tehát, hogy amennyiben csak a NIS 2 megfelelés lenne a szervezet motivációja az AI rendszerek használatához, azzal egy másik jogszabály hatálya alá is kerülne az adott szervezet, ami további teendőket jelent[65]. Amennyiben az ebben a fejezetben említett javaslatoknak van az AI Act-ben megfeleltethető fejezet, azokra hivatkozni fogok.

AI Act szerinti definíciója[66]: *"gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet*

65 Az AI Act a szolgáltatók (fejlesztők) számára olyan kötelezettségeket ír elő, amik az általuk készített (AI alapú) termékek minőségét és megbízhatóságát hivatottak biztosítani. Ez az AI rendszert használó szervezetek (alkalmazó) számára garanciát jelenthet a termékkel kapcsolatban.

66 AZ EURÓPAI PARLAMENT ÉS a TANÁCS (EU) 2024/1689 RENDELETE 1. fejezet 3. cikk

tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet".

Talán triviális megállapítás, de mégis szeretnénk felhívni a figyelmet arra, hogy az AI/MI rendszerek a kapott bemenetből (legyen az a végrehajtandó instrukció, a modell tanítására rendelkezésre álló adat, vagy az adat, amin műveleteket fog a rendszer végrehajtani) tudnak kiindulni: és igaz a garbage in – garbage out alapelv. Emiatt az egyik feltételezés az, hogy főleg azok a szervezetek tudnak majd profitálni az AI használatból a törvény és vonatkozó rendeletei megfelelésében, amelyeknél a bemeneti adat minősége lehetővé teszi azt, hogy az AI rendszer által generált kimenet használható legyen.

Prompt engineering

"A prompttervezés (prompt engineering) a mesterséges intelligencia modell által értelmezhető és megérthető utasítások (promptok) strukturálásának a folyamata."[67] a prompt megfogalmazása és részletessége jelentősen befolyásolja egy AI rendszer által generált kimenetet. Érdemes tehát gyakorolni a promptok írását – lehetőleg szintetikus, nem saját adattal – erre lehet jó a "digital twin". a szükséges ismeretek elsajátításához kurzusok, könyvek, whitpaper-ök[68] állnak rendelkezésre.

AI hallucináció

Egyes generative AI rendszerek kockázata az, hogy abban az esetben is választ fog adni, amennyiben nem áll rendelkezésére minden szükséges adat, mely esetben a kapott válasz nem lesz teljesen megalapozott. Létezik egy NIST 800-53 GPT[69] (Generative Pre-trained Transformer), amely állítása szerint "segítséget nyújt a NIST SP 800-53 rev 5 szabványnak megfelelő rendszerbiztonsági tervek szabályozási megvalósítási részleteinek megírásában, és végigvezeti a teljes értékelési és engedélyezési (A&A) folyamaton". Ezt tesztelve az alábbi képen látható kimenetet kaptam, amellyel kapcsolatban két hibára érdemes felhívni a figyelmet: a PE-14-es kontrollok (amiket az MK rendeletben "12.37. Környezeti védelmi intézkedések" néven találhatunk) valójában már az alap biztonsági osztálynál is alkalmazandók, illetve PE-14(3)-as kontroll nem létezik.

Emberi felügyelet[70]

Még ha nem is lenne az AI Act miatt kötelező, minél komplexebb és fontosabb/kockázatosabb feladatokat tervezünk AI rendszer segítségével végrehajtani[71], annál fontosabb az emberi felügyelet: győződjünk meg arról, hogy a rendszer által generált kimenet minősége és pontossága az általunk elérni kívánt célnak megfelel. Ha szabályzatírási feladatra használjuk, tartalmaz -e az AI által generált szabályzat olyan követelményt, amelynek a szervezet nem tud majd megfelelni? Rendelt -e esetleg olyan munkakörhöz egy adott feladatot/felelősséget, amely nem létezik a szervezeten belül?

67 Prompttervezés – Wikipédia Stable Diffusion Prompt Book openAI

68 White Paper | The Cyber Security Professional's Guide to Prompt Engineering | Check Point Software

69 ChatGPT – NIST 800-53 Risk Management Framework GPT

70 AZ EURÓPAI PARLAMENT ÉS a TANÁCS (EU) 2024/1689 RENDELETE 1. fejezet 14. cikk

71 AZ EURÓPAI PARLAMENT ÉS a TANÁCS (EU) 2024/1689 RENDELETE 3.

Step 1: Identify Applicable Baseline for PE-14 Control

According to **NIST SP 800-53B (Control Baselines)**, the PE-14 control applicability is as follows:

Control ID	Control Name	Low	Moderate	High
PE-14	Environmental Controls		✔	✔
PE-14(1)	Automatic Controls		✔	✔
PE-14(2)	Monitoring with Alarms and Notifications		✔	✔
PE-14(3)	Redundant Systems			✔

Explanation:

- **Low Baseline:** PE-14 is generally **not applicable** at the Low security categorization level.
- **Moderate Baseline:** PE-14 **and enhancements (1), (2)** are required.
- **High Baseline:** PE-14 **and enhancements (1), (2), and (3)** are required.

Alacsony kockázatú feladatok

Excel függvények írása: gyakran hasonlítják az Excel-t svájci bicskához, az igazán összetett feladatok jellemzően hasonlóan összetett függvényeket, makrókat kívánnak meg. Ebben igazán nagy segítséget tudnak adni a különböző AI modellek.

Tananyagok, összefoglalók készítése: a vonatkozó jogszabályoknak való megfelelés egyik velejárója a robosztus szabályzat és eljárásrend dokumentálási kényszer. a dokumentumok megléte önmagában nem elegendő, azokat oktatni és követni kell. Jellemzően ezek a dokumentumok eltérő mértékben állapítanak meg felelősségeket a szervezeten belül (pl.: RACI). Elősegítheti a szabályok betartását és betartatását, ha az elvárások címzettjei rájuk szabott oktatásban részesülnek – ebben szintén segítséget nyújthatnak az AI alapú rendszerek, mint pl.: az adott szerepkörre vonatkozó követelmények kigyűjtése, abból tanagyag, vagy összefoglaló készítése, akár az írott szövegből beszéddé, videóvá transzformálva.

Kiberbiztonság – beágyazott AI funkciók

Nagy mennyiségű adatok (naplóbejegyzések, hálózati forgalom stb.) automatizált elemzésének kontextusában nehezen elképzelhető manapság olyan kiberbiztonságot támogató szolgáltatás/eszköz, amely nem használ AI-t valamilyen szinten, legyen az a végpontok védelme szignatúra alapú vírusdetektálás helyett a végpont viselkedését monitorozza folyamatosan, vagy a be- és kimenő e-mail-eket vizsgálja át kártékony kódok után kutatva. Ennek alapján, a tudomány és technológia állását figyelembe véve (lásd még: GDPR 32. cikk), AI alkalmazása nélkül, még ha az nem is kifejezetten tudatosan valósul meg a szervezet részéről (mivel ezek beágyazott AI funkciók), a NIS 2-nek megfelelni nem realisztikus.

AI az MK rendelet kontextusában
Vannak olyan kiegészítő védelmi intézkedések a rendeletben, amelyek bevezetése AI használatot igényel, mint pl.:

- 10.24. Kellő időben történő karbantartás – Prediktív karbantartás automatizált támogatása
- 15.8. Kockázatelemzési és kockázatkezelési eljárásrend – Prediktív elemzés

mely intézkedésekből látható, hogy azok nagy mennyiségű adat elemzéséből származtatott előrejelzésekre épülnek.

Agentic AI

A szervezetekre váró komplex kihívásokból látható, hogy egy több EIR-rel rendelkező szervezet esetében, amely a jelentős/magas biztonsági osztályba tartozik, a NIS 2 megfeleléshez (emberi) erőforrásokra van szükség: legyen az audit evidenciák gyűjtése és tárolása a belső ellenőrzések a kötelező auditokhoz, megtalálni pont azt a szabályzatot, amely a dokumentumok útvesztőjében elrejtőzött, de már biztos, hogy láttam valahol. Lehetnek ezek között olyan tevékenységek, amiket AI agent-ek hatékonyabban végre tudnak hajtani – természetesen megfelelő óvintézkedések mellett.

Az összetett és egymásra gyakran visszautaló, egymással összefüggő szabályzatok, folyamatok, végrehajtási útmutatók, valamint az ezekre épülő oktatóanyagok és megállapodások világában gyakran előfordul, hogy az egyik komponens megváltoztatása nem kerül azonnal átvezetésre a többi dokumentumba. Ez okozhat értelmezési és megfelelési gondokat is: AI agent-ek használatával ezek a hibák kiküszöbölhetőek lehetnek.

Továbbá, az önellenőrzéssel kapcsolatos feladatok gyakran az elmúlt 1/3/6 hónapra tekintenek vissza – megfelelően alkalmazott AI agent-ek gyakorlatilag valós időben, de mindenféleképpen gyakrabban hajthatják végre azokat a tevékenységeket helyettünk, amelyekhez a szükséges hozzáféréseket megkapja.

Low-code, no code megoldások

Egy magyar fejlesztő 3 hét alatt low-code, no code megoldásokkal képes volt létrehozni az “X” (korábban Twitter) platform másolatát egy kihívás során[72]. Természetesen nincs garancia arra, hogy egy ilyen módon, házon belül elkészített NIS 2 alkalmazás képes lesz ugyanazokat a funkciókat biztosítani, mint egy erre a célra fejlesztett szoftver: megfelelő kreativitás, fejlesztői (és természetesen vezetői) támogatás és a büdzsé hiányának együttállása azonban eredményezhez olyan helyzetet, amikor érdemes lehet próbát tenni egy saját szervezeti használatra fejlesztett alkalmazással.

12.4. Evidenciafeldolgozás nyelvi modellekkel: lehetőségek és korlátok

A NIS2-re való felkészülés és az auditok támogatása során egyre gyakrabban merül fel a lehetőség, hogy a szervezet által feltöltött dokumentumokat, bizonyítékokat és technikai nyomokat nagy nyelvi modellek segítségével dolgozzák fel. Bár kézenfekvőnek tűnhet több száz oldalnyi szabályzat, log, konfiguráció vagy riport automatikus kontroll-hozzárendelése, a gyakorlatban ez jóval összetettebb feladat. A nehézséget nem elsősorban a dokumentumok mennyisége, hanem azok heterogenitása, eltérő minősége és az a tény okozza, hogy a kontrollmegfelelés megállapítása nem egyszerű szövegkeresés, hanem értelmezési és bizonyítási folyamat.

72 BOBCATTER: OUR AI-ASSISTED NO-CODE “X-PERIMENT” What we learned from cloning X using only AI tools?

A szervezeti evidenciák jellemzően nem auditlogika szerint készülnek. Egy szabályzat, eljárásrend vagy SIEM-riport egyszerre több kontrollhoz is kapcsolódhat, miközben nem hivatkozik közvetlenül jogszabályi kontrollazonosítókra. Egy nyelvi modell számára ezért nemcsak az a kérdés, hogy mit tartalmaz egy dokumentum, hanem az is, hogy annak mely részei relevánsak egy adott kontroll szempontjából, és azok valódi megfelelést vagy csupán közvetett utalást jelentenek-e. A magyar szabályozások ráadásul absztrakt kontrollnyelvet használnak, amelyet a szervezeti dokumentáció ritkán követ szó szerint. Emiatt a modellnek egyszerre kellene értelmeznie a kontrollnyelvet, a szervezeti működést, a technológiai környezetet és a bizonyítékok bizonyító erejét.

Az audit során nem elegendő megtalálni a kapcsolódó dokumentumokat. Azt is meg kell állapítani, hogy azok tényleges működést igazolnak-e. Egy szabályzat megléte például nem bizonyítja önmagában annak gyakorlati végrehajtását. A modellek könnyen tévesen pozitív következtetésre juthatnak, ha egy jól megfogalmazott szabályzatot működési bizonyítékként értelmeznek. Ezt tovább nehezíti, hogy az evidenciák részben strukturáltak, részben strukturálatlanok, így például a szkennelt PDF-ek, logok, képernyőképek, táblázatok vagy konfigurációs exportok eltérő módon értelmezhetők. Minél heterogénebb és rendezetlenebb az evidenciakészlet, annál kevésbé megbízható az automatizált feldolgozás.

A nagy mennyiségű dokumentáció kezelése önmagában is kihívás. Több ezer oldalnyi dokumentum, képernyőkép és logsor nem dolgozható fel egyetlen összefüggő szövegként, ezért az anyagokat darabolni, indexelni kell és metaadatokkal is el kell látni. A kontroll-hozzárendelés pontossága így nemcsak a modellen múlik, hanem a teljes feldolgozási láncon (a dokumentum-előkészítésen, kereshetőségen, chunkoláson, címkézésen és verziókezelésen) is. Ebben a folyamatban nem feltétlenül kizárólag nagy nyelvi modellek játszanak szerepet. A gépi tanulási megoldások is hasznosak lehetnek dokumentumtípusok osztályozásában vagy relevancia szerinti rangsorolásban.

A lehetőségek ugyanakkor jelentősek. Egy jól alkalmazott modell képes lehet releváns dokumentumok azonosítására, kontrollokhoz kapcsolódó szakaszok kiemelésére, bizonyítékok összekapcsolására és hiányosságok előzetes jelzésére. A szervezetek számára ez elsősorban előaudit és önellenőrzési támogatást jelenthet. Így gyorsabban áttekinthetővé válik, hogy mely kontrollokhoz milyen meglévő dokumentáció kapcsolható, és hol vannak hiányok. Ez csökkentheti az audit-előkészítés idejét és segítheti az evidenciák rendszerezését.

Ugyanakkor a modellek nem helyettesítik a szervezet önismeretét és szakmai döntéseit. Fennáll a „false confidence” veszélye, amikor a modell magabiztosan ad szakmailag hibás választ. Egy szabályzat megléte nem bizonyítja például a jogosultság-felülvizsgálatok tényleges végrehajtását, ahogyan egy konfigurációs screenshot sem feltétlenül igazolja az éles működést. Ezért az eredményeket mindig előzetes hipotézisként kell kezelni, nem végleges megfelelőségi bizonyítékként. További fontos szempont az adatvédelem és információbiztonság, mivel az auditanyagok gyakran érzékeny adatokat, sebezhetőségi információkat vagy incidensnyomokat tartalmaznak.

Az auditor számára a modellek legnagyobb előnye az evidenciatömegben való gyorsabb navigáció és a kontrollonkénti evidenciatérképek előállítása lehet. Segíthetnek az elsődleges és másodlagos bizonyítékok elkülönítésében, az ellentmondások felismerésében és a mintavétel fókuszálásában. Az auditvélemény felelőssége azonban nem ruházható át a modellre. Az evidenciák értékelése továbbra is szakmai ítélőképességet, kontrollértelmezést és emberi validációt igényel. A modellek különösen problémásak

lehetnek, ha nem kezelik megfelelően a bizonyítékok időbeliségét vagy a kontrollok közötti finom különbségeket.

A modellek hatékonysága nagymértékben függ a megfelelő promptolástól is. Általános kérdések gyakran felszínes válaszokat eredményeznek, míg a pontos, kontrollspecifikus kérdések strukturáltabb és relevánsabb eredményeket adhatnak. Emellett a különböző modellek eltérően kezelhetik a hosszú kontextust, a bizonytalanságot vagy a strukturált válaszadást, ezért célszerű rugalmas, több modell használatára alkalmas architektúrában gondolkodni. A gyakorlatban elengedhetetlen a „human-in-the-loop" megközelítés, ahol a modell az információk feltárását és rendszerezését végzi, míg a végső értelmezés és minősítés emberi szakértői feladat marad.

A jövőbeni fejlődés egyik kulcsa a nyelvi modellek és strukturált adatmodellek kombinációja lehet. Strukturált auditadatok esetén a modellek sokkal pontosabban tudják összekapcsolni a kontrollokat, bizonyítékokat és megfigyeléseket. Gyakorlati példaként egy felhasználói jogosultságkezelési kontroll esetén a modell összegyűjtheti a kapcsolódó szabályzatokat, IAM-exportokat, ticketeket és felülvizsgálati listákat, azonban annak megállapítása, hogy a folyamat ténylegesen működik-e, továbbra is auditori feladat marad. Nagy szervezeteknél a modellek valódi előnye a skálázhatóságban jelentkezik, ugyanakkor az adatmennyiség növekedésével a téves összekapcsolások kockázata is nő. Emiatt a nagy nyelvi modellek auditkörnyezetben elsősorban támogató, előszűrő és rendszerező eszközként tekinthetők megbízhatónak, nem pedig önálló megfelelőségi döntéshozóként.

13

Incidenskezelés és válságkommunikáció

A kiberbiztonsági incidensek és más válsághelyzetek komoly kockázatot jelentenek egy szervezet működésére, hiszen nemcsak az informatikai rendszerek biztonságát, hanem az üzleti folyamatok folytonosságát, a pénzügyi helyzetet és a hírnevet is veszélyeztethetik. Az ilyen események kezelésére nem elegendő az ad hoc reakció: előre megtervezett lépésekre, kijelölt felelősökre és összehangolt kommunikációra van szükség. a kríziskommunikáció célja ebben az, hogy a szervezet a válság alatt is következetes, hiteles és kontrollált üzeneteket közvetítsen minden érintett felé.

A sikeres válságkezelés nem kizárólag technikai feladat: vezetői, jogi, PR és partnerkapcsolati szinten is összehangolt fellépést igényel. Ezért kiemelten fontos a felkészülés, a gyakorlatok, valamint a szerepek és felelősségek pontos meghatározása. Jelen fejezet ezeknek az általános kereteit ismerteti, és alapot teremt a később részletezett forgatókönyvekhez, jelentési kötelezettségekhez és kommunikációs feladatokhoz.

13. Incidenskezelés és válság-kommunikáció

Írták: Frey Krisztián, dr. Jeney Andrea, Nagy Ágnes Beáta dr. Novák Anett, Dr. Váczi Dániel

A kiberbiztonsági incidensek és más válsághelyzetek komoly kockázatot jelentenek egy szervezet működésére, hiszen nemcsak az informatikai rendszerek biztonságát, hanem az üzleti folyamatok folytonosságát, a pénzügyi helyzetet és a hírnevet is veszélyeztethetik. Az ilyen események kezelésére nem elegendő az ad hoc reakció: előre megtervezett lépésekre, kijelölt felelősökre és összehangolt kommunikációra van szükség. a kríziskommunikáció célja ebben az, hogy a szervezet a válság alatt is következetes, hiteles és kontrollált üzeneteket közvetítsen minden érintett felé.

A sikeres válságkezelés nem kizárólag technikai feladat: vezetői, jogi, PR és partnerkapcsolati szinten is összehangolt fellépést igényel. Ezért kiemelten fontos a felkészülés, a gyakorlatok, valamint a szerepek és felelősségek pontos meghatározása. Jelen fejezet ezeknek az általános kereteit ismerteti, és alapot teremt a később részletezett forgatókönyvekhez, jelentési kötelezettségekhez és kommunikációs feladatokhoz.

13.1. Általános keretek

A válságok jelentős hatással lehetnek egy szervezet működésére, hiszen nem csupán a napi operatív tevékenységet zavarhatják meg, hanem az üzleti, pénzügyi helyzetet, valamint a szervezet hírnevét is súlyosan érinthetik. Egy válság – például egy kiberbiztonsági incidens (avagy incidensközeli helyzet) vagy egy kibertámadás – legtöbb esetben váratlanul és hirtelen következik be. Kezelése nem illeszthető be a megszokott üzleti folyamatok keretei közé, hanem eltérő szervezeti hozzáállást és specifikus kommunikációs stratégiát igényel.

Ezért elengedhetetlen, hogy a szervezet tudatosan és előre felkészüljön a válsághelyzetekre. Egy jól begyakorolt, előre kidolgozott fogatókönyv lehetővé teszi, hogy az érintettek nyomás alatt is hatékonyan reagáljanak, megfelelő válaszokat adjanak a munkatársak, a partnerek és a közvélemény kérdéseire, kezeljék a stresszhelyzeteket, illetve az esetleges álhíreket. Így a szervezet képes a válság megoldására és a működés mielőbbi helyreállítására koncentrálni.

A kríziskommunikáció háromlépcsős modellje szerint a válság három fő szakaszra – időszakra – osztható:

- Prekrízis szakasz: a válságot megelőző időszak, amely a felkészülést, tudatosítást és megelőző intézkedések kidolgozását foglalja magában;
- Akut krízis szakasz: maga a válság időszaka, amikor gyors, célzott és koordinált reakciókra van szükség;
- Posztkrízis szakasz: a válság utóélete, amikor a helyreállítás, az értékelés és a tanulságok levonása történik.

Kiberbiztonsági incidensek esetében e szakaszok különösen jól elkülöníthetők, és szervezeti szinten is dokumentálhatók. Kiemelt jelentőséggel bír e tekintetben a kríziskommunikációs terv és az incidenskezelési szabályzat. Ezek a dokumentumok pontosan rögzítik:

- az egyes folyamatokért felelős személyeket vagy szervezeti egységeket,
- a követendő eljárásrendeket (protokollokat),
- valamint a kommunikációs üzenetek tartalmát és célcsoportjait.

A hatékony incidenskezelés és válságkommunikáció feltétele a rendszeres gyakorlatok

végrehajtása és folyamatos tudatosság növelés a munkavállalók szintjén. Emellett lényeges, hogy a korábbi incidensek és válságok tapasztalatai beépítésre kerüljenek a meglévő dokumentációs struktúrákba és sablonokba.

Jelen fejezet részletesen bemutatja a lehetséges gyakorlati forgatókönyveket kiberbiztonsági incidensek esetére, ismerteti, hogy milyen hatóságokat, szervezeteket kell, illetve célszerű bevonni az incidensek kezelése során, továbbá sablon mintákat is mellékel, amelyek gyakorlati útmutatóként szolgálnak arra vonatkozóan, hogy milyen információkat, kikkel és milyen formában kell megosztania a szervezetnek egy kiberbiztonsági incidens bekövetkezésekor.

Mindezek segítségével a szervezet képes felkészülten és proaktívan kezelni a válsághelyzeteket, minimalizálva azok negatív következményeit és elősegítve a gyors helyreállítás gyakorlati forgatókönyvének megvalósulását.

13.1.1 Gyakorlati forgatókönyvek

A gyakorlati forgatókönyvek fejezet két, egymást kiegészítő folyamatot mutat be, amelyek egy biztonsági incidens során párhuzamosan zajlanak: az incidenskezelési és a válságkommunikációs forgatókönyvet. Az incidenskezelés a technikai és szervezeti lépésekre összpontosít az észleléstől a helyreállításig, míg a válságkommunikáció célja a hatóságok, ügyfelek, partnerek, érdekelt felek és a nyilvánosság időbeni, pontos tájékoztatása a jogszabályi előírások betartásával. a két folyamat közös időkeretekkel és részben átfedő szereplőkkel dolgozik, így hatékonyságuk alapja a szoros összehangolás.

13.1.2. Incidenskezelés forgatókönyv

Az incidenskezelési forgatókönyv célja, hogy lépésről lépésre bemutassa a folyamatot az észleléstől a helyreállításon át az utóelemzésig, biztosítva a gyors, összehangolt és dokumentált reagálást. a forgatókönyv alapját azok a fő fázisok alkotják, amelyek az incidens észlelésétől és jelentésétől kezdve az értékelésen, a válaszreakciókon és az elhárításon át egészen a tanulságok levonásáig vezetnek.

0. fázis: Előfeltételek

Mielőtt a tényleges incidenskezelés megkezdődne, a szervezetnek rendelkeznie kell egy kidolgozott és tesztelt Incidens Reagálási Tervvel (IRT/IRP), kijelölt CSIRT- vagy IT-biztonsági csapattal, előre elkészített kommunikációs sablonokkal és kapcsolattartói listával, valamint naprakész hatósági elérhetőségekkel (például NKI/CSIRT-Hungary, NAIH).

1. fázis: Incidens észlelése és azonosítása (0–2 óra)

Ebben a szakaszban cél az esemény mielőbbi észlelése, az incidens bekövetkezésének megerősítése és a prioritás meghatározása. a folyamat automatikus vagy manuális riasztások feldolgozásával indul (pl.: SIEM rendszer, EDR), melyet gyors technikai vizsgálat (logok, hálózati forgalom) követ. a besorolás (kritikus, magas, közepes, alacsony) után szükség esetén a válságstáb azonnali összehívására kerül sor. Felelősök: IT-biztonság, CSIRT.

2. Fázis: Eszkaláció és első kommunikáció (2–6 óra)

A cél a kulcsszereplők (pl.: IT-vezetés, CISO, jogi osztály, felsővezetés) azonnali értesítése, valamint a hatóságok felé történő előzetes bejelentés (például NKI/CSIRT-Hungary felé 24 órán belül). Ekkor aktiválják a válságkommunikációs csoportot, validálják az első üzeneteket a szóvivői csatornák számára, és szükség esetén tájékoztatják az ügyfeleket, partnereket, beszállítókat. Felelősök: CISO, kommunikációs vezető, jogász.

3. Fázis: Elemzés és izolálás (6–24 óra)

Ebben a szakaszban felmérik az incidens hatókörét és intézkednek a további károk megelőzésére. Ez magában foglalja az érintett rendszerek izolálását, forenzikus vizsgálatot a támadási pont és a támadói tevékenység feltárására, valamint a kárfelmérést az adatvesztés és szolgáltatáskiesés mértékének meghatározásához. a vezetés és a hatóságok folyamatos tájékoztatása elengedhetetlen. Felelősök: IT-biztonság, forenzikus elemző, kommunikációs csoport.

4. Fázis: Helyreállítás és visszaállás (1–5 nap)

Cél az érintett rendszerek működésének biztonságos helyreállítása. Ez megbízható biztonsági mentésekből történő visszaállítással, biztonsági frissítések és új hitelesítő adatok bevezetésével történik. a helyreállítás során a munkatársak felé folyamatos, tényszerű és időszerű belső státuszfrissítéseket érdemes (és szükséges) adni, míg szükség esetén a szervezeten kívülre az ügyfeleket és a sajtót is tájékoztatni kell. Tudatosan figyeljünk arra, hogy a kommunikált információknak milyen hatása lehet. Kerüljük a felesleges részletek korai közlését és csak a szükséges, de elégséges tényeket közöljük. a kommunikáció hangnemében legyen meg a magabiztosság és a transzparencia. Törekedjünk a pánikkeltést elkerülésére. a cél a bizalom fenntartása és a szervezet helyzetkezelési képességének megerősítése a külső és belső szereplők szemében. Felelősök: IT Üzemeltetés, CISO, kommunikációs vezető.

5. Fázis: Jelentés és utóelemzés (1–30 nap)

A szervezet 72 órán belül részletes jelentést készít a hatóság felé, majd 30 napon belül zárójelentést állít össze az incidens okairól, a válaszlépésekről és a kockázatcsökkentési intézkedésekről. a „Lessons learned” megbeszélések során a tapasztalatok beépülnek a jövőbeli folyamatokba. Felelősök: CISO, jogi osztály, IT-biztonság, compliance.

6. Fázis: Javító intézkedések (1–2 hónap)

Ebben a szakaszban a cél az incidens során feltárt gyengeségek megszüntetése és a szervezet védelmi képességeinek megerősítése. Ide tartozik a sérülékenységek kijavítása, például biztonsági frissítések (patch-ek) telepítése és tűzfalszabályok módosítása, az incidenskezelési és kommunikációs terv aktualizálása, a dolgozók biztonságtudatosságának növelése (pl.: célzott phishing tréningekkel), valamint a partnerek és beszállítók biztonsági megfelelőségének felülvizsgálata. Felelősök: IT, HR, Beszerzés, Compliance. CISO.

7. fázis: Tanulás

Az incidens lezárását követően részletesen meg kell vizsgálni annak kialakulási okait és lefolyását, hogy azonosíthatók legyenek azok a pontok, ahol megelőzhető vagy mérsékelhető lett volna a hatás. a vizsgálat eredményeként szükséges intézkedéseket kell hozni a jövőbeni hasonló események elkerülésére vagy hatásuk csökkentésére.

+1 utólagos elemzés (Post-Mortem)

Ez magában foglalja az észlelési, reagálási és elhárítási folyamatok értékelését, a kapcsolódó dokumentáció újbóli áttekintését, a feltárt okok részletes elemzését, valamint az intézkedési terv felülvizsgálatát és szükség szerinti módosítását.

A felkészültség fenntartása érdekében ajánlott évente legalább egyszer asztali gyakorlatokat (tabletop exercises) és éles szimulációkat végezni, amelyek célja a csapat reakcióképességének tesztelése, a tervek kipróbálása, valamint a gyors és hatékony reagálás biztosítása. Alapvetően nem hagyható ki a legalább

félévenkénti mentés visszaállítás és ellenőrzés sem.

13.1.3. Válságkommunikációs forgatókönyv

A válságkommunikációs forgatókönyv célja, hogy amint a szervezet tudomást szerez az incidensről, az előre meghatározott időkeretek betartásával biztosítsa a gyors, összehangolt és jogszabályoknak megfelelő kommunikációt. a fázisoknál zárójelben feltüntetett idő számításának kezdete minden esetben az incidens észlelése.

1. Fázis: Kezdeti értékelés és döntéshozatal (0-2 óra)

Első lépésként az incidenskezelő csapat az előre meghatározottak szerint haladéktalanul tájékoztatja a felsővezetést, ideértve a legmagasabb szintű tisztségviselőket (C-szintű vezetők), a kommunikációs vezetőt és a jogi osztály képviselőit, az incidens jellegéről, súlyosságáról és lehetséges következményeiről. Ennek célja a gyors helyzetfelmérés és annak eldöntése, hogy szükség van-e a válságkommunikációs csapat aktiválására.

Amennyiben a helyzet ezt indokolja, az előre kijelölt válságkommunikációs csapat azonnal megkezdi a munkát. a csapat tagjai közé jellemzően a kommunikációs vezető, a PR-szakember, a jogi képviselő, a felsővezetői szóvivő és az IT vagy biztonsági kapcsolattartó tartozik. Feladatuk a kommunikációs tevékenységek összehangolása és a kulcsüzenetek meghatározása.

Ezzel párhuzamosan megkezdődik a NIS 2 szerinti első incidensbejelentés előkészítése a kijelölt szervezet az NKI felé, amelyet a tudomásszerzéstől számított 24 órán belül kell megtenni. a jogi és incidenskezelő csapat együtt dolgozik a jogszabályi megfelelőség biztosításán és a hatóság mielőbbi értesítésén.

2. Fázis: Információgyűjtés és üzenetkészítés (1-3 nap)

Ebben a szakaszban a válságkommunikációs csapat folyamatos kapcsolatban marad az incidenskezelő csapattal annak érdekében, hogy naprakész információkkal rendelkezzen az eseményről. Ide tartozik a támadás pontos okának feltárása, az érintett rendszerek azonosítása, az adatvesztés mértékének meghatározása és a helyreállítás állapotának nyomon követése.

Az összegyűjtött adatok alapján a csapat kialakítja a fő kommunikációs üzeneteket a különböző célközönségek számára. Az üzeneteknek hitelesnek, átláthatónak és a szervezet proaktív hozzáállását tükrözőnek kell lenniük.

Ebben a fázisban meghatározzák, kiket kell tájékoztatni, és milyen prioritási sorrendben. Kötelezően értesítendő a nemzeti felügyeleti hatóság (NKI), valamint szükség esetén más szabályozó szerv, például a nemzeti adatvédelmi hatóság (NAIH), ha adatvédelmi incidens is történt. Kritikus célcsoportnak számít a vezetőség, az alkalmazottak, a közvetlenül érintett ügyfelek és a kulcsfontosságú partnerek, érdekelt felek,-míg egyéb célcsoport lehet a média, a befektetők vagy a szélesebb nyilvánosság.

A szakasz része a NIS 2 szerinti részletes bejelentés elkészítése is, amelynek a tudomásszerzéstől számított 72 órán belül kell megtörténnie. Ez a dokumentum tartalmazza a támadás valószínűsíthető okait és hatásait, az eddig elvégzett intézkedéseket, valamint a további tervezett lépéseket.

3. Fázis: Kommunikáció és reagálás (3+ nap)

Ebben a szakaszban alapvető az információk rendszeres frissítésének biztosítása és a folyamatos tájékoztatás, miközben célszerű a közösségi média felületek folyamatos figyelése is.

A belső kommunikáció jellemzően az incidens észlelését követő 1–4 órában történik, amikor tájékoztatót küldenek a munkavállalóknak

a helyzetről, a válaszlépésekről, valamint az esetlegesen tőlük elvárt intézkedésekről. Ennek célja, hogy a munkatársak naprakész információval rendelkezzenek, fennmaradjon a belső morál, és megelőzhetők legyenek a téves információk és pletykák.

A külső kommunikáció, amelyre az incidens bekövetkezésétől számított 4–48 órában kerülhet sor, akkor indokolt, ha a nyilvánosság tájékoztatása elengedhetetlen, például széleskörű szolgáltatáskiesés vagy adatlopás esetén. Ilyenkor sajtóközleményt adnak ki, hivatalos tájékoztatást tesznek közzé a szervezet weboldalán és közösségi média felületein, valamint közvetlen üzenetekben tájékoztatják azokat az ügyfeleket vagy partnereket, akiket az incidens közvetlenül érint, például e-mail vagy levél formájában. Fontos feladat a médiavisszhang és a közösségi média kommentek folyamatos figyelése, a felmerülő kérdések megválaszolása, és szükség esetén a téves információk gyors és pontos korrigálása.

Mindeközben folyamatos kapcsolattartás történik a hatóságokkal, különösen az NKI-val, amelynek további frissítéseket kell küldeni minden új információ vagy jelentős helyzetváltozás esetén, ezzel biztosítva a NIS 2 folyamatos bejelentési kötelezettségének teljesítését.

4. Fázis: Utólagos értékelés és fejlesztés

Az incidens lezárása után a válságkommunikációs csapat részletesen elemzi a teljes kommunikációs folyamatot, amelyet utólagos elemzésnek, vagyis post-mortemnek is nevezünk. Ennek során megvizsgálják, hogy az üzenetek mennyire voltak hatékonyak, a tájékoztatások időben történtek-e, milyen médiavisszhangot kapott az eset, és miként működött a belső kommunikáció.

Az így szerzett tapasztalatok alapján tanulságokat vonnak le, és konkrét fejlesztési javaslatokat dolgoznak ki a válságkommunikációs terv, valamint a kapcsolódó folyamatok finomítására. a felkészültség fenntartása érdekében a NIS 2 előírásainak megfelelően rendszeres időközönként, ajánlás szerint évente, asztali gyakorlatokat (table top exercises) és szimulációkat végeznek a válságkommunikációs csapat bevonásával a tervek tesztelésére és a gyors, hatékony reagálás képességének megőrzésére.

A folyamat része egy záró tájékoztató elkészítése is, amely átláthatóan összefoglalja, mi történt pontosan, milyen intézkedéseket tett a szervezet, és milyen jövőbeli lépéseket tervez. a hosszú távú bizalomépítés érdekében elindítható egy megerősített biztonsági programot bemutató kampány, transzparens auditfolyamat, valamint kérdőív formájában visszajelzések gyűjthetők az érintettektől. Amennyiben indokolt, a sajtókapcsolatok kezelésének részeként záró interjúkat is előkészítenek és lebonyolítanak.

Kulcsfontosságú Válságkommunikációs alapelvek NIS 2 Kontextusban

A válsághelyzetekben a kommunikáció minősége és sebessége közvetlen hatással lehet a szervezet megítélésére és a helyzet sikeres kezelésére. a NIS 2 irányelv által meghatározott szigorú bejelentési kötelezettségek mellett különösen fontos, hogy a kommunikációs tevékenység jól meghatározott alapelveken nyugodjon. Az alábbi irányelvek biztosítják, hogy az incidensekre adott kommunikáció gyors, összehangolt és bizalomépítő legyen.

- Gyorsaság: a NIS 2 által előírt 24 és 72 órás bejelentési határidők betartása kritikus. a kommunikációnak is gyorsnak, precíznek és pontosnak kell lennie.
- Átláthatóság és őszinteség: Ne próbáljuk eltusolni az incidenst. Az őszinte és transzparens kommunikáció hosszú távon építi a bizalmat.
- Konzisztencia: Minden kommunikációs csatornán ugyanazt az üzenetet kell közvetíteni. Ne legyenek eltérések.

- Empátia: Különösen, ha az incidens ügyfeleket vagy felhasználókat érint, az empátia kifejezése elengedhetetlen.
- Tényeken alapuló: Csak ellenőrzött információkat közöljünk. Kerüljük a spekulációkat.
- Proaktivitás: Ne várjuk meg, amíg a média vagy az érintettek kérdéseket tesznek fel. Kezdeményezzük a kommunikációt.
- Jogosultságok és felelősségek: Egyértelműen rögzítsük, ki miről és mikor kommunikálhat.
- Kapcsolattartás a hatóságokkal: Fenntartani a nyílt és együttműködő kapcsolatot a nemzeti felügyeleti hatósággal.

13.1.3. Gyakorlati szimulációk

A gyakorlati szimulációk az információbiztonságban és kockázatkezelésben olyan ellenőrzött gyakorlatok, amelyekkel egy szervezet teszteli, hogy valós támadás vagy krízis esetén hogyan reagálna. Ennek két nagyon gyakori formáját szokták alkalmazni:

- Tabletop gyakorlat
- Red Team / Blue Team gyakorlat

A gyakorlatok két különböző megközelítést képviselnek:

- A tabletop gyakorlat célja a döntéshozatali és koordinációs szimuláció vezetői és operatív szinten,
- A Red / Blue Team gyakorlat pedig technikai támadási szimuláció a védelmi képességek tesztelésére.

Mindkét gyakorlat az incidenskezelési és válságkezelési folyamat ellenőrzésére és fejlesztésére szolgál, azonban eltérő mélységben és módszertannal.

Tabletop gyakorlat – Ransomware incidens szimuláció

A tabletop gyakorlat egy forgatókönyv-alapú vezetői és operatív döntési szimuláció, amelyben a résztvevők egy hipotetikus incidensre reagálnak. A cél annak tesztelése, hogy a szervezet hogyan alkalmazza a korábban definiált incidenskezelési és válságkezelési folyamatokat.

Gyakorlat célja

- incidenskezelési terv tesztelése
- döntéshozatal és felelősségi körök vizsgálata
- kommunikáció és koordináció értékelése
- hiányosságok feltárása

Tabletop gyakorlat forgatókönyve:

Fázis	Szimulált esemény	Résztvevők adata	Kapcsolódás az incidenskezelési folyamathoz	Várható eredmény
1. Indító esemény	A SOC több szerveren gyanús titkosítási folyamatot észlel	Az IT és SOC értékeli a riasztást	Észlelés és azonosítás	Első incidensbesorolás
2. Incidens megerősítése	Megjelenik egy ransomware üzenet a fájlszerveren	A technikai csapat megerősíti az incidens típusát	Elemzés és validáció	Incidens hivatalos deklarálása
3. Eszkaláció	Több üzleti rendszer is elérhetetlenné válik	A vezetés aktiválja az incidenskezelési csapatot	Eszkaláció	Incident Response Team aktiválása
4. Operatív döntések	A fertőzés tovább terjed a hálózaton	A csapat dönt a hálózati izolációról és a rendszerleállításról	Kármentesítés	Fertőzés izolálása
5. Külső kommunikáció	Ügyfelek szolgáltatáskiesést jelentenek	PR és jogi csapat kommunikációs stratégiát dolgoz ki	Válságkommunikáció	Egységes kommunikáció
6. Szabályozói kötelezettségek	Adatszivárgás gyanúja merül fel	A jogi csapat értékeli a bejelentési kötelezettséget	Compliance	Hatósági értesítés előkészítése
7. Helyreállítás	A rendszereket biztonsági mentésből kell visszaállítani	IT csapat recovery tervet készít	Helyreállítás	Szolgáltatás helyreállítása
8. Kiértékelés	A gyakorlat lezárása	A csapat értékeli a reakciót és az együttműködést	Tanulságok levonása	Fejlesztési javaslatok

A hatóságokkal való kapcsolattartás tesztelését a hatóságokkal előzetesen egyeztetett módon is meg lehet tenni és ezt érdemes beilleszteni a fenti gyakorlatba, hogy ez is a mindennapok része legyen. A hatóságok is szoktak gyakorlatot kezdeményezni, ezekre való reagálás egy visszamérése a gyakorlati megvalósításnak.

Red / Blue Team gyakorlat – Célzott támadás szimuláció

A Red / Blue Team gyakorlat egy technikai támadás-szimuláció, amely során a támadó (Red Team) valós támadási módszereket alkalmaz, míg a védő (Blue Team) megpróbálja azonosítani és megállítani azokat.

Ez a gyakorlat közvetlenül teszteli:

- a detekciós képességeket
- az incidenskezelési reakcióidőt
- a biztonsági eszközök hatékonyságát

Red / Blue Team gyakorlat folyamata

Fázis	Red Team tevékenység	Blue Team feladata	Kapcsolódás incidenskezeléshez	Mérési szempont
1. Felderítés	Nyilvános információk gyűjtése a szervezetről	nincs aktív reakció	Megelőzés	Felderítés észlelhető-e
2. Belépési pont keresése	Phishing vagy sérülékeny szolgáltatás kihasználása	Email és hálózati riasztások monitorozása	Észlelés	Riasztás generálása
3. Initial Access	Egy felhasználói fiók kompromittálása	Gyanús bejelentkezések vizsgálata	Azonosítás	SOC reakcióidő
4. Jogosultság emelés	Adminisztrátori hozzáférés megszerzése	Endpoint és log elemzés	Elemzés	Privilege escalation észlelése
5. Laterális mozgás	Más szerverek elérése a hálózaton	Hálózati forgalom monitorozása	Kármentesítés	Lateral movement detektálása
6. Kritikus rendszer elérése	Domain controller vagy adatbázis kompromittálása	Incidens deklarálása és izoláció	Reagálás	Izoláció gyorsasága
7. Adatkivitel	Érzékeny adatok exfiltrációja	DLP és hálózati riasztások kezelése	Incidens kezelés	Adatszivárgás észlelése
8. Zárás	Red Team bemutatja a teljes támadási láncot	Blue Team elemzi a hiányosságokat	Tanulságok	Védelem fejlesztése

A két gyakorlat egymást kiegészítve vizsgálja tehát a szervezet felkészültségét, ellenálló képességét:

- a tabletop gyakorlat a vezetői és szervezeti reagálást teszteli
- a Red / Blue Team gyakorlat a technikai védelem hatékonyságát vizsgálja

Ezek rendszeres alkalmazása lehetővé teszi, hogy a szervezet ne csak dokumentált incidenskezelési tervvel rendelkezzen, hanem annak működőképességét is igazolja valósághű szimulációk segítségével.

13.1.4. Eddigi tanulságok

Az eddigi audit tapasztalatok alátámasztják, hogy minden kommunikációs lépést és döntést auditálhatóan rögzíteni szükséges, beleértve a lehetséges egyedi kommunikációs azonosítókat (Communication ID), jóváhagyási lépéseket és határidőket. Ezzel nem csak belső megfelelés biztosítható, hanem az esetlegesen hatósági felülvizsgálatok során is hiteles bizonyíték áll rendelkezésre. Ezeket az audit evidenciákat az auditorok rendelkezésére kell bocsátani.

Általános megállapítás, hogy azok a szervezetek tudják sikeresen kezelni a válságokat, ahol a vezetés, jogi és PR csapat az incidens korai fázisában kerül bevonásra a kommunikációs protokollok definiálásába és rendszeresen gyakorolják a fent említett módszereket. Ez előmozdítja a kontrollált, és jogilag megalapozott kommunikációt az érdekelt felek között.

A korai magyar audit és compliance tapasztalatok szerint a NIS 2-nek való megfelelés nemcsak technikai feladat, hanem szervezeti kultúra és irányítási feladat is, amelyben a kommunikáció minden szintje szerepel az auditálandó kontrollok között, így az ezeknek való megfelelés valós kihívás.

13.2. CSIRT jelentési kötelezettségek

A NIS 2 irányelv szigorúbb és részletesebb jelentési kötelezettségeket vezet be a kiberbiztonsági incidensek bejelentésére vonatkozóan. Az irányelv célja, hogy elősegítse a gyors, strukturált és következetes információáramlást az érintett szervezetek és az illetékes hatóságok között – különös tekintettel a nemzeti CSIRT-ekre.

Az irányelv 23. cikkében foglaltak szerint az alapvető és fontos szervezeteknek minden olyan eseményt jelenteniük kell, amely „jelentős hatást gyakorolhat a szolgáltatás nyújtására”.

A hazai szabályozás ezt implementálva bevezeti a jelentős kiberbiztonsági incidens fogalmát. Jelentősnek minősül például az az incidens, amely legalább 5%-os szolgáltatás-kiesést vagy bevételcsökkenést okoz, súlyos működési zavart idéz elő, pénzügyi vagy reputációs kárt okoz, illetve jelentős hátrányt jelent más szervezetek vagy személyek számára. Ezekről az eseményekről haladéktalanul tájékoztatni kell minden érintett szervezetnek a nemzeti kiberbiztonsági incidenskezelő központot (CSIRT-et), amely szükség esetén kötelező intézkedéseket is előírhat a helyzet rendezésére. A kisebb, nem jelentősnek minősülő események bejelentése ugyan önkéntes, de erősen ajánlott, hiszen ezek is hasznos információt nyújtanak a kibertér biztonsági helyzetének megértéséhez. Az ilyen bejelentések hozzájárulnak a nemzeti és EU-s ellenállóképesség növeléséhez, és elősegítik, hogy a hatóságok időben felismerjék a mintázatokat vagy új fenyegetéseket. A kötelező bejelentés elmulasztása jogkövetkezményekkel járhat, ezért minden szervezetnek célszerű világos belső eljárást kialakítania a jelentős és a kisebb incidensek megkülönböztetésére, dokumentálására és megfelelő kezelésére.

A jelentéstétel folyamatát az alábbi lépések mentén javasolt elvégezni[73]:

Kezdeti értesítés (Initial Notification)

Az incidens észlelését vagy a jelentős eseményről való tudomásszerzést követően a szervezetnek indokolatlan késedelem nélkül, de legfeljebb 24 órán belül értesítenie kell a nemzeti CSIRT-et vagy az illetékes hatóságot[74].

Az érintettek a bejelentéseket az alábbi hatósági felületeken tehetik meg:

https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/

https://nki.gov.hu/intezet/tartalom/incidens-bejelentes-anonim/
(anonim bejelentés lehetősége)

Ez a bejelentés elsősorban a korai figyelmeztetést szolgálja, még akkor is, ha a részletes műszaki információk még nem állnak teljeskörűen rendelkezésre. Az előzetes értesítésnek jeleznie kell, ha az esemény vélhetően rosszindulatú vagy jogellenes tevékenység eredménye, valamint, hogy van-e határokon átnyúló hatása.

Részletes jelentés (Incident Notification)

Az előzetes értesítést követően legfeljebb 72 órán belül részletes eseménybejelentést kell benyújtani. Ebben már szerepelnie kell az esemény elsődleges értékelésének, ideértve annak súlyosságát és hatását, továbbá a megfigyelt viselkedési mintákat, illetve (amennyiben elérhetőek) a technikai azonosítókat (például fertőzöttségi mutatókat). a bejelentésnek tartalmaznia kell minden olyan információt, amely alapján a hatóság vagy a CSIRT felmérheti az eset jelentőségét és kockázatát.

Közbenső jelentések

A hatóság vagy a CSIRT kérésére a szervezetnek közbenső jelentést kell készítenie, ha az incidens kivizsgálása vagy kezelése még folyamatban van. Ezekben frissíteni kell az esemény leírását, pontosítani az érintett rendszerek körét, valamint megosztani az addig megtett technikai, szervezési vagy kommunikációs intézkedéseket. Ez lehetővé teszi a hatóság számára az esemény folyamatos nyomon követését és értékelését.

Záró jelentés (Final Report)

A részletes eseménybejelentést követően legkésőbb 30 napon belül kötelező zárójelentést benyújtani. Ebben részletesen dokumentálni kell az esemény lefolyását, hatását, az azonosított kiváltó okokat, a reagálási és helyreállítási folyamatot, valamint azokat az intézkedéseket, amelyek a jövőbeli hasonló események megelőzését szolgálják. a zárójelentésnek ki kell térnie az esetleges határokon átnyúló következményekre is.

Folyamatban lévő események esetén

Amennyiben az incidens nem zárult le a zárójelentés határidejéig, a szervezet köteles benyújtani egy részjelentést az addig elért eredményekről. Ezt követően, az esemény végleges lezárásától számított egy hónapon belül szükséges a végleges zárójelentés beadása.

Együttműködési és adatszolgáltatási kötelezettségek

A jelentéstételen túl a NIS 2 előírja az érintett szervezetek aktív együttműködési kötelezettségét az illetékes hatóságokkal és a CSIRT-ekkel. Ez különösen a 21-22. cikkek alapján a következőket foglalja magában:

- az incidens kivizsgálásának támogatása,
- az eseményekkel kapcsolatos információk, naplók, dokumentációk rendelkezésre bocsátása,

73 Forrás: (EU) 2022/2555 irányelv – a hálózat- és információbiztonság magas szintjének biztosításáról az Unióban (NIS 2) Felhasznált részek: 23. cikk (1) és (3), 21–22. cikkek

74 Forrás: NBSZ NKI – Nemzeti Kiberbiztonsági Intézet (CSIRT) – https://nki.gov.hu

- a helyszíni ellenőrzések vagy auditok lehetővé tétele,
- technikai és vezetői szintű kapcsolattartás fenntartása a hatóságokkal,
- és adott esetben további intézkedések végrehajtása a hatóság kérésére.

A hatóság jogosult visszajelzést adni az alkalmazott intézkedések megfelelőségéről, és előírhat korrekciós vagy további megelőző intézkedéseket is.

Határidők és együttműködés

A jelentési és együttműködési kötelezettségek a szervezetek kiberbiztonsági ellenállóképességének alapfeltételei. a NIS 2 célja a hatékonyabb incidensreagálás és a tagállamok közötti koordináció erősítése. Az időben és megfelelő tartalommal teljesített jelentések, valamint a konstruktív együttműködés alapvető eszközei ennek a célkitűzésnek.

A határidők elmulasztása, a nem megfelelő vagy hiányos tájékoztatás, illetve az együttműködés megtagadása szankciókat, pénzbírságot és akár működési korlátozásokat is eredményezhet.

Bejelentési folyamat

2026. február 1-től kezdődően az NKI felületén (https://incidens.nki.gov.hu/customer) új incidensbejelentő űrlap érhető el. A bejelentés feltétele a bejelentő fél azonosítása, de van lehetőség anonim bejelentésre is. Az űrlap tartalmazza az incidenshez kapcsolódó legfontosabb információkat, melyek az alábbiak:

- incidenssel érintett szervezet,
- felügyelő hatóság,
- szervezet törzsszáma,
- bejelentő neve, telefonszáma, kapcsolattartó e-mail cím,
- incidens jellege,
- incidensben érintett rendszer megnevezése,
- incidens rövid leírása,
- fertőzöttsége mutatók,
- URL-ek, Domain-ek, Hash-ek,
- fájlok csatolása (legfeljebb 8 fájl).

A pénzügyi szervezetek külön űrlapon teljesítik az incidens bejelentést.

Trendek

Az NKI honlapján heti bontásban szerepelnek a bejelentett incidensek szám szerint. Trendelemzés alapján kimutatható, hogy kb. heti 55-60 bejelentés érkezik, mely 2025-26-os évben átlag 2.800-3.200 esetet jelent. Ez a létszám várhatóan hetei 65-70-re növekszik 2026-ban, így a várható incidens szám 2026-ban kb. 3.200-3.800 bejelentésre nő.

Ennek indoka lehet, hogy az adathalász támadások száma folyamatosan növekszik, ugyanakkor ezzel párhuzamosan nő az érintett szervezetek információbiztonsági tudatossága is. A tudatosság növelés eredményességét szervezeti szinten gyakorlati szimulációkkal és folyamatos teszteléssel lehet visszamérni. Az incidensek számát illetően pontos adatokat a bejelentések nagyszámú látenciája miatt nehéz adni.

13.3. Média, partnerek, felügyeletek, NAIH – mit, mikor, kinek?

Incidensek esetén a kommunikáció a szervezet által elfogadott kríziskommunikációs terv szerint kell, hogy történjen. Ez egy jól definiált forgatókönyvet határoz meg a tájékoztatás rendjével kapcsolatban. Az incidensekkel kapcsolatos kommunikáció egy pontos szervezeti protokoll szerint zajlik, a kommunikációs célcsoportok és a kommunikációs trendek ismeretében. a kommunikációs elemek

meghatározását kockázatértékelés előzi meg, mely részletesen reagál az esetleges sérülékenységekre, fenyegetésekre.

A kommunikáció részét képezi a válságstáb felállítása, amely egységes, összehangolt lépéseket tesz az érintettek hatékony tájékoztatása érdekében. a média, partnerek felügyeletek a külső kommunikációhoz tartoznak, hiszen a szervezeten kívül helyezkednek el.

A külső kommunikáció legfontosabb elvei az alábbiak:

Törvényesség és időbeliség

Ennek értelmében az illetékes hatóságok felé (NAIH, SZTFH, NKI) az incidenst a jogszabályi előírásoknak megfelelően, az ott meghatározott tartalommal és időben kell teljesíteni. Ez azért lényeges, mert ennek hiányában jogsértés következik be, mely szankciókat, illetve nem megfelelő incidenskezelést, majd bírságot vonhat maga után.

A NIS 2 irányelv szerinti információbiztonsági incidens jelentést az NKI-nek kell küldeni (lásd 13.2. fejezet). Ezzel szemben az adatvédelmi incidensre eltérő szabályok irányadók. Ez utóbbi esetben az incidenst NAIH kell bejelenteni. Az incidensbejelentésre az incidens bejelentésére az általános adatvédelemi rendelet 33-34. cikkében foglaltak az irányadók. Eszerint az incidenst az Adatkezelő a tudomásra jutástól számított 72 órán belül köteles bejelenteni, kivéve, ha az nem jár kockázattal a természetes jogaira és szabadságaira nézve. Ennek mérlegelése az Adatkezelő feladata.

Külső partnerek és ügyfelek tájékoztatása

A hatóságok felé tett bejelenetést követően szükséges a külső partnereket és ügyfeleket is tájékoztatni, a kontrollált transzparencia elve alapján. Ez minden esetben proaktív tájékoztatást jelent ellenőrzött környezetben. a szervezet elismeri az incidens tényét, azonban csak a legszükségesebb, jogi vezetők által jóváhagyott tényszerű információk közlésére kerül sor. Ez a proaktív kommunikáció bizalmat épít, ugyanis a kontrollálatlan kommunikáció komoly üzleti és reputációs károkat jelenthet a szervezetnek, melyet el kell kerülni. a kommunikáció során érvényre kell juttatni a felelősségvállalás elvét, amely annak kifejezését jelenti, hogy a szervezet komolyan veszi az incidenst, mint problémát, és törekszik annak mielőbbi megoldására és a jövőbeli hasonló esetek megelőzésére. Ez nem jelenti a felelősség elismerését jogi értelemben, hiszen a vizsgálat lezárultáig erről korai lenne nyilatkozni. Ez a megközelítés mutatja a szervezet elkötelezettségét az incidenskezelés irányában, egyúttal védi jogi pozíciót is.

A média és a sajtó tájékoztatása

A média és a sajtó tájékoztatása a szervezet kommunikációs stratégiájában meghatározott modell szerint történik. a kommunikációs modellválasztás kulcsfontosságú, mivel hosszú távon kihat a szervezet megítélésére és értékelésére. a kommunikációs modell kiválasztását az alábbi néhány példa segíti[75]:

- Sajtóügynökségi modell: ennek célja a közvélemény saját céljaink szerinti befolyásolása és jó imázs kialakítása.
- Tájékoztatási modell: a közvélemény tájékoztatására hiteles, valós információk alapján kerül sor.
- Kétirányú asszimetrikus modell: közvélemény csoportok meggyőzését célozza, ehhez kutatásokat használ fel.
- Kétirányú szimmetrikus modell: kölcsönös alkalmazkodás szervezeti modellje, ez dialógusban és hosszú távon gondolkodik.
- Személyi kultusz modell: ez a távol-keleti gyakorlatokat helyezi előtérbe, egy

75 Bor Olivér: Válságmenedzsment és kríziskommunikáció (NKE, EIV képzés, 2024-25. II. félév)

személyt preferál, és személyes befolyásoláson alapul.

- Kulturális közvetítő modell: ennek alapja a kulturális alkalmazkodás.

A sajtó tájékoztatása többféleképpen történhet: sajtóközlemény, hírlevél, tájékoztató anyag, sajtótájékoztató, avagy interjú formájában. Ezeket a szervezet a kríziskommunikációs tervben foglaltak szerint mérlegeli és eseti döntést hoz. a megfelelő kommunikációs modell, illetve stratégia megválasztása azonban kulcsfontosságú, hiszen a kommunikáció magát az incidenskezelés hatékonyságát is befolyásolja, egyúttal a szervezet reputációjára is komoly hatással van.

A kommunikáció lebonyolítására célszerű szóvívót igénybe venni, ő a szervezet hangja és szimbóluma egy személyben. Fontos, hogy jól felkészült személy legyen, aki ismeri a szükséges kommunikációs technikákat, mert a nem megfelelő fellépés könnyen súlyosbíthatja a válsághelyzetet. a szóvívő felelőssége a pontos, következetes információátadás a célzott személyi kör részére. Ez a sikeres válságkezelés egyik mérföldköve.

13.4. Vezetői, PR és jogi szereplők bevonása

A kiberbiztonsági incidensek a szervezetek reputációjára komoly hatással lehetnek, így az ezzel kapcsolatos klasszikus IT megközelítés túlhaladott, a kérdést több szakterület együttműködésében kell értelmezni.

A kommunikációs csatornák belső körét a vezetők, PR és jogi szereplők képezik. Ők a válságstáb tagjai, tehát az incidensmenedzsment fontos részei.

Vezető

A vezetői felelősségvállalás az incidensek tekintetében elengedhetetlenül fontos, mivel a szervezet vezetője dönt a stratégiai válaszlépések elfogadásáról és az incidenskezelés módjairól, többek között a külső partnerekkel való együttműködésről is.

Ez a vezetői felelősségvállalás valamennyi NIS 2-vel kapcsolatos folyamaton tetten érhető, hiszen a biztonsági osztályba sorolást[76] és a kockázatértékelést is vezetői jóváhagyás kell, hogy kövesse. Ezzel összhangban a hatékony döntéshozatal érdekében az információbiztonságot érintő minden információt a lehető legrövidebb időn belül meg kell osztani a felsővezetéssel.

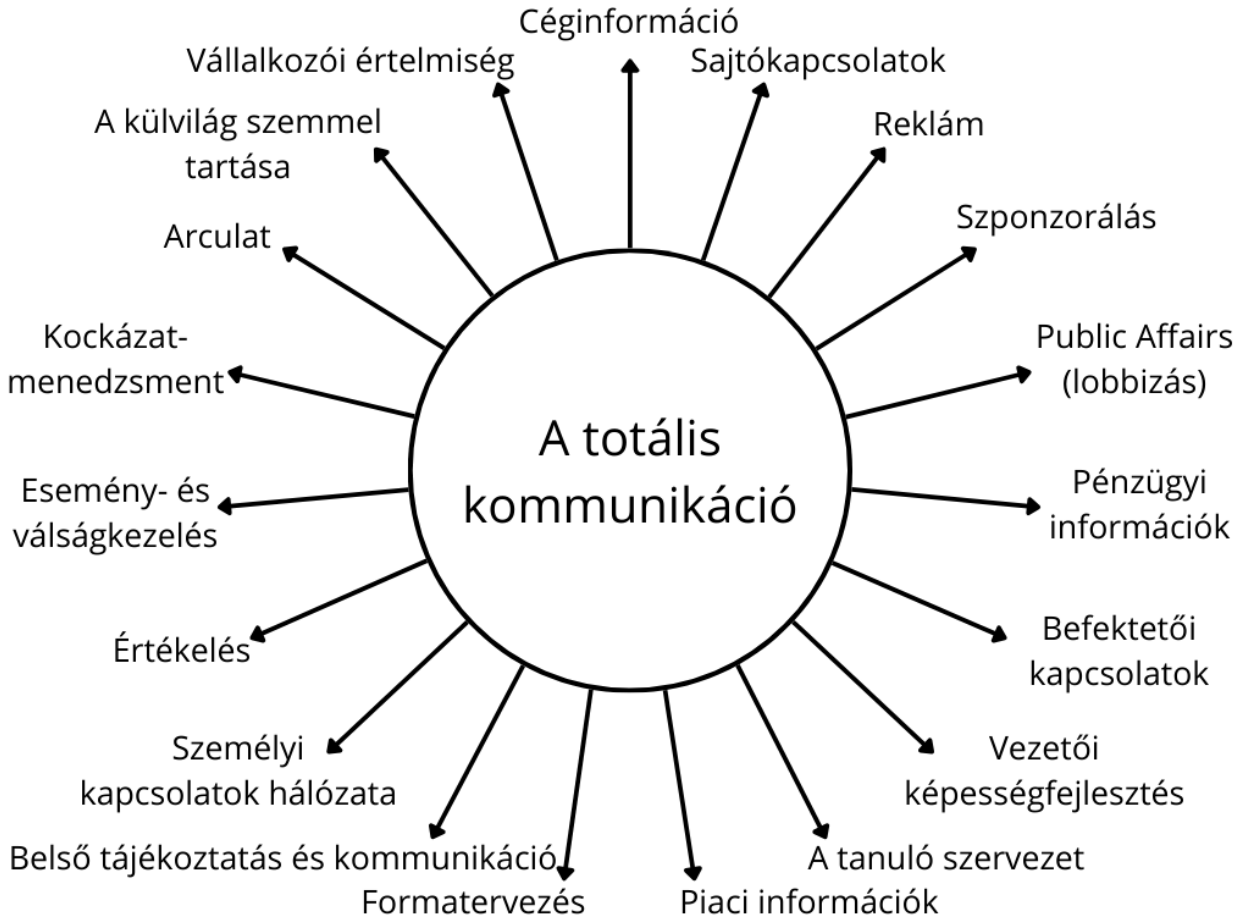
Mivel a kiberbiztonsággal kapcsolatos dokumentumok, folyamatok, működési modellek elfogadása alapvetően vezetői kérdés, így a válságkezelésnek a szervezet vezetője is aktív részese.

A Kiberbiztonsági tv. szerint a szervezet vezetője jelöli ki az elektronikus információs rendszer biztonságáért felelős személyt, vagy a szervezeten kívüli személlyel megállapodást köt (IBF). a döntéshozatalt megelőzően a vezető ugyanakkor kikérheti az információbiztonsági vezető szakmai álláspontját, aki alternatívákat fogalmazhat meg, a döntés joga azonban a vezetőt illeti.

A felelősség kérdését szabályozó dokumentumok a kiberbiztonsági audit vizsgálat tárgyát képezik, ennélfogva különleges jelentőségük van.

Az alábbi ábra a szervezeti kommunikáció integrált szemléletét tükrözi, kiemelve a kommunikáció egyes részterületeinek fontosságát. a szervezeti kommunikáció tehát vezetői, PR és IT szakemberek kölcsönös együttműködését feltételezi, különös tekintettel incidensek bekövetkezése esetén.

76 Kormányrendelet



Bor Olivér: Válságmenedzsment és kríziskommunikáció c. tananyagában használt ábrája alapján (NKE, EIV képzés 2024-25. II. félév

PR szerepe

A társadalmi kapcsolatok (Public Relations, továbbiakban: PR) részleg az incidenskezelés egyes fázisaiban különböző szerephez jut: a felkészülési fázisban kialakítja és működteti, teszteli a lehetséges kommunikációs csatornákat, valamint részt vesz kiberbiztonsági gyakorlatokban.

Incidens bekövetkezte esetén az azonosítási fázis során részletes tájékoztatást kell kapjon a kommunikációs elemekről és a nyilvánossággal való kapcsolatfelvétel kérdéséről. a közzétételre kerülő tartalom és időzítés a felsővezetéssel külön egyeztetésre kerül.

Az incidens időtartama alatt kezeli az értesítéseket, sajtóközleményeket, üzeneteket, emellett a szervezeti arculat és hitelesség megőrzésére is törekszik.

A helyreállítási fázisban fontos kitérnie a helyreállítási lépésekre és ennek keretében az ún „lessons learned”, azaz a tanulságok levonása is megtörténik. Fontos kiemelni, hogy a PR csapat önálló döntési jogkörrel nem rendelkezik, hiszen egy jól meghatározott forgatókönyv szerint végzi tevékenységét. Ennek a forgatókönyvnek az egyes elemeit a jogi osztály – a felsővezetővel egyeztetve – határozza meg.

Milyen a jó és tényszerű tájékoztatás? Rövid, tömör, közérthető, vagyis mi történt, mit tesz

a szervezet, és milyen következményekkel jár az incidens. E kritériumoknak az incidens és a szervezet jellege ismertében kell eleget tenni.

Jogi szereplők

A jogi közreműködést az incidensről való tudomásszerzést követően célszerű minél előbb igénybevenni, ugyanis a megfelelő jogi válaszlépések megfogalmazása így lehetséges a leghatékonyabban. Ennek feltétele, hogy a jogi osztályt az incidens részleteiről teljeskörűen tájékoztatni szükséges, illetve a válságstáb tagjai között a jogi szakterület is képviselteti magát.

A jogi válaszlépéseknek elsősorban az incidenst követően lehet kiemelt jelentősége, például a jogi felelősségi kérdések tekintetében. Mivel az incidensért való szervezeti felelősségvállalás a szervezet kártérítési felelősségét eredményezheti harmadik felek irányában, ezért a felelősségi kérdésekben a jogi osztály mindig egyeztet a felsővezetéssel.

Az incidens következményeként újabb dokumentumok készítése, esetlegesen a meglévők módosítása lehet indokolt, így a későbbi incidensek a jövőre nézve megelőzhetőek. Ennek részleteit a jogi szereplőknek kell megfogalmazni.

Az alábbi táblázat az incidenst követően bevonásra kerülő szereplőket tartalmazza, vagyis az incidens menedzsment a szereplők komplex együttműködését feltételezi. Erre azért van szükség, hogy a tanulságok levonása ne csak egy-egy szakterületen valósuljon meg, hanem átfogó megközelítéssel a későbbi incidenseket célzó megelőző intézkedések tervezésénél is érvényesüljön.

Egy jól kialakított Információbiztonsági irányítási rendszer része, hogy meghatározzuk, hogy az incidens evidenciákat milyen formában és mennyi ideig kell megőrízni.

Incidens utáni javaslatok

Incidens célpontja	ISP/ICP	CERT-ek	Jogi terület	Incidens forrása
Minden elérhető napló összegyűjtése	Naplók megőrzése	Kapcsolat közvetítése a helyi ISP/ICP felé	Jogi tanács megosztása	Események naplózása
Az incidens leírása	Segítség a műveleti intézkedésekben	Tanácsadás hasonló esetekben	Jogi eljárás támogatása	Gyanús felhasználók keresése
Az incidens tanulságainak megosztása / tanács, hogyan kerülhető el	A működési mechanizmus magyarázata	Tanulságok megosztása	Tájékoztatás az eredményről / jogi lépés javaslata	Tanács, hogyan kerülhető el a „támadóvá válás”

Tikos Anita: Incidensmenedzsment Elmélet c. tananyagában használt ábrája alapján (NKE, EIV képzés 2024-25. II. félév)

13.5 Digital Omnibus Package

Kiemelésre szorul az EU Bizottság Digital Omnibus Package 3 csomagja, amelynek hátterében az egyszerűbb és gyorsabb Európa kialakításának gondolata áll, a jogszabályok számának csökkenésével és a meglévő rendelkezések harmonizálásával. A javaslat ún. egyablakos ügyintézési pontot vezetne be, amely a NIS2, GDPR, eIDAS rendelet, és CER irányelvhez kapcsolódó incidens bejelentéseket egy egységes bejelentő rendszerbe integrálná. Ennek lényege szerint az érintett szervezeteknek csupán egyszer, egy űrlapon kellene bejelenteni az incidenst. Ez a javaslat szerint költséghatékonyabb, gyorsabb megoldást eredményezne mind hatósági, mind szervezeti oldalon egyaránt.

A bejelentési határidő adatvédelmi incidensek esetében 96 órára változna, a bejelentési kötelezettség pedig csak a magas kockázatú adatvédelmi incidensekre korlátozódna. Ez jelentősen szűkítené a bejelentendő incidensek körét.

Az adatvédelmi incidens kockázati besorolása az adatkezelő, az incidenssel érintett szervezet feladata, azonban a felügyeleti hatóság jogosult azt felülmérlegelni. Kérdéses, hogy a szervezeti kultúra fejlődését mennyiben mozdítaná elő a bejelentési rendszer ezirányú változása.

Fontos megjegyezni, hogy ez jelenleg csak tervezet, az egyeztetések folyamatban vannak, ennek hatályos joganyagba ültetése még hosszú, bizonytalan folyamat. Megfelelő alkalom lenne arra, hogy gyakorlatban elkülönüljenek a különböző kockázatú incidensek, és a szakmai gyakorlat is mélyülne.

14

Fizikai biztonsági intézkedések

Az elektronikus információs rendszerek biztonsága összetett megközelítést igényel, amely fizikai, informatikai és környezeti intézkedések összehangolásán alapul. a védelem szintjét mindig kockázatértékelés és üzleti hatáselemzés alapján kell meghatározni. a fizikai biztonság alapja a hozzáférések szabályozása: kockázati besorolás, beléptető rendszerek, időkorlátos engedélyek és a „legkisebb jogosultság elve”. a belépések dokumentálása és rendszeres felülvizsgálata nélkülözhetetlen.

A környezeti kockázatok mérséklésére mechanikus és elektronikus eszközök – például kamerák, tűz- és vízjelző rendszerek, szünetmentes áramellátás – alkalmazhatók, különösen a szervertermekben. a passzív tűzvédelem (tűzálló falak, nyílászárók, tömítések) és az egészségre nem ártalmas oltórendszerek további védelmet nyújtanak. a kimeneti eszközök (monitorok, nyomtatók, adathordozók) védelme szintén kulcsfontosságú, például zárt helyiségekkel és georedundáns tárolással. Mindezek mellett a külső szállítók kezelése is fontos.

14. Fizikai biztonsági intézkedések

Írták: Kalmár István, Lendák Imre, Lóth Tamás, Major Róbert, Dr. Tiszolczi Balázs Gergely

Az elektronikus információs rendszerek biztonságának fenntartása komplex megközelítést igényel, amelyben a fizikai biztonsági, informatikai és egyes esetekben egészségvédelmi intézkedések összehangolt alkalmazása kulcsfontosságú. a rendszerek, rendszerelemek érdekében alkalmazott védelem szintjének, konkrét eszközeinek meghatározása minden esetben az információbiztonsági, a fizikai biztonsági, és a munkavédelmi kockázatértékelések, továbbá az üzleti hatáselemzés eredményein kell, hogy alapuljon. a kockázatok csökkentésére különféle védelmi intézkedések alkalmazhatók, amelyek közül a szervezet saját működési környezetének és kockázati profiljának megfelelően választhat.

14.1 A fizikai biztonság szintjei

A fizikai biztonság szintjét a fizikai térben védeni kívánt rendszerek és azok elemeinek kritikussági szintje alapján határozzuk meg, és a következők lehetnek: maximális, magas, közepes, alacsony, minimális vagy nulla (azaz nincsenek semmilyen fizikai biztonsági intézkedések).

14.1. táblázat: A fizikai biztonság szintjei

Biztonsági szint	Biztonsági intézkedések (egymásra épülnek)	Példák
Nulladik	Nincsenek	Lakott településeken kívül, hajózási útvonalak
Minimális	Nyílt terek, megvilágítás, kerítések, falak	Lakóházak és lakások, lakott területek
Alacsony	Biztonságos kapuk, megerősített zárak, rácsos ablakok, riasztó	Kisebb üzletek, raktárak, szerver szobák
Közepes	A külső mellett belső védelem is: belső távfelügyelet, hangos riasztó, fegyvertelen őr, magas kerítés	Gyárak, bevásárlóközpontok, kisebb adatközpont
Magas	24/7 távfelügyelet, ellenőrzött be- és kilépés, fegyveres őrök, őrkutyák, kapcsolat rendvédelmi szervekkel	Börtön, hadiipar, elektronikai és gyógyszeripari üzemek, nagyobb (esetleg állami) adatközpontok
Maximális	24/7 harcedzett biztonsági szolgálat, biztonságos riasztó, (még) szigorúbb be- és kilépés, fegyveres élőerős külső reagálás	Katonai és nukleáris létesítmények, kiemelt biztonságú börtönök, különösen fontos kormányzati létesítmények, nagykövetségek

A táblázatban felsorolt szintek a lakott településen kívül tapasztalható nulladik szinttől, az átlagos családi otthonok minimális szintjén keresztül egészen a maximális biztonságig terjednek, mint amilyenek például egyes nagykövetségek, illetve katonai és nukleáris létesítmények. Fontos hangsúlyozni, hogy a táblázatban a biztonsági intézkedések egymásra épülnek, a magasabb szint örökli, esetleg bővíti és tovább fejleszti/erősíti az alacsonyabb szinten már bevezetett intézkedések halmazát.

A felsorolt fizikai biztonsági szintek, a vizsgált szervezet ágazatának általános és várható kockázati szintjének ismeretében szükséges minden egyes telephelyet, üzemet és fizikai végpontokat tartalmazó helyszínt felmérni, lehetőség szerint a fenn felsorolt biztonsági szintekbe sorolni és az alapján védeni. Ez például azt jelentheti, hogy egy kritikus gyártóüzem (pl. energetikai eszközök gyártása) várhatóan közepes biztonsági szintű lesz, illetve egy kisebb, regionális internet szolgáltató cég irodája és szerver szobája pedig alacsony besorolást kaphat az ahhoz tartozó biztonsági intézkedésekkel.

14.2 Biztonsági intézkedések

A fizikai hozzáférés kontrollálása és a szükséges technológiai intézkedések pontos és részletes meghatározása érdekében javasolt lehet az EIR-eket kiszolgáló létesítmények, helyiségek, területek és tárolók azonosítása, és ezek kockázat alapú besorolása, megkülönböztetése. Az ilyen területekre történő belépés szabályozására többféle megoldás alkalmazható, például elektronikus beléptető rendszerek, őrzött beléptetés vagy kísérettel történő hozzáférés. Az elektronikus beléptető rendszerek tervezésekor kritikus szempont az alkalmazott kártyatechnológia biztonsági szintje. Az alapvető, ún. „legacy” NFC megoldások ma már nem nyújtanak érdemi védelmet a célzott támadásokkal szemben.

A magas biztonsági igényű (EIR) rendszerek esetén a NIST SP 800-116 irányelveivel összhangban javasolt a modern, intelligens kártya technológiák alkalmazása, amelyek hardveres szinten gátolják a másolást, és támogatják a biztonságos, végpontok közötti titkosítást az olvasó és a vezérlőegység között is (OSDP protokoll).

A fizikai hozzáférés kontrollálása és a szükséges technológiai intézkedések pontos és részletes meghatározása érdekében javasolt lehet az EIR-eket kiszolgáló létesítmények, helyiségek, területek és tárolók azonosítása, és ezek kockázat alapú besorolása, megkülönböztetése. Az ilyen területekre történő belépés szabályozására többféle megoldás alkalmazható, például elektronikus beléptető rendszerek, őrzött beléptetés vagy kísérettel történő hozzáférés. a hozzáférési jogosultságok kezelése során célszerű szerepkör-alapú hozzáférés-kezelést alkalmazni, amelyet a kockázatelemzés során meghatározott hozzáférési szintekhez lehet rendelni. a jogosulatlan hozzáférés kockázatának csökkentésére alkalmazható a „legkisebb jogosultság elve”, amely szerint minden felhasználó kizárólag a munkaköréhez és feladatához szükséges hozzáféréseket kapja meg. a kiemelt biztonságú helyiségekbe történő belépés további kockázatot jelenthet, ezért az ilyen hozzáférések engedélyezését célszerű (magas besorolású rendszerek esetén kötelező) külön, akár írásbeli jóváhagyáshoz kötni. a belépési engedélyek időkorlátos kiadása, valamint a hozzáférések rendszeres felülvizsgálata szintén hozzájárulhat a kockázatok csökkentéséhez. Szerződéses partnerek, beszállítók beléptetése esetén a kísérettel történő beléptetés nyújt megfelelő biztonságot. a beléptetés visszakereshető módon történő dokumentálása elengedhetetlen egy incidens utáni vizsgálat vagy audit során. Egyes időszakok – például karbantartás, átszervezés vagy rendezvény – fokozott fizikai biztonsági kockázatot jelentenek. Ilyenkor külön figyelmet kell fordítani az ideiglenes belépések, áthidaló

megoldások és átmeneti védelmi hiányosságok kontrolljára.

A fizikai és környezeti kockázatok mérséklésére különféle elektronikus és mechanikus biztonságtechnikai eszközök alkalmazhatók. Az elektronikus eszközök közé tartozhatnak a videó megfigyelő rendszerek, behatolásjelző rendszerek, tűzjelző és tűzoltó rendszerek, valamint a környezeti paramétereket felügyelő szenzorok. a mechanikus védelem eszközei lehetnek zárak, lakatok, biztonsági rácsok, ajtók, egyéb épületszerkezetek, illetve biztonsági tárolók. a környezeti feltételek monitorozására alkalmazhatók hőmérséklet-, páratartalom- és folyadékszivárgás-érzékelők, amelyek riasztást küldenek, ha az értékek eltérnek az előre meghatározott tartománytól.

Ezek az eszközök különösen fontosak az egyes rendszerelemeket koncentráltan tartalmazó géptermekben (szervertermekben), ahol a környezeti paraméterek közvetlen hatással lehetnek az informatikai rendszerek működésére. Ezekben a helyiségekben már a tervezési fázisban célszerű olyan építészeti és egyéb műszaki megoldásokat alkalmazni, amelyek eleve kizárják a leggyakoribb kockázatokat. Ilyen lehet többek közt a csővezetékek, víz- és gázvezetékek elkerülése a határoló falazatokban, a tűzveszélyes technológiák kizárása a közvetlen környezetből, valamint a tűzálló épületszerkezetek és zárható, szükség esetén gáztömör helyiségek kialakítása. Az áramellátás biztonságának növelésére szünetmentes tápegységek, aggregátorok, valamint túlfeszültség-védelem alkalmazható. a kábelezés fizikai védelme (pl.: kábelcsatornák, zárt kábelutak, egyéb mechanikai védelem) szintén hozzájárulhat a rendszer rendelkezésre állásának és integritásának megőrzéséhez. a víz- és egyéb környezeti kockázatokból eredő károk megelőzésére – amennyiben azok építészeti megoldásokkal nem küszöbölhetők ki – többféle műszaki eszköz alkalmazása is indokolt lehet. Ilyen például a vízérzékelő rendszerek telepítése, amelyek képesek időben jelezni a szivárgásokat vagy vízbetöréseket, lehetőséget adva a gyors beavatkozásra. Az itt felsorolt követelményeket már a tervspecifikációban célszerű rögzíteni.

A tűzvédelmi kockázatok csökkentésére több szintű megoldás alkalmazható. Magasabb kockázat, illetve a technológia kritikus jellege esetén célszerű az automatikus tűzjelző rendszerekben nagy érzékenységű aspirációs érzékelőket alkalmazni, amelyek pontszerű, optikai érzékelőkkel és kettős jelzésverifikációval kombinálva tovább fokozzák a védelmet. Ez a megközelítés nemcsak a tűz korai észlelését teszi lehetővé, hanem segít a téves riasztások kiszűrésében is, így elkerülhetők a felesleges beavatkozások és az üzletmenet-folytonosság szempontjából nem kívánatos technológiai leállások.

Egyes esetekben – különösen, ha a védett területen személyzet is tartózkodik – további, például egészségvédelmi szempontokat is figyelembe kell venni. Ilyen környezetben előnyben részesíthetők az egészségre nem ártalmas, gázzal oltó rendszerek, amelyek nem igénylik a védett technológia előzetes áramtalanítását, és lehetővé teszik az emberi beavatkozást is az oltás közben vagy közvetlen utána.[77]

Az aktív tűzvédelmi rendszerek és berendezések mellett a passzív tűzvédelem is kulcsszerepet játszik a kockázatok csökkentésében. a helyiség határoló szerkezeteinek – beleértve a falakat, mennyezetet, aljzatot, ajtókat – meg kell felelniük a kockázati besorolás szerinti tűzállósági követelményeknek. a faláttörések, kábel- és gépészeti átvezetések tűzálló tömítésekkel való lezárása, valamint automatikus ajtóbehúzók és tűzjelző vezérlésű nyílászárók alkalmazása szintén javasolt. Ma már általános az alacsony füstkibocsátású halogénmentes burkolatú

77 Tiszolczi Balázs Gergely (2019). Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 19(2-3), 233–249.

kábelek használata, azonban javasolt ennek dokumentált alkalmazása.

A helyiség villamos hálózatát célszerű az épület többi részétől elkülönítetten, külön kapcsolható módon kialakítani. a helyileg telepített vészleállító kapcsolókat védeni kell az illetéktelen vagy véletlen aktiválástól, és úgy kell elhelyezni, hogy azok vészhelyzetben könnyen hozzáférhetők legyenek. a vészvilágítás kiépítése – amely áramszünet esetén automatikusan működésbe lép – tovább növeli a technológia és az azt üzemeltető személyzet biztonságát.

A védelmi intézkedések konkrét kiválasztása és alkalmazása a jó gyakorlat szerint egy olyan, a kockázatértékelés eredményei alapján adatokkal feltöltött műszaki védelmi katalógus alapján történik, amely lehetőséget biztosít a kockázatokhoz illeszkedő, költséghatékony és célzott intézkedések meghatározására. Ez a katalógus támogatja a tervezési, átalakítási és üzembe helyezési folyamatokat, beleértve az új létesítmények kialakítását, valamint a külső szolgáltatók által biztosított informatikai rendszerek védelmének megtervezését is. Az így kiválasztott és jóváhagyott intézkedések megvalósításáért és üzemeltetéséért a kijelölt felelős szervezeti egységek vagy – kiszervezett környezet esetén – a szerződött szolgáltatók felelnek. a megvalósítás során biztosítani kell az eszközök és rendszerek szakszerű telepítését, konfigurálását, valamint a működésük folyamatos felügyeletét, karbantartását és dokumentálását. a dokumentáció naprakészen tartása és az intézkedések rendszeres felülvizsgálata elengedhetetlen a megfelelőség és a működésbiztonság fenntartása érdekében. a karbantartás, felülvizsgálat során nemcsak az eszközök működőképességét, hanem a szabályzatok, folyamatok, jogosultságkezelés és auditálhatóság aktuális állapotát is értékelni kell. a fizikai védelmi rendszerek megbízhatóságát csak rendszeres teszteléssel és gyakorlatokkal lehet fenntartani. a tűz- és behatolásjelző rendszerek működését, valamint a riasztásokra adott válaszidőt előre meghatározott időközönként tesztelni kell. Emellett javasolt az üzemeltető személyzet részére rendszeres szituációs gyakorlatokat tartani, hogy vészhelyzet esetén azonnal és megfelelő módon tudjanak reagálni. (Fontos részletkérdés a tűzjelző rendszerek és a szünetmentes tápellátó berendezések működésének összehangolása, a gyakorlat és a valós vészhelyzet megkülönböztetésével).

Az egyes helyszíneken a szervertermi területen kívül vezetett adatátviteli hálózat védelme kiemelt fontosságú, mind a jogosulatlan hozzáférés (pl.: lehallgatás vagy szabotázs elkerülése), mind a véletlen eseményekből származó (pl.: nem szándékos) károk megelőzése tekintetében. Az informatikai kockázatértékelés és az üzleti hatáselemzés alapján megállapított bizalmassági és rendelkezésre állási igények szerint a szervezet fokozatosan vezetheti be az alábbi intézkedéseket:

- Zárható kábelrendezők, hálózati elosztók. Minden olyan helyiség, ahol hálózati eszközök vagy kábelek találhatók, legyen zárható, és kizárólag az arra jogosult személyek számára hozzáférhető. a kábeleket és hálózati eszközöket koncentráltan tartalmazó helyiségek, szekrények esetén behatolásjelző rendszer alkalmazása is indokolt lehet, amely riasztást generál nem engedélyezett hozzáférés esetén.
- Kábelcsatornák és védőcsövek alkalmazása: a falon kívül vezetett kábelek fizikai sérülésének megelőzése érdekében javasolt azok védőcsatornákban vagy csövekben történő elvezetése.
- Árnyékolt és optikai kábelek használata: Az elektromágneses interferencia csökkentése és a lehallgatás elleni védelem érdekében ajánlott árnyékolt réz- vagy optikai kábelek alkalmazása.
- Inaktív portok letiltása vagy fizikai lezárása: Az illetéktelen eszközcsatlakozások

megelőzése érdekében minden nem használt hálózati portot le kell tiltani vagy fizikai zárral kell ellátni. a gyártási területen levő portok leválasztása történhet a zárt térben elhelyezett elosztópanelen történt bontással is. a portokhoz történő hozzáféréseket naplózni kell, különösen ideiglenes vagy karbantartási célú használat esetén.

- Redundáns adatátviteli útvonalak kialakítása: a hálózati infrastruktúra megbízhatóságának növelése érdekében javasolt több, egymástól független és eltérő nyomvonalon vezetett adatátviteli útvonal kiépítése. Ez biztosítja a szolgáltatás folyamatosságát egy esetleges kábel- vagy eszközhiba esetén is.

Az adat és energiaátviteli utak védelme mellett az elektronikus információs rendszerek által előállított kimenetekhez való fizikai hozzáférés biztonsága is alapvető követelmény, különösen a bizalmas adatok megjelenítése, feldolgozása vagy továbbítása esetén. a szervezetnek biztosítania kell, hogy az ilyen információkhoz kizárólag az arra jogosult személyek férhessenek hozzá, és az információk ne váljanak illetéktelenek számára hozzáférhetővé – akár szándékos, akár véletlen esemény következtében. a kontroll megfelelő implementálásához első sorban az EIR input- és output pontjainak teljes körű azonosítása és dokumentálása szükséges. Kimeneti eszköz lehet minden olyan interfész, amelyen keresztül adatokat jelenítünk meg, nyomtatunk, rögzítünk, exportálunk vagy más rendszerekkel fizikai kapcsolatot létesítünk. Ide tartoznak a monitorok, nyomtatók, szkennerek, hangkimeneti eszközök, faxkészülékek, másolók, az egyes informatikai eszközök fizikai portjai stb.[78] Az informatikai kockázatértékelés és az üzleti hatáselemzés alapján megállapított bizalmassági és rendelkezésre állási igények szerint a szervezet az alábbi intézkedéseket vezetheti be:

- Zárt helyiségek alkalmazása: Az EIR kimeneti eszközeit zárt, nyilvános terektől elkülönített helyiségekben kell elhelyezni. Egy helyiség akkor tekinthető zártnak, ha azt ellenőrzötten kezelt kulccsal, és/vagy elektronikus beléptető rendszerrel védik. a fizikai védelem kiegészítése (pl.: behatolásjelző rendszer) alkalmazása indokolt lehet ott, ahol több informatikai kiszolgáló és/vagy hálózati eszköz, illetve azok perifériái koncentráltan vannak jelen.
- Monitorok és egyéb kijelzők elhelyezése és védelme: a kijelzőket úgy kell elhelyezni, hogy azokon megjelenített információk ne legyenek láthatók illetéktelen személyek számára. Ennek érdekében javasolt betekintés védő vagy adatvédelmi szűrő (privacy filter) használata, valamint a kijelzők pozicionálása úgy, hogy azok ne legyenek beláthatók közös vagy nyilvános terekből. Ez a követelmény kiterjed minden olyan kijelzőre is, amely biztonságtechnikai vagy üzemviteli célokat szolgál, például kódtasztatúrákra vagy térképes felügyeleti rendszerekre.
- Nyomtatók és másolók használata: a nyomtatás során biztosítani kell, hogy a kimenet kizárólag az arra jogosult személyhez kerüljön. Ez történhet személyes felügyelet mellett, vagy elektronikus azonosításhoz kötött nyomtatással. a kinyomtatott dokumentumokat a felhasználónak azonnal el kell távolítania az eszközből, hogy azok ne maradjanak felügyelet nélkül.
- Hangkimeneti eszközök kezelése: Érzékeny információk hangalapú megjelenítése esetén fejhallgató vagy fülhallgató használata javasolt. Amennyiben ez nem megoldható, a helyiség ajtaját zárva kell tartani, hogy

78 Dr. Tiszolczi Balázs Gergely (2023): Információbiztonság alapjai. Biztonságtechnikai rendszerek védelme, biztonságos üzemeltetése, egyetemi jegyzet.

a hangalapú információk ne legyenek hallhatók illetéktelen személyek számára.

- Adathordozók és biztonsági mentések védelme: a biztonsági mentések védelmének kulcseleme a földrajzilag elkülönített, georedundáns tárolás. Így egy helyi fizikai incidens – például tűz vagy fizikai megsemmisülés – nem veszélyezteti az adatok visszaállíthatóságát. a külön helyszíneken történő tárolás mellett fontos a mentések hozzáférésének kontrollja és az adatok mozgásának naplózása is.

Az elektronikus információs rendszereket tartalmazó létesítmények fizikai védelme nem csupán a hozzáférés korlátozását, hanem a hozzáférések folyamatos felügyeletét és az eseményekre adott gyors reakciót is magában foglalja. a fizikai hozzáférések felügyelete azt jelenti, hogy a szervezet képes észlelni, naplózni és kezelni minden olyan eseményt, amely a védett területekhez vagy technológiákhoz való jogosulatlan hozzáférésre utalhat. a fizikai biztonság fenntartása érdekében az alábbi felügyeleti intézkedések alakíthatóak ki:

- Folyamatos személyes jelenlét, vagyonvédelmi szolgálat biztosításával: a vagyonőri szolgálatnak folyamatosan (beleértve a szolgálatellátással kapcsolatos holtidőket is, úgy, mint pihenőidő kiadás, szociális szükségletek biztosítása stb.) meg kell valósítania a fizikai jelenlétet, különösen a kritikus infrastruktúrát tartalmazó területeken.
- Távfelügyeleti szolgáltatás igénybevétele: a riasztások fogadását és kezelését távfelügyeleti központ végezheti, amely szükség esetén kivonuló szolgálatot is biztosít. Ez ésszerű kompromisszum lehet az egyébként folyamatos felügyeleten kívül eső időszakokban pl.: munkaidőn kívüli időszakok.
- Elektronikus behatolásjelző rendszerek alkalmazása: Az elektronikus behatolásjelző rendszerek, valamint az analitikával támogatott kamerarendszerek képesek automatikusan riasztást generálni jogosulatlan hozzáférés esetén. a kameraanalitika alkalmazása lehetővé teszi a gyanús viselkedésminták automatikus felismerését is.
- Elektronikus beléptető rendszerek felügyelete: a beléptető rendszerek esetében figyelni kell a kényszerített nyitásokra, érvénytelen azonosítók használatára, valamint a hosszú ideig nyitva hagyott ajtókra. Ezek az események automatikusan naplózhatók és riasztást válthatnak ki.
- Riasztási események kezelése: Az elektronikus riasztások kezelésére többféle csatorna alkalmazható, például e-mail, SMS, távfelügyeleti integráció, diszpécserközpont vagy biztonsági műveleti központ (Security Operations Center – SOC). Fontos, hogy a riasztásokra a nap 24 órájában, az év minden napján biztosított legyen az élőerős, hatékony reagálás.

A fizikai biztonsági eseményekre adott azonnali reagálás mellett kiemelten fontos, hogy a szervezet képes legyen utólag is azonosítani a potenciális incidenseket. Ennek érdekében rendszeres időközönként át kell vizsgálni a fizikai belépésekkel kapcsolatos naplókat, és azokat célzottan elemezni kell, különösen akkor, ha azok jogosulatlan hozzáférés gyanúját vetik fel. Gyanús esemény lehet például a normál munkaidőn kívüli belépés, a szokatlanul hosszú bent tartózkodás, a nem megszokott területekre történő ismételt belépés, vagy az érvénytelen azonosítóval történő próbálkozás. a hosszú ideig nyitva hagyott ajtók, illetve a beléptető rendszerek által rögzített egyéb szokatlan mintázatok szintén figyelmet igényelnek.

A kamerarendszerek felvételeinek elemzése során azonosíthatók lehetnek olyan szabálytalanságok, mint a nem regisztrált vendégek jelenléte, a munkavállalók csoportos belépése

egyetlen azonosítóval, vagy az emberi figyelmetlenséget kihasználó besurranás (tailgating – amikor valaki egy másik személy mögött, azonosítás nélkül jut be a védett területre).

A szervezet információbiztonsági architektúrájába illesztett SIEM rendszer lehetőséget biztosít arra, hogy a fizikai biztonságtechnikai rendszerek eseményei – például behatolásjelzések, szabotázsjelzések, kényszerített belépések, érvénytelen mozgási riasztások, vagy kamerarendszerek által generált események – központilag, strukturált módon kerüljenek feldolgozásra. a naplóadatok valós idejű gyűjtése és korrelációja révén a rendszer képes automatikusan azonosítani a gyanús viselkedésmintákat, és azokra előre definiált szabályok (use case-ek) alapján riasztásokat generálni.

A SIEM-rendszer nemcsak az azonnali reagálást támogatja, hanem lehetőséget ad arra is, hogy a fizikai hozzáférési eseményekről rendszeres vagy eseti riportok készüljenek. Ezek a jelentések testreszabható szempontok szerint – például időszak, érintett terület, felhasználó vagy eseménytípus alapján – készülhetnek el, és automatikusan továbbíthatók az illetékes biztonsági vagy informatikai felelősök részére. Ez jelentősen növeli az átláthatóságot, támogatja a visszamenőleges vizsgálatokat, és hozzájárul a fizikai biztonsági incidensek megelőzéséhez, illetve gyors kezeléséhez.

Biztonsági követelmények külső szolgáltató által üzemeltetett elektronikus információs rendszerek esetén

Ha az elektronikus információs rendszerek külső szolgáltató által üzemeltetett infrastruktúrán (biztosított környezetben) kerülnek elhelyezésre, abban az esetben is elengedhetetlen a biztonsági követelmények érvényesítése. Amennyiben a szolgáltató kizárólag a fizikai környezetet biztosítja – például adatközponti infrastruktúrát, energiaellátást, klimatizálást –, míg az informatikai eszközök és rendszerek a megrendelő tulajdonában és üzemeltetésében maradnak, a biztonsági követelmények fókusza a környezeti feltételek megfelelőségére, a fizikai hozzáférés kontrolljára, továbbá az egyes incidensek kezelésére helyeződik.

A fizikai védelemre vonatkozó intézkedéseket – így például a beléptető rendszerek, az élőerős vagy egyéb elektronikus biztonságtechnikai, valamint a tűzvédelmi megoldások – a szerződésben részletesen dokumentálni kell. a szerződésnek ki kell térnie továbbá a szolgáltató mellékkötelezettségeire, a kártérítési felelősségre, valamint a megrendelő auditálási jogaira is, amelyek lehetővé teszik a biztonsági intézkedések rendszeres és célzott ellenőrzését. a szerződésben rögzíteni javasolt továbbá az exit feltételeket, amelynek célja annak biztosítása, hogy a megrendelő tulajdonában álló eszközök és adatok a szolgáltatási viszony megszűnésekor biztonságosan, sértetlenül és maradéktalanul elszállíthatók legyenek. a megállapodásnak tartalmaznia kell a hozzáférés biztosításának módját, az elszállítás technikai és logisztikai feltételeit, valamint a szolgáltató együttműködési kötelezettségét a folyamat során. Továbbá elvárás, hogy a szolgáltató a megrendelő kérésére hitelt érdemlően igazolja a környezetben esetlegesen tárolt adatok teljes törlését, és biztosítsa, hogy semmilyen másolat vagy hozzáférési lehetőség ne maradjon vissza a szolgáltatási időszak lezárását követően.

Abban az esetben azonban, ha a szolgáltató nem biztosít lehetőséget egyedi szerződéses feltételek rögzítésére – például általános szerződési feltételek (ÁSZF) alkalmazása esetén –, kizárólag olyan szolgáltató választható, aki (akár az az ÁSZF részeként biztosított) szolgáltatási szint megállapodásban (Service Level Agreement – SLA) egyértelműen, dokumentáltan és ellenőrizhető módon garantálja azokat a fizikai biztonsági és rendelkezésre állási feltételeket, amelyeket a szervezet saját kockázatértékelése alapján

meghatározott, és amelyeket a belső rendszerek esetében is érvényesít.

A hozzáférés-szabályozásnak átlátható, dokumentált folyamatokon kell alapulnia, amely biztosítja a jogosultságok megfelelő kiosztását, rendszeres felülvizsgálatát és a hozzáférési események naplózását. Az incidensek kezelésére vonatkozóan a jelentési kötelezettséget, a határidőket és az eljárási lépéseket szintén szerződésben kell rögzíteni.

Ezen követelmények teljesítése alapvető feltétele annak, hogy a hosztolt rendszerek biztonsága hosszú távon fenntartható és ellenőrizhető legyen.

15

Folyamatos fenntartás és megfelelő-ségmenedzs-ment

A kiberbiztonsági megfelelőség fenntartása nem egyszeri feladat, hanem folyamatos fejlesztést és alkalmazkodást igénylő folyamat. a szervezetnek nem elég teljesíteni a jogszabályi követelményeket, hanem biztosítania kell, hogy a működés során felmerülő változásokra, új fenyegetésekre és kockázatokra is időben reagáljon. Ez különösen fontos a NIS 2 irányelv és a magyar jogszabályi környezet elvárásai szempontjából, hiszen a jogalkotó a folyamatos kiber ellenállóképesség meglétét követeli meg. Ehhez elengedhetetlen a kockázatok folyamatos értékelése, a rendszeres belső auditok, valamint a tudatos, dokumentált intézkedési tervek kialakítása.

15. Folyamatos fenntartás és meg-felelőség- me-nedzsment

Írták: dr.Jeney Andrea, Kalmár István, dr. Novák Anett

15.1. Mit kell tennünk a következő 2 évben?

A fenntartáshoz számos elemet lehet és kell figyelembe venni, illetve integrálni a működő folyamatokhoz.

Ilyen mérőpont lehet (fő teljesítménymutatók – KPI) a folyamatos kockázatértékelés, BCP-DRP tervek, belső auditok, incidenskezelés, oktatások. Szintén fontosak az indikátorokból meghatározható és nyomon követhető levont következtetések, illetve tanulságok.

Javasolt negyedéves státuszriportok készítése, illetve a tervek végrehajtását megjelenítő felületek (dashboard) kialakítása és nyomonkövetése. a két év kis idő arra, hogy megfelelően felkészüljünk, mindeközben a jelenlegi állapotot is fenn kell tartani, illetve fejleszteni kell.

Az audit után, az auditmegállapításokat fel kell dolgozni és szükség esetén el kell készíteni azokat a mérföldköveket is tartalmazó intézkedési terveket, amelyek segítségével elérhetjük azt a felkészültségi szintet, amit elvár mind a jogalkotó, mind pedig saját magunk a szervezettől.

15.2. Intézkedési tervek kialakítása

Az MK rendelet támogató jelleggel ugyan, de megköveteli minden érintett és audit kötelezett szervezettől, hogy a kockázatkezelés során azonosított sérülékenységek és hiányok megoldására intézkedési tervet készítsen. Ezt szervezeti szinten kell előállítani és a megléte kötelező akkor is, ha a kötelezett szervezet csak egy EIR-t azonosított. Az intézkedési terveknek pontosnak, mérhetőnek, elérhetőnek, relevánsnak és időhöz kötöttnek (SMART – Specific, Measurable, Achievable, Relevant, Time-bound) kell lenniük. Fontos megjegyezni, hogy ezek nem statikus dokumentumok, belső felmérések eredményei alapján folyamatosan finomítani és aktualizálni szükséges őket.

Célszerű a kockázatalapú megközelítés, tehát minden intézkedés mögött konkrét, azonosított kockázat áll, amellyel foglalkozni kell. Az intézkedési terv pontos és egyértelmű megfogalmazása annak, hogy mit kell tenni. Nem minden hiányosság egyforma súlyú. Először azokat a feladatokat kell ütemezni, amelyek:

- Közvetlenül és kritikus módon érintik a jogszabályi megfelelést (pl.: hatósági jelentési kötelezettség).
- Jelentős kockázatot jelentenek a Szervezetre nézve (pl.: kritikus sebezhetőség).
- Előfeltételei más fontos tevékenységeknek.

A folyamatos kockázatkezelési ciklussal mérhetővé tesszük a szervezetet:

- Kockázat azonosítása,
- Kockázatértékelés,
- Intézkedések kidolgozása,
- Megvalósítás,
- Hatásmérés / újraértékelés.

Ez a ciklikus modell is biztosíthatja, hogy az intézkedések ne egyszeri, hanem fenntartható módon csökkentsék a szervezeti sebezhetőséget.

A prioritás szerinti sorrend kialakítása esetén az üzletmenetet leginkább veszélyeztető hiányosságok kezelése élvez elsőbbséget. a szervezet elsődlegesen ezekért a folyamatokért felelős.

Eredmény (Kimutatás): Mi lesz a tevékenység befejezett kimenetele? Ez lehet egy

dokumentum (pl.: frissített szabályzat), egy rendszerfunkció (pl.: bevezetett többfaktoros hitelesítés (MFA), egy képzés elvégzése vagy egy teszt sikeres lebonyolítása.

Felelős(ök) hozzárendelése a feltárt hiányosságokhoz, vagy a fejlesztendő területekhez. Minden egyes lépéshez kijelölt felelős(ök) és jóváhagyó(k) tartoznak; akik felügyelik és kontrollálják a folyamatokat.

Határidők meghatározása: Fontos, hogy a meghatározott határidők reálisak és betarthatók legyenek, amihez plusz erőforrások bevonása is szükséges lehet. Figyelembe kell venni a külső tényezőket (pl.: jogszabályi változás, újítások) és a belső erőforrás-korlátokat egyaránt.

Erőforrás-igények becslése: a feladatokhoz rendelni kell a becsült költségeket és a szükséges humán, technikai és egyéb erőforrásokat. Ez alapvető a költségvetés jóváhagyásához és az erőforrások allokációjához.

Az intézkedések négy fő kategóriába sorolhatók:

- Szervezeti intézkedések – pl.: információbiztonsági szerepkörök és felelősségi mátrix kialakítása.
- Technikai intézkedések – pl.: tűzfal- és végpontvédelmi megoldások fejlesztése, naplózás bevezetése.
- Folyamat- és szabályzatalapú intézkedések – pl.: incidenskezelési szabályzat frissítése, mentési eljárásrend módosítása.
- Tudatosságnövelő intézkedések – pl.: képzési programok, szimulációs gyakorlatok, phishing-teszt kampányok.

Az intézkedési terv kialakítása egy iteratív folyamat, ezért állandó felülvizsgálatot és a változó körülményekhez való alkalmazkodást igényel.

15.3. PPT érettségi szint követése

A kiberbiztonsági felkészültség és megfelelőség mérésére PPT (People, Process, Technology) érettségi modell alkalmazása javasolt. Ez segít vizualizálni a jelenlegi állapotot, a kívánt célszintet, és a fejlődési irányt. Az érettségi szintek általában 1-től 5-ig terjednek:

- 1. szint (Kezdő): a fenyegetésekre, illetve azonnali igényekre adott minimális reakciók, ad-hoc biztonsági intézkedések. Nincs egységes megközelítés vagy dokumentált folyamat. a tudatosság alacsony.
- 2. szint (Alapszintű): Néhány alapvető biztonsági kontroll működik, de nem rendszerezett Bizonyos feladatokat ismétlődően, bár még nem teljesen formális módon végeznek el. Néhány folyamat részben dokumentált, de nincs átfogó stratégia. a felelősségek nem megfelelően tisztázottak.
- 3. szint (Definiált): Meghatározott eljárások, szerepkörök, dokumentált folyamatok és azonosított kockázatok. Felelősségi körök tisztázottak, és a programba bevonták a kulcsfontosságú érintetteket. Van egy felismerhető biztonsági program. Ez a NIS 2 és a Kiberbiztonsági tv. minimum elvárása. Itt már rendelkezünk azokkal az alapvető keretekkel és dokumentációval, amelyek a megfeleléshez szükségesek, de a hatékonyság és az optimalizáció még hiányozhat.
- 4. szint (Kezelt és Mérhető): a definiált folyamatokat aktívan kezelik és mérhetőek. Teljesítménymutatókat (KPI-ket) gyűjtenek és elemeznek a program hatékonyságának értékelésére. Rendszeres tesztelés (pl.: incidenskezelési gyakorlatok, penetrációs tesztek) történik, és az eredményeket felhasználják a folyamatok javítására. a biztonság szerves része az üzleti

működésnek. Ez a szint az elérendő cél a következő 2 évben. Ezen a szinten a szervezet nem csupán „megfelel”, hanem aktívan és mérhetően biztosítja kiberbiztonságát, jelentősen csökkentve a kockázatokat és a jogi szankciók esélyét.

- 5. szint (Optimalizált): a kiberbiztonsági program folyamatosan fejlődik és proaktívan alkalmazkodik a változó fenyegetésekhez és üzleti igényekhez. a bevált gyakorlatokat beépítik, az automatizáció magas szintű. a kiberbiztonság a szervezeti kultúra szerves részévé vált, és stratégiai előnyként kezelik.

A megfeleléshez folyamatosan lépkedünk az érettségi skálán felfelé, egyre fejlettebb és komplexebb rendszerként kell újra gondolnunk a szervezetünket. Ehhez tudunk kell, hogy hol tartunk és mi az a szint, amit el tudunk érni, amennyiben megfelelően definiáljuk, priorizáljuk a feladatainkat.

A PPT-keretrendszer mentén végzett érettségértékelés segíti:

- az aktuális állapot objektív megértését,
- a gyenge pontok célzott fejlesztését,
- a fejlesztések priorizálását,
- a hosszú távú megfelelőség és védelmi szint fenntartását.

15.4. IT, biztonság és üzlet súlyozása

A NIS2 irányelv és annak hazai jogszabályi környezete holisztikus megközelítéssel a szervezet vezetésének szintjére emeli a kiberbiztonság kérdését. Ezért elengedhetetlen, hogy az intézkedési terv és annak végrehajtása során az IT, a biztonság és az üzleti területek közötti együttműködés kiemelt hangsúlyt kapjon.

a kiberbiztonsági megfelelőség nem csak technikai kérdés, hanem üzleti kockázatkezelési feladat is. Ennek megfelelően súlyozzuk a négy fő szakterület együttműködését:

- IT – technológiai eszközök, hozzáférések, frissítések, mentések.
- Biztonság – szabályzatok, kockázatelemzés, incidensmenedzsment.
- Üzlet – kritikus folyamatok, szolgáltatás-folytonosság, költség- és hatásbecslés.
- Ellátási lánc biztonsága

Az egyes területeket vizsgálva az alábbiak szerint csoportosíthatók:

- IT (Informatikai osztály): Az IT elsődleges feladata a rendszerek biztonságos üzemeltetése és karbantartása. Ide tartozik a technikai megoldások bevezetése, a frissítések és javítások kezelése, a monitorozó eszközök működtetése és a biztonsági incidensek technikai elhárítása. Az IT feladata, hogy a mindennapi működés során a biztonsági szempontokat érvényesítse.
- Biztonság (CISO és kiberbiztonsági csapat): a Biztonsági terület határozza meg a szakmai kereteket és a szabályozási elvárásokat. Feladata a biztonsági szabályzatok kidolgozása, a kockázatkezelési folyamat irányítása és az incidenskezelés koordinálása. Ők gondoskodnak a fenyegetési környezet folyamatos értékeléséről, a jogszabályi megfelelésről, valamint a hatóságokkal való kapcsolattartásról.
- Üzlet (üzleti egységek és felső vezetés): Az üzleti területek felelőssége a kritikus szolgáltatások, rendszerek és adatok azonosítása, valamint azok védelmének támogatása. a vezetők feladata, hogy a kiberkockázatokat beépítsék a döntéshozatalba, biztosítsák a szükséges erőforrásokat, és jóváhagyják a kiberbiztonsági stratégiát. a kiberbiztonság az üzleti működés része, amely hozzájárul a versenyképességhez és az ügyfelek bizalmához.

- Ellátási lánc: Az IT és a Beszerzés/Jogi terület szorosabb együttműködése szükséges a beszállítói kockázatok kezeléséhez. Nem elég, ha szervezet megfelelően védett, hanem olyan beszállítókkal szükséges együtt dolgozni, akik szintén megfelelő kiber védelemmel rendelkeznek, Az intézkedési tervnek tartalmaznia kell a beszállítói lánc auditját, mivel a szervezet biztonsága csak annyira erős, mint a legygyengébb partnere.

Ez a négy pillér csak szoros együttműködéssel és közös felelősségvállalással tudja biztosítani a fenntarthatóságot és a megfelelőséget.

Súlyozási elv a döntéshozatalban (irányadó arány) lehet:

- IT: 30%
- Biztonság: 40%
- Üzlet: 30%
- Ellátási lánc biztonsága 10%

Ez az arány tükrözi, hogy a biztonsági kontrollok nem gátolhatják az üzleti működést, viszont nem is rendelődhetnek teljesen annak alá. a hármas egyensúly biztosítása kritikus a hosszú távú fenntarthatóság érdekében.

Ez nem a költségvetésből származó ráfordítást tükrözi, hanem azt, hogy mely területet mennyire kell figyelembe venni a döntés során. Általános gondolkodásmód, hogy ez a terület csak pénzkidobás, egészen addig, amíg nem megfelelő döntés vagy felkészültség miatt incidens lesz a szervezetnél. A döntéshozatal során alkalmazott súlyozás garantálja, hogy a kiberbiztonság ne egy elszigetelt technikai projekt, hanem a szervezet ellenálló képességének (resilience) alapköve legyen.

15.5. SZTFH és/vagy NKI szerepe

A NIS 2 irányelv célja a kulcsfontosságú ágazatok kiberrezilienciájának megerősítése és egy egységes védelmi szint kialakítása az Európai Unióban. Ennek keretében új feladat- és hatáskörökkel ruházza fel a tagállami hatóságokat annak érdekében, hogy a jogszabályi előírásoknak való folyamatos megfelelés biztosított legyen.

A megfelelőségmenedzsment tevékenység elsődleges célja a folyamatos megfelelés biztosítása, és az ehhez kapcsolódó folyamatos kontrollrendszer kiépítése. E tevékenység magában foglalja különösen:

- a kockázatalapú megközelítés alkalmazását,
- az irányítási rendszerek dokumentált működtetését (pl.: IBIR) és felülbírálatát,
- az EIR-ek tekintetében az alkalmazott technikai és szervezési intézkedések rendszeres felülvizsgálatát,
- az érintettek (vezetők, IT-szakemberek, jogi felelősök) aktív részvételét és folyamatos képzését (tudásmenedzsment).

Ebben a folyamatban az SZTFH és az NKI, mint hatóság kulcsszerepet tölt be. Ennek megértéséhez a hatáskörök rövid bemutatása szükséges.

SZTFH

A Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) eredetileg a szabályozott tevékenységek – többek között a bányászat, a dohánykereskedelem és a szerencsejáték – hatósági felügyeletére jött létre, és e területeken rendelkezik hatósági jogkörökkel. a szervezet mandátuma később bővült a kiberbiztonsági megfelelés ellenőrzésével és felügyeletével, amelynek keretében az SZTFH vált a Kibertantv., majd a Kiberbiztonsági tv. hatálya

alá tartozó – jellemzően – piaci szervezetek kijelölt kiberbiztonsági hatóságává. E feladatkörök ellátása a Kiberbiztonsági tv. 23. § (1) bekezdésén alapul. a kiberbiztonsági hatáskörök gyakorlása az SZTFH szervezetén belül működő Kiberbiztonsági Igazgatóságon keresztül történik, míg egyes ágazatok – így a közigazgatás és a pénzügyi szektor – más hatóság felügyelete alá tartoznak.

Hatósági feladatait a Kiberbiztonsági tv. 24. §-a és a 3/2025. (IV.17.) SZTFH rendelet fejti ki részletesen. Ez igen részletes jogosultságokat takar. Csoportosítva ezeket: egyes jogkörök tekintetében megkülönböztetünk vizsgálati, ellenőrzési jogköröket, tehát mint hatóság, hatósági jogkörökkel rendelkezik (pl.: szankciókat szabhat ki), másrészt javaslattevő, véleményező szerv minden információbiztonsági kérdésben, ezen túlmenően fontos nyilvántartási jogkörei is vannak, hiszen a NIS 2 kötelezett szervezet a nyilvántartásba vételét az SZTFH-nál elektronikus úton kezdeményezi az érintettség megállapítását követő 30 napon belül.

Nyilvántartási jogköre keretében nyilvántartja a kiberbiztonsági auditorokat és az elektronikus információs rendszerek biztonságáért felelős személyek adatait. Emellett információbiztonsági tudatosságnövelő tevékenységekben is részt vesz, és a NIS 2 irányelv szerinti egyedüli tagállami kapcsolattartó pontként jár el.

Jogköreit vázlatosan az alábbi táblázat szemlélteti:

Nemzeti szabályozási keretrendszer – Állami felelősség (SZTFH)
NIS 2 ágazatokban működő szervezetek, kivéve: közigazgatás és pénzügy

nyilvántartás	megfelelés ellenőrzése	audit eredmény	audit ellenőrzése
intézkedés elrendelése	elhárításra kötelezés	rendkívüli ellenőrzés	rendkívüli audit
info. bizt. felügyelő	irányelvek, ajánlások	tudatosítás, gyakorlatok	felügyeleti díj
EGYÜTTMŰKÖDÉS – NEMZETKÖZI KÉPVISELET – MŰKÖDÉST TÁMOGATÓ ATTITŰD			

Bonnyai Tünde: Kiberbiztonsági szabályozás Európában c. tananyagában használt ábrája alapján (NKE, EIV képzés 2024-25. II. félév)

A NIS 2-t érintően saját rendeletalkotási jogköre révén a NIS auditok részletszabályaira vonatkozó döntést hoz.[79]

Minden érintett szervezet köteles az SZTFH felé bejelenteni a nyilvántartásba vétel során közölt adataiban bekövetkezett változásokat. Ennek elmulasztása bírságot vonhat maga után, amelyet a vonatkozó Kormányrendelet is rögzít. a folyamatos felügyelet keretében az SZTFH ezen túlmenően auditálással, kötelező

79 SZTFH rendelet, 2/2025. (01.31.) a kiberbiztonsági felügyeleti díjról

önértékelési jelentésekkel és automatizált jelentésbekérési rendszerekkel vizsgálja a szervezetek NIS 2 felkészültségét. Az önellenőrzés tényét a szervezetek dokumentumokkal igazolhatják a Hatóság felé.

Az SZTFH a NIS 2 auditok kapcsán komoly hatósági ellenőrzési jogköröket kap, így jogosult az audit során feltárt hiányosságok megszüntetése érdekében intézkedéseket elrendelni, rendkívüli auditot elrendelni (erős jogosítvány), szükség esetén helyszíni ellenőrzésről rendelkezni, illetve az audit dokumentumait bekérni és az audittal kapcsolatos minden információhoz hozzáférni. Hatósági jogkörei tekintetében a szankciók alkalmazása során egyedi mérlegelés alapján hoz döntést, itt a 3/2025. (IV.17.) SZTFH rendelet 6.§ (5) bekezdésében foglalt szempontokat mérlegeli (jogsértés időtartama, súlya, ismétlődő jellege, szándékosság, gondatlanság, érintett szervezet magatartása stb.)

Nemzeti Kiberbiztonsági Intézet (a továbbiakban: NKI)

Az NKI a Nemzetbiztonsági Szakszolgálat fennhatósága alatt működő szervezet, melynek jogköreit több jogszabály tartalmazza.[80] Kiberbiztonsági kérdésekben nemzeti kapcsolattartó pontként működik.

Feladata többek között a megelőzés biztosítása a kiberteret érintő fenyegetések és incidensek tekintetében, kezeli a kiberbiztonsági incidensbejelentéseket, fogadja, kivizsgálja és nyilvántartja azokat, a válsághelyzetek kezelése érdekében folyamatosan kapcsolatot tart más szervekkel, többek között részt vesz az EUCyLON rendszerben, sérülékenységvizsgálatokat végez, valamint koordinálja az ehhez kapcsolódó feladatokat, emellett tájékoztatási, tudatosító tevékenysége is van, melynek keretében elemzéseket, jelentéseket, kibergyakorlatokat szervez a tudatosság növelés és megelőzés érdekében, és nemzetközi együttműködésekben vesz részt (CSIRT hálózat).

80 https://nki.gov.hu/intezet/tartalom/magunkrol/

Nemzeti szabályozási keretrendszer – Állami felelősség (NBSZ NKI)
Közigazgatás, önkormányzatok, többségi állami befolyású szervezetek

szervezetek azonosítása	nyilvántartás	IBF nyilvántartás	bizt. oszt. validálás
megfelelés ellenőrzése	fejlesztések ellenőrzése	irányelvek, ajánlások	szabvány
elhárításra kötelezés	incidens utáni eljárás	info. bizt. felügyelő	tudatosítás, gyakorlatok
EGYÜTTMŰKÖDÉS – NEMZETKÖZI KÉPVISELET – MŰKÖDÉST TÁMOGATÓ ATTITŰD			

Bonnyai Tünde: Kiberbiztonsági szabályozás Európában c. tananyagában használt ábrája alapján (NKE, EIV képzés 2024-25. II. félév)

A közigazgatás, az önkormányzatok és a többségi befolyás alatt álló állami szervek kiberbiztonsági incidensei tekintetében rendelkezik hatáskörrel.

Az alábbi táblázat a jogköröket vázlatosan mutatja be:

A magyarországi kiberbiztonsági szervezeti intézményrendszer az állami rendszerbe betagozódva működik, az egyes intézmények hatásköreit megalapozó körülményeket mutatja az alábbi táblázat:

Nemzeti szabályozási keretrendszer – Állami felelősség (NBSZ NKI)
Szabályozás és felelősségi körök, kötelező együttműködés

NBSZ NKI	SZTFH	HKH	MNB *
Közigazgatás, önkormányzatok	NIS2 ágazatokban működő szervezetek	Honvédelmi célú rendszerek	Pénzügyi szervezetek
Többségi állami befolyású szervezetek	Kivéve: közigazgatás és pénzügy		

Bonnyai Tünde: Kiberbiztonsági szabályozás Európában c. tananyagában használt ábrája alapján (NKE, EIV képzés 2024-25. II. félév)

16

Kapcsolódó feladatok és megfelelések

A NIS 2 megfelelés szorosan kapcsolódik más jogszabályi kötelezettségekhez és iparági sztenderdekhez, ezért egységes megfelelési környezet részeként kell kezelni. a párhuzamos szabályozások – különösen a több ágazatban vagy határon átnyúlóan működő szervezeteknél – fokozott koordinációt, átlátható felelősségmegosztást és integrált stratégiát igényelnek.

Ez a fejezet áttekinti a NIS 2-vel összefüggő főbb szabályozási és tanúsítási rendszereket, ideértve a NAIH felé fennálló adatvédelmi kötelezettségeket, a pénzügyi szektor DORA rendelet szerinti elvárásait, valamint a nemzetközi információbiztonsági tanúsításokat. Kiemeli a NIS 2-vel való tartalmi átfedéseket és azokat a gyakorlati szempontokat, amelyek támogatják az összehangolt és hatékony megfelelést.

16. Kapcsolódó feladatok és megfelelések

Írták: dr. Albert Ágota, Apró William Z., Arató György, Biró Gabriella, Gedra János, dr. Jeney Andrea, Dr. Kiss Judit, Máté Márk, Dr. Váczi Dániel

16.1. NAIH kötelezettségek

A NIS 2 irányelv alkalmazása során a kiberbiztonsági megfelelés nem választható el az adatvédelemtől. A szervezetek működésében a kiberbiztonsági és adatvédelmi követelmények egyre szorosabban összekapcsolódnak, különösen az incidenskezelés területén, ahol egy biztonsági esemény gyakran személyes adatok érintettségével is jár. Ennek következtében a NIS 2 hatálya alá tartozó szervezetek számára az adatvédelmi kötelezettségek, különösen az incidensek kezelése és bejelentése, kiemelt jelentőséggel bírnak.

Az adatvédelmi incidens fogalmát az általános adatvédelmi rendelet (GDPR) 4. cikk 12. pontja határozza meg az alábbiak szerint: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Fontos hangsúlyozni, hogy az incidens fogalmának nem eleme a jogellenesség, a rosszhiszeműség vagy az adatkezelő közrehatása. A fogalom pontos ismerete kiemelt jelentőségű, mivel ez alapozza meg a kapcsolódó kötelezettségek teljesítését, és a téves jogértelmezés nem mentesíti az adatkezelőt a felelősség alól.

- Adatvédelmi incidens esetén az adatkezelő kötelezettségei röviden az alábbiakban foglalhatók össze:
- nyilvántartási kötelezettség [GDPR 33. cikk (5) bekezdés],
- bejelentési kötelezettség a felügyeleti hatóság felé [GDPR 33. cikk (1) bekezdés],
- az érintettek tájékoztatása [GDPR 34. cikk (1) bekezdés],

további technikai és szervezési intézkedések megtétele [GDPR 32., 24., 25. cikk].

A Hatóság gyakorlata alapján az adatvédelmi incidensek bejelentése több csatornán történhet, azonban a bejelentő rendszer használata egyértelműen domináns. A 2024. évi adatok szerint összesen 577 incidensbejelentés érkezett, amelyből 321 esetben az elektronikus incidensbejelentő rendszeren keresztül történt a bejelentés, míg a fennmaradó esetek hivatali kapun, e-mailen vagy postai úton érkeztek. A Hatóság célkitűzése a jövőre nézve a hitelesített elektronikus csatornák használatának erősítése és az e-mail alapú bejelentések visszaszorítása.

Az adatok alapján az incidensek száma az elmúlt években stabil, éves szinten mintegy 500–600 közötti értéket mutat, ugyanakkor az informatikai rendszereket érintő támadások aránya növekvő tendenciát mutat. Kiemelten érintett szektorok a biztosítási és egészségügyi ágazatok, ahol nagy mennyiségű és érzékeny személyes adat kezelése történik.

Fontos kiemelni továbbá, hogy a hatályos szabályozás alapján az adatvédelmi incidens bejelentése nem váltja ki más – például kiberbiztonsági – bejelentési kötelezettségek teljesítését, így adott esetben párhuzamos bejelentések megtétele is szükséges (pl. NKI irányába).

A NIS 2 esetében a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH, Hatóság),[81] speciális szerephez jut, hiszen az általános adatvédelmi rendelet 57. cikke szerinti jogkörében, mint felügyeleti hatóság jár el, s mint ilyen, független szervezetként az egyes adatkezelési tevékenységek tekintetében tanácsadó, javaslattevő és koordinatív feladatokat lát el. E feladatkörében figyelemmel kíséri az egyes adatkezelési műveleteket és az általános adatvédelmi rendelet alkalmazását. Ez a szervezetek részéről folyamatos együttműködési, kommunikációs kötelezettséget teremt annak érdekében, hogy az egyes adatkezelési műveletek során a személyes adatok védelme hatékonyan biztosított legyen.

A NAIH hatáskörét az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 38.§ (2) bekezdése tartalmazza. Eszerint a Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése.

A fentiek alapján a Hatóság hatáskörét a személyes adat érintettsége alapozza meg. Személyes adatnak minősül az általános adatvédelmi rendelet 4. cikk 1. bekezdése szerint az azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Ennélfogva a személyes adat fogalma igen tág, tehát pl.: név, az e-mail cím, a bankkártya adatok is ide tartoznak. Nem minősül személyes adatnak a jogi személy vagy más szervezet működésével, gazdálkodásával összefüggő információ, ezért az ilyen adatok nem részesülnek az adatvédelmi jogszabályok szerinti védelemben. a védelem azonban kiterjed a jogi személyek által kezelt személyes adatokra.

A NIS 2 hatálya alá tartozó szervezetekre – amennyiben személyes adatot kezelnek – adatkezelőként a GDPR szerinti kötelezettségek a többi jogalanyhoz hasonlóan ugyanúgy vonatkoznak. Ez magában foglalja a megfelelő dokumentáltság biztosítását (Adatkezelési Szabályzat, Adatvédelmi tájékoztató, Munkaszerződések, Incidens kezelési Szabályzat), ezáltal az elszámolthatóság elvének érvényesülését, az általános adatvédelmi rendelet 37. cikke szerinti adatvédelmi tisztviselő kijelölési kötelezettségét, és az adatbiztonság elvének érvényre juttatását már az adatkezelési műveletek megkezdését megelőzően, illetve a teljes adatkezelési folyamaton keresztül.

A Hatósággal történő kapcsolattartás elsősorban két aspektusból vizsgálható: (1) adatvédelmi tisztviselő kijelölése kapcsán, illetve (2) adatvédelmi incidensbejelentés kapcsán.

Az adatvédelmi tisztviselőt – az általános adatvédelmi rendelet 37. cikk (1) bekezdés szerinti kötelező esetek hiányában is – minden esetben célszerű kijelölni, annak érdekében, hogy a Hatósággal történő kapcsolattartást ellássa. Az adatvédelmi tisztviselő ugyanis egy szakmai kapcsolattartó pont, akinek a szervezet egyes adatkezelési tevékenységeit ismernie és menedzselnie szükséges, tevékenysége révén hozzájárul az adatvédelmi incidensek hatékony feltárásához, valamint biztosítja a szükséges kommunikációt a Hatóság felé. Az adatvédelmi tisztviselő bejelentését külön elektronikus űrlapon kell teljesíteni a Hatóság felé.[82]

81 A Hatóság önálló jogi személyiséggel rendelkező autonóm államigazgatási szerv, mely az adatvédelmi biztos jogutódjaként jött létre 2012-ben.

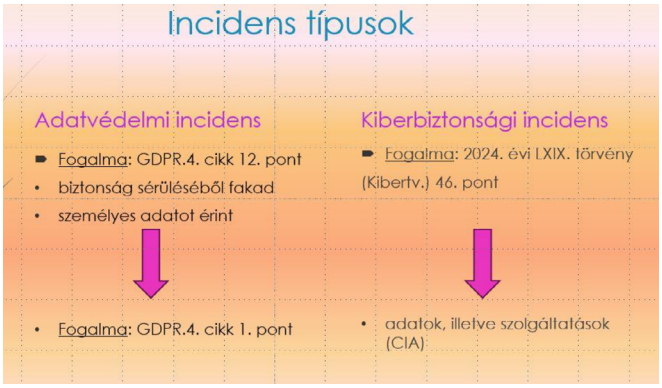
82 https://www.naih.hu/adatvedelmi-tisztviselo-bejelento-rendszer

Fontos kiemelni, hogy a Hatóság a fenti koordinatív, szakmai szerepkörén túlmenően hatósági jogkört is gyakorol az adatkezelési tevékenységek felügyelete során, amely magában foglalja az adatvédelmi jogsértések szankcionálását is. Ez kiterjed az általános adatvédelmi rendelet rendelkezéseinek nyomon követésére és kikényszerítésére kötelezéssel (pl.: adatkezelés megtiltása, korlátozása) vagy szükség esetén szankcióként bírság kiszabására is. a hatósági jogkör minden esetben jogi kikényszeríthetőséget jelent, ez biztosítja a döntés kötelező érvényét.

Adatvédelmi incidensbejelentés esetén is alapvetően hatósági jogkör érvényesül. Ez az általános adatvédelmi rendelet 4. cikk 12. pontja szerint mindig a biztonság olyan sérüléséből fakad, s amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

A NIS 2 érintett szervezetek kiberbiztonsági incidensei gyakran adatvédelmi incidensnek minősülnek. Fontos, hogy a két incidens típus – több hasonlósága ellenére – jelentős eltéréseket mutat.

Az alábbi ábra az adatvédelmi és kiberbiztonsági incidensek összehasonlítását szemlélteti:



Saját ábra (dr. Jeney Andrea – NKI -EIV Válságmenedzsment és kírziskommunikáció beadandó, 2024-25/II. félév)

Az adatvédelmi incidens tekintetében az érintett szervezet az átalános adatvédelmi rendelet 33-34. cikkében foglaltak szerint köteles eljárni.

A 33. cikk (1) bekezdése kimondja, hogy az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Itt kerül előtérbe a fent részletezettek szerint az adatvédelmi tisztviselő személye, aki köteles az adatvédelmi incidenst kategorizálni és a GDPR 33. cikk (1) bekezdés szerinti feltételek fennállta esetén a Hatóság felé az incidens bejelentését megtenni. Az incidensbejelentés kötelező tartalmi elemeit az általános adatvédelmi rendelet 33. cikk (3) bekezdése tartalmazza.

Az incidens kategorizálása tehát az érintett szervezet feladata, azonban a Hatóság jogosult annak felülvizsgálatára. a kategorizálásnak azért is van jelentősége, mert a valószínűsíthetően magas kockázatú incidensek esetében az érintett szervezet, mint adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. a tájékoztatás megtörténtét a Hatóság felé dokumentálni és igazolni szükséges.

Ezen túlmenően a szervezet köteles az adatvédelmi incidenseket nyilvántartani a GDPR 33. cikk (5) bekezdésében foglaltak szerint. a nyilvántartást a szervezet a Hatóság kérésére köteles rendelkezésre bocsátani. Ez a felügyeleti hatóság ellenőrzési jogosultságainak érvényesülését és alapelvi szinten az elszámoltathatóságot szolgálja. Könnyű belátni, hogy ezeknek az adminisztratív és szakmai feladatoknak

leghatékonyabban az adatvédelmi tisztviselő segítségével tud eleget tenni egy szervezet.

Az Infotv. 25/N.§ (2) bekezdése alapján a Hatóság évente megrendezi az adatvédelmi tisztviselők konferenciáját[83], amely az adatvédelmi tisztviselők rendszeres és interaktív kapcsolattartó fóruma. Célja az egységes jog-gyakorlat kialakítása az adatvédelemmel kapcsolatos jogszabályok értelmezése során.

A Hatóság fokozott célkitűzése a jövőre nézve az, hogy a proaktív védelem és fenntarthatóság elvét a fenti adatkezelések során is előmozdítsa, hozzájárulva ezáltal a NIS 2 szervezetek adatbiztonsági és kiberbiztonsági kockázatainak felismeréséhez és csökkentéséhez. Ez intenzív tudásmegosztást és az adatvédelmi joggyakorlat folyamatos fejlesztését jelenti.

16.2. DORA megfelelés

A NIS 2 irányelvvel egy időben jelent meg az Európai Unió hivatalos lapjában a DORA (Digital Operational Resilience Act) rendelet, azaz teljes nevén az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról. a DORA alapvető célja, hogy az egész Európai Unióban egységes követelményrendszert állítson fel a pénzügyi intézmények informatikai rendszereivel és környezetével kapcsolatban. Ezzel a céllal összhangban a DORA hatóköre a rendelet 2. cikkében felsorolt 20-féle pénzügyi szervezetre és a harmadik fél IKT-szolgáltatókra terjed ki. E szervezetek egy része a NIS 2 irányelv 3. cikkét átültető nemzeti szabályok értelmében alapvető vagy fontos szervezetnek is minősül, így esetükben a DORA mellett a NIS 2 is alkalmazandó.

Az alapvető vagy fontos szervezetként azonosított pénzügyi szervezetek tekintetében a DORA a NIS 2 irányelv vonatkozásában ágazatspecifikus uniós jogi aktusnak (lex specialis) minősül. Egyszerűbben fogalmazva, a NIS 2 hatálya alá első pénzügyi szervezetek esetében a DORA rendelkezései alkalmazandóak első sorban. Fontos különbség a NIS 2 és a DORA közt az is, hogy míg a NIS 2 irányelv és át kell ültetni a nemzeti szabályozásba, addig a DORA közvetlenül alkalmazandó Uniós rendelet, tehát pontosan ugyanaz a szabályozás vonatkozik minden olyan szervezetre, amire a hatálya kiterjed.

A DORA főbb részei a következők:

- IKT-kockázatkezelés,
- IKT-vonatkozású biztonsági események,
- Digitális működési ellenállóképesség tesztelése,
- Harmadik féltől eredő IKT-kockázatok kezelése,
- Információ megosztásra vonatkozó megállapodások,
- Kompetens hatóságok.

Az IKT-kockázatkezeléssel kapcsolatban és a többi elvárás kockázatokkal arányos megfogalmazása során a rendelet a NIS 2-ben is hivatkozott mikrovállalkozás, valamint kis-és középvállalkozás definíciókat alkalmazza.

A DORA és a NIS 2 által szabályozott területek között a gyakorlatban a legfontosabb átfedés az incidensek bejelentésének kötelezettsége. a DORA előírja az incidensek bejelentésének kötelezettségét a pénzügyi felügyeleti hatóságok (Magyarországon a Magyar Nemzeti Bank) részére, és ehhez részletes szabályokat, valamint egységes bejelentési sablonokat határoz meg. Ugyanakkor lehetővé teszi, hogy a NIS 2 hatálya alá tartozó szervezetek esetében az irányelv nemzeti átültetése során a szabályozó előírja a nemzeti CSIRT felé történő incidensbejelentést is. Magyarországon – több más EU tagországhoz

83 Erről részletesebben: https://www.naih.hu/adatvedelmi-tisztviselok-konferenciaja

hasonlóan – ennek köszönhetően a DORA hatálya alá tartozó intézmények a CSIRT részére is bejelentik a jelentős incidenseket. (A CSIRT-tel kapcsolatban lásd 14.2.)

16.3. ISO 27001

Az ISO/IEC 27000 szabványsorozat az információbiztonsági szabványok és iránymutatások családja. Az ebbe a családba tartozó szabványok az információbiztonsági irányítási rendszer keretén belül bevezetett információbiztonsági kontrollok végrehajtásával az információbiztonsági kockázatok kezelésének legjobb gyakorlatát biztosítják. Az ISO/IEC 27000 szabványsorozat több tucat információbiztonsággal és kiberbiztonsággal kapcsolatos nemzetközi szabványt tartalmaz, melyek közül talán a legfontosabb és legszélesebb körben használt az ISO/IEC 27001:2022 szabvány.

Az ISO/IEC 27001:2022 szabvány egy iparág független nemzetközi szabvány, amely az információbiztonsági irányítási rendszer (IBIR) kialakítására, működtetésére, felügyeletére és folyamatos fejlesztésére vonatkozó követelményeket határozza meg.

Az IBIR elsődleges célja a szervezet által kezelt adatok bizalmasságának (a védendő adatokhoz kizárólag az arra illetékes személyek férhessenek hozzá), sértetlenségének (védendő információk sérülésének – törlés, módosítás – felismerése, megelőzése és korrekciója), rendelkezésre állásának (a védendő információk legyenek rendeltetésszerűen elérhetőek és felhasználhatóak az arra illetékes személyek számára) biztosítása. a három alapelv magyar vagy angol nyelvű megfelelőjének kezdőbetűit összeolvasva, ezt szokták BSR vagy CIA elvként is hivatkozni.

Szervezeti háttér

Az ISO/IEC 27001:2022 szabványt a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) dolgozta ki közös munka eredményeként. a szabvány első változata 2005-ben került kiadásra, melynek azóta 2013-ban és 2022-ben történt verzióváltása.

A tanúsítás szabályozói háttere

Az ISO 27001 tanúsítás egy hivatalos eljárás, amely során egy független, akkreditált tanúsító szervezet ellenőrzi, hogy a szervezet információbiztonsági irányítási rendszere (IBIR) megfelel-e az ISO/IEC 27001:2022 szabvány követelményeinek.

Az ISO/IEC 27001:2022 szabvány „A” mellékletében részletezett információbiztonsági kontrollok megvalósítására vonatkozó iránymutatást az ISO/IEC 27002:2022 szabvány tartalmazza. Utóbbi tehát nem követelményeket tartalmaz, hanem gyakorlati útmutatást ad a kontrollok bevezetéséhez.

Az ISO 27001 tanúsítás hatóköre

A szervezetek maguk határozzák meg, hogy információbiztonsági irányítási rendszerük (IBIR) hatályát mire terjesztik ki, ugyanakkor magának az ISO 27001 auditnak a hatóköre megegyezik az IBIR hatókörével.

Belső audit

Az ISO/IEC 27001:2022 szabvány a teljesítményértékelés keretében tervezett időközönként előírja a szervezet számára belső audit végzését annak érdekében, hogy kiderüljön az IBIR megfelel-e a szervezet információbiztonság-irányítási rendszerére vonatkozó saját követelményeinek és az ISO/IEC 27001:2022 szabvány követelményeinek, illetve eredményesen van-e megvalósítva és karbantartva.

Tanúsító audit

A tanúsítvány 3 évre szól, de évente felügyeleti audit szükséges, valamint 3 év után megújító audit történik. Az auditálás személyesen történik.

Az ISO/IEC 27001:2022 szabvány és a NIS 2 kapcsolata

Az ISO/IEC 27001:2022 szabvány és a hatályos magyar jogszabályi előírások szerinti NIS 2 védelmi intézkedések között van átfedés mind a szervezeti, a személyi, a fizikai védelmi és a technológiai kontrollok tekintetében is.

Ugyanakkor

- az átfedés nem teljeskörű és nem feltétlen azonos megközelítésű,
- ISO/IEC 27001:2022 szabvány információbiztonsági, míg a NIS 2 megfelelés kiberbiztonsági vonatkozású,
- az egyezést befolyásolja, hogy a szervezet az IBIR hatókörét milyen terjedelemben határozta meg,
- az egyezést szintén befolyásolja, hogy a szervezet NIS 2 vonatkozásában milyen biztonsági szintnek köteles megfelelni, valamint
- ki kell emelni, hogy az ISO/IEC 27001 szabvány megvalósításának alapjául szolgáló ISO/IEC 27002:2022 szabvány gyakorlati útmutatás, míg a NIS 2 védelmi intézkedések jogszabályon alapuló kötelező előírások, amelyek alapját az NIST SP800-53r5 szabvány előírásai adják.

A fentiek alapján szervezetenként eltérő az átfedés mértéke, de akár ISO 27001 tanúsítvány birtokában vág bele egy szervezet a NIS 2 megfelelésbe, akár fordítva, célszerű egy mélységi GAP elemzéssel indítani a felkészülést, mert nagy valószínűséggel a megfelelés jól látható része már a szervezet rendelkezésére áll.

Szempont	ISO 27001	NIS2
Cél	Információbiztonsági irányítási rendszer (IBIR) kialakítása és működtetése	EU-szintű kiberbiztonsági megfelelés kritikus és fontos ágazatokban
Jogszabályi háttér	Nemzetközi szabvány (önkéntes, tanúsítható)	EU irányelv (2022/2555), kötelező a tagállamokban
Alkalmazási terület	Iparág független	Széles körű ágazatok: energia, egészségügy, közlekedés, digitális stb.
Alapja	ISO/IEC 27001:2022 ISO/IEC 27002:2022	Kiberbiztonsági tv. Kormányrendelet MK rendelet NIST SP800-53r5 szabvány
Audit jellege	Önkéntes, de strukturált és harmadik fél által végzett	Kötelező auditok és felügyeleti jelentések

Szempont	ISO 27001	NIS2
Tanúsítás	ISO 27001 tanúsítvány	Nincs tanúsítvány, hanem megfelelőségi kötelezettség
Fókuszterületek	Információbiztonság, minimális adatvédelem	Kiberbiztonság
Érintett szervezetek	Bármely szervezet, mérettől és ágazattól függetlenül	Kiberbiztonsági tv. 1 § (1) bekezdés alatti szervezetek, így többek között: állami és közszféra szereplők magánszektor kockázatos vagy kiemelten kockázatos ágazataiba tartozó szereplők
Kapcsolat	Szervezetenként eltérő az átfedés mértéke, de amennyiben ISO 27001 tanúsítvány birtokában vág bele egy szervezet a NIS 2 megfelelésbe, vagy fordítva, célszerű egy mélységi GAP elemzéssel indítani a felkészülést, mert nagy valószínűséggel a megfelelés jól látható része már a szervezet rendelkezésére áll.	

16.4. TISAX

Az ENX 2025. július elején egy 75 oldalas megfelelési útmutatót tett közzé, amely a TISAX-tanúsítással rendelkező vállalatok támogatását szolgálja. Tekintettel arra, hogy az ENX részletes elemzést hozott nyilvánosságra, így ezen fejezetben csak megemlítjük a TISAX és a NIS 2 megfelelés, másképpen TISAX rendszerben történő megfeleltetése lehetséges és hosszútávon célszerű együttesen kezelni.

A TISAX (Trusted Information Security Assessment Exchange) egy információbiztonsági tanúsítási rendszer, ami a német autóipari szövetség (VDA – Verband der Automobilindustrie) kezdeményezésére jött létre 2017-ben.

A tanúsítási rendszert kifejezetten az autóipar számára fejlesztették ki. a célja, hogy

- megbízható módon értékelje és biztosítsa a vállalatok – különösen a beszállítók – információbiztonsági szintjét a teljes gyártási ciklusban,
- egységesítse az autóipari szereplők információbiztonsági követelményeit,
- csökkentse az auditálási költségeket és komplexitást,
- lehetővé tegye az auditált eredmények kölcsönös elismerését a partnerek között.

A TISAX tanúsítvány elengedhetetlen az autóipari beszállítók számára, különösen azoknak, akik német vagy más európai gyártókkal dolgoznak együtt. Enélkül sok esetben nem is lehet gazdasági tevékenységet végezni az iparágban.

Szervezeti háttér

A TISAX gondozását az ENX Association egy független, nemzetközi szervezet végzi, amelyet 2000-ben alapítottak, és amelyben autógyártók, beszállítók és nemzeti autóipari szövetségek vesznek részt. a szervezet célja, hogy biztonságos és megbízható együttműködést tegyen lehetővé az iparági szereplők között, különösen az információbiztonság, a prototípusvédelem és az adatvédelem területén.

Főbb feladatai:

- a TISAX hivatalos irányító és felügyelő szervezete,
- közös iparági szabványok kidolgozása és fenntartása, mint pl a TISAX audit alapját képező VDA ISA kérdőív,
- TISAX szolgáltatók tanúsítása,
- ENX adatkommunikációs hálózat működtetése az autóipari szereplők között.

A tanúsítás szabályozói háttere

Az iparág független szabványok kialakítása a „one size fits all" megoldásra törekszik a személyre szabott megoldások helyett. Ezen igyekszik a VDA és az ENX változtatni azáltal, hogy a TISAX tanúsítást az autóipar sajátos igényeire szabja.

A TISAX tanúsítás az ISO/IEC 27001 szabvány alapjaira épül, de egyúttal kiegészül az autóipar specifikus információbiztonsági elvárásaival is, melyeket a VDA ISA (Information Security Assessment) kérdőív tartalmaz. Megjegyezendő, hogy a kérdőív illeszkedik a NIST 800-53 rev5 keretrendszerhez is.

A TISAX tanúsítás hatóköre és célkitűzése[84]

A TISAX audit hatókörének meghatározásakor az alapot mindig a szervezet információbiztonsági irányítási rendszere (IBIR) képezi, ugyanakkor a TISAX audit hatóköre ezen belül lehet szűkebb is mindaddig, amíg az lefedi a vállalat minden olyan területét, amely partner adatot, bizalmas információt kezel. Ennek kiegészítéseként a hatókör megválasztható standard és egyedi formában is.

Az audit célkitűzés megjelölésével a vállalat azokat az alkalmazandó követelményeket határozza meg, amelyeket információbiztonsági irányítási rendszerének (IBIR) teljesítenie kell. Ez teljes mértékben a vállalatnak a partnere nevében kezelt adatai típusán alapul. Jelen dokumentum publikálásakor az ENX TISAX résztvevőkre érvényes Kézikönyve (TISAX Participant Handbook) alapján 12 TISAX audit célkitűzés közül lehet választani 3 témakörben (információbiztonság, adatvédelem, prototípusvédelem), melyek közül legalább 1-et kötelező választani, de egyszerre többet is lehet.

A vállalat által megjelölt audit célkitűzés(ek) határozza meg az audit típusát, amely a jelen dokumentum kiadásakor az ENX TISAX résztvevőkre érvényes Kézikönyve (TISAX Participant Handbook) alapján az alábbi 3 változat lehet:

84 TISAX Participant Handbook

AL 1	Elsősorban belső célokat szolgál, lévén, hogy az auditor a kitöltött VDA ISA tábla meglétét ellenőrzi, azonban annak tartalmát nem értékeli és nem vizsgál további bizonyítékokat. Lényegében egy önértékelésnek felel meg, így alacsony bizalmi szintet élvez.
AL 2	Az auditor az önértékelés (VDA ISA) plauzibilitási ellenőrzését végzi el (az értékelési körbe tartozó összes helyszínre vonatkozóan), amit a bizonyítékok ellenőrzésével és az információbiztonságért felelős személlyel folytatott interjúval támaszt alá. Az auditor az interjút általában webkonferencián keresztül végzi, de kérésre személyesen is van rá mód. Alternatív megoldás lehet, ha a plauzibilitás ellenőrzés helyett az auditor teljes távértékelést végez. Ezt a módszert néha „2.5. értékelési szint” néven emlegetik.
AL 3	Az auditor átfogóan ellenőrzi, hogy a vállalat megfelel-e az alkalmazandó követelményeknek. Az önértékelést és a benyújtott dokumentációt használja fel az értékelés elkészítéséhez, valamint a helyszínen: • tervezett interjúkat folytat a folyamatgazdákkal; • megfigyeli a helyi körülményeket; • megfigyeli a folyamatok végrehajtását; • nem tervezett interjúkat készít a folyamatok résztvevőivel.

A TISAX és a NIS 2 kapcsolata

A TISAX és a NIS 2 irányelv között egyre szorosabb kapcsolat van, különösen az információbiztonsági megfelelés területén, mivel mindkettő célja a kiberbiztonság megerősítése, de eltérő megközelítéssel és hatókörrel.

A kapcsolatot tovább erősíti, hogy a TISAX végrehajtási iránymutatások között a VDA ISA megjelöli az NIST SP800-53r5 szabványt is, amelynek előírásain a hatályos magyar NIS 2 jogi szabályozás érdemben alapul. Tehát amennyiben a vállalat a TISAX megfelelését az NIST SP800-53r5 szabvány iránymutatását követve alakította ki, akkor az tekintélyes részben biztosíthatja egyúttal a NIS 2 előírásoknak történő megfelelését is és fordítva. Az átfedés mértéke ugyanakkor függ attól is, hogy NIS 2 vonatkozásában a vállalat milyen biztonsági szintnek köteles megfelelni.

Az ENX külön 75 oldalas megfelelési dokumentumot hozott nyilvánosságra 2025. július elején, amellyel támogatni kívánja a TISAX labellel rendelkező cégeket, vállalatokat.

Szempont	TISAX	NIS2
Cél	Autóipari információbiztonság értékelése és tanúsítása	EU-szintű kiberbiztonsági megfelelés kritikus és fontos ágazatokban
Jogszabályi háttér	Nem kötelező, de iparági elvárás	EU irányelv (2022/2555), kötelező a tagállamokban
Alkalmazási terület	Autóipari szereplők (OEM-ek, beszállítók, partnerek)	Széles körű ágazatok: energia, egészségügy, közlekedés, digitális stb.
Alapja	ISO/IEC 27001 + VDA ISA NIST SP800-53r5 szabvány	Kiberbiztonsági tv. Kormányrendelet MK rendelet NIST SP800-53r5 szabvány
Audit jellege	Önkéntes, de strukturált és harmadik fél által végzett	Kötelező auditok és felügyeleti jelentések
Tanúsítás	TISAX label	Nincs tanúsítvány, hanem megfelelőségi kötelezettség
Fókuszterületek	Információbiztonság, prototípusok védelme, adatvédelem	Kiberbiztonság
Érintett szervezetek	Főként autóipari beszállítók és partnerek	Kiberbiztonsági tv. 1 § (1) bekezdés alatti szervezetek, így többek között: állami és közszféra szereplők magánszektor kockázatos vagy kiemelten kockázatos ágazataiba tartozó szereplők
Kapcsolat	Amennyiben a vállalat a TISAX megfelelését a NIST SP800-53r5 szabvány iránymutatására kívánja alapozni, a NIS 2 jogszabályi előírásoknak történő megfelelés ehhez érdemi alapot nyújt. Az átfedés mértéke ugyanakkor függ attól is, hogy NIS 2 vonatkozásában a vállalat milyen biztonsági szintnek köteles megfelelni.	Amennyiben a vállalat a TISAX megfelelését az NIST SP800-53r5 szabvány iránymutatását követve alakította ki, akkor az érdemi részben biztosíthatja egyúttal a NIS 2 előírásoknak történő megfelelését is. Az átfedés mértéke ugyanakkor függ attól is, hogy NIS 2 vonatkozásában a vállalat milyen biztonsági szintnek köteles megfelelni.

16.5. A NIS 2 és a GDPR kapcsolata

A NIS 2 és a GDPR szabályozási területe eltérő, azonban a gyakorlatban gyakran átfedik egymást. Különösen igaz ez olyan elektronikus információs rendszerek esetében, amelyek személyes adatokat is kezelnek. a két szabályozás követelményeinek összehangolása elengedhetetlen a jogszerű és biztonságos működéshez, ehhez azonban ismernünk kell azokat a különbségeket, amelyek a két szabályozás eltérő céljából adódnak.

A NIS 2 és a GDPR célja

A NIS 2 irányelv *„a belső piac működésének javítása érdekében intézkedéseket határoz meg az egységesen magas szintű kiberbiztonság Unión belüli elérése céljából”*[85], *míg az irányelvet implementáló hazai törvény szerint „társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme, amely hozzájárul Magyarország és az Európai Unió biztonságához, ellenálló képességének és versenyképességének növeléséhez.”*[86]

A GDPR *„a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.”*[87]

Mindkét jogszabály kockázati alapú megközelítést alkalmaz, és előírja, hogy a szervezetek a tevékenységükhöz és a kockázati tényezőkhöz arányos technikai és szervezési intézkedéseket alkalmazzanak. Bár a két szabályozás célja eltér, sok esetben ugyanazon adatokra és rendszerekre egyidejűleg vonatkozik. Ezért kulcsfontosságú az összehangolt alkalmazásuk. A NIS 2 elsődlegesen az információbiztonságra, szolgáltatásfolytonosságra, a rendszerek védelmére, a kiberbiztonsági incidens-kezelési kötelezettségre fókuszál. A GDPR elsődlegesen az érintetti jogokra, a szükségesség-arányosságra, a célhoz kötöttségre, adattakarékosságra, korlátozott időbeni tárolásra, az adatvédelmi incidens-kezelési kötelezettségre, valamint a magánszféra védelmére koncentrál.

Amennyiben kétség merül fel, mely szabályozás előírásait kell elsődlegesen alkalmaznunk, a személyes adatok védelmét biztosító uniós rendelet, a GDPR közvetlenül alkalmazandó és elsőbbséget élvez a nemzeti vagy uniós irányelvi szintű szabályokkal szemben. Ugyanakkor mindkét szabályozás célját figyelembe kell venni, és a rendelkezéseket lehetőség szerint össze kell hangolni.

A NIS 2 és a GDPR találkozása

A NIS 2 irányelv hatálya alá tartozó szervezetek esetében bizonyos körülmények fennállása mellett szükségessé válhat a GDPR és a NIS 2 irányelvben meghatározott követelmények egyidejű teljesítése.

- Tipikusan ilyen helyzet áll fenn az alábbi esetekben: Az EIR személyes adatot is kezel (pl.: HR-rendszerek, ügyféladatbázis stb.)
- A szervezet a GDPR alapján adatkezelőnek / közös adatkezelőnek / adatfeldolgozónak minősül (pl.: munkavállalók alkalmazása, kamerarendszer üzemeltetése stb.)

---

85 AZ EURÓPAI PARLAMENT ÉS a TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv), 1. cikk (1) bekezdés

86 Kiberbiztonsági tv. preambulum [2]

87 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, „GDPR”), 1. cikk (2) bekezdés.

- kiberbiztonsági incidens a szervezet által kezelt személyes adatot is érint (pl.: adatvesztés, zsarolóvírus támadás stb.). Ez esetben mind a két jogszabályi alapján fennállhat az illetékes hatóságok felé a bejelentési kötelezettség, ezért célszerű olyan belső eljárásrendet kialakítani, amely mind a két jelentési kötelezettséget figyelembe veszi.
- olyan EIR esetében végzett kiberbiztonsági kockázatelemzést, mely rendszerben folytatott adatkezelésünk magas kockázatot jelent az érintettek jogaira és szabadságaira nézve[88] (pl.: munkavállalók megfigyelésére szolgáló kamerarendszer, GPS nyomonkövetésre alkalmazása stb.). a NAIH a honlapján közzéteszi azokat az adatkezeléseket, amelyek esetében kötelező adatvédelmi hatásvizsgálatot lefolytatnunk.[89]

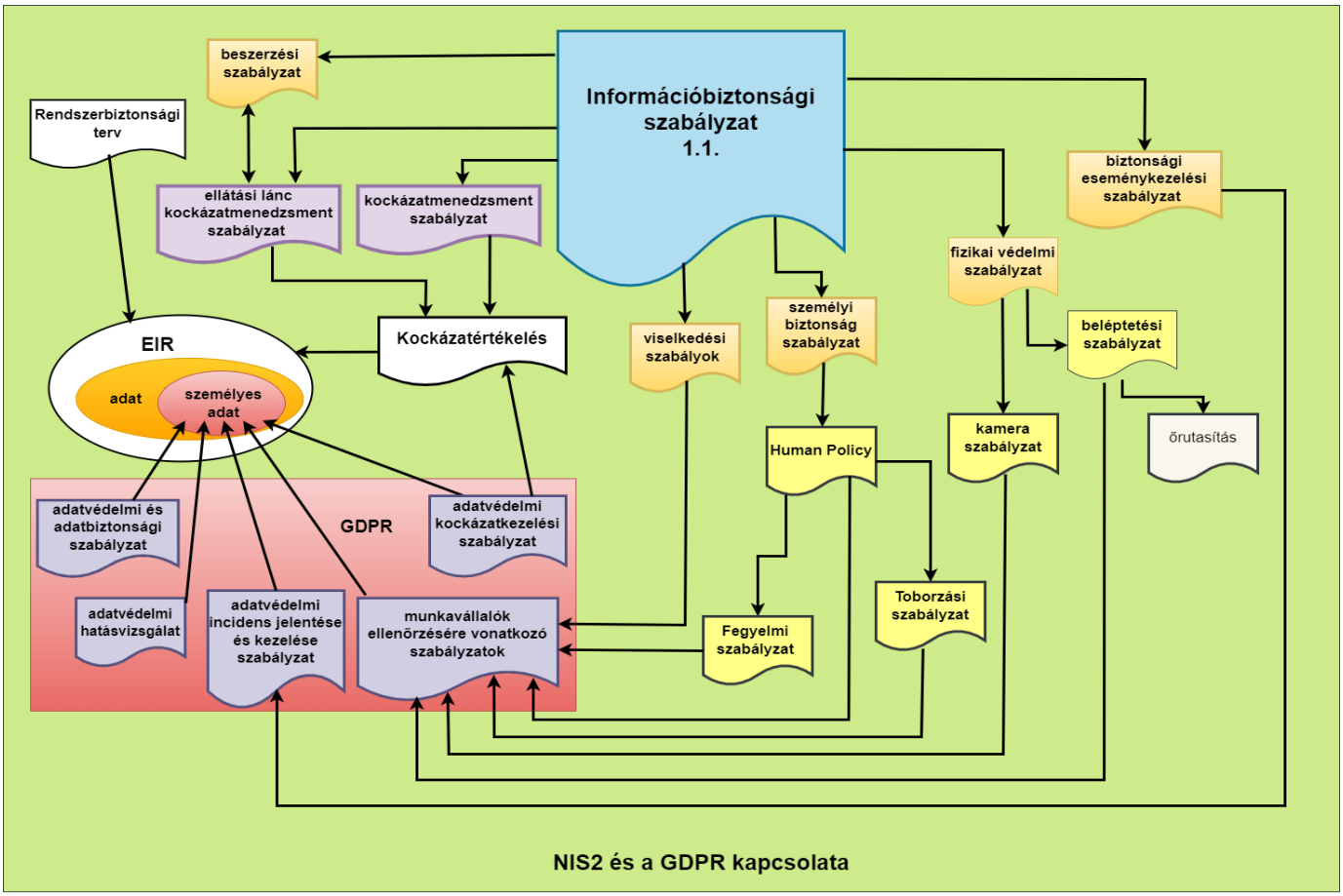
Mivel az incidensben személyes adatok is érintettek, a GDPR alapján az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásunkra jutott, be kell jelenteni a NAIH-nak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.[90] Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatnunk kell az érintett(ek)et is az adatvédelmi incidensről.[91]

88 GDPR 35. cikk (1) bekezdés

89 https://naih.hu/hatasvizsgalati-lista

90 GDPR 33. cikk (1) bekezdés

91 GDPR 34. cikk (1) bekezdés.



NIS2 és a GDPR kapcsolata

Incidenskezelés: kettős megfelelés példa: egy máshova nem sorolt gépgyártás miatt NIS 2 hatálya alá tartozó vállalat esetében egy zsarolóvírusos támadó hozzáférést szerez az egyik olyan szerverhez, amelyen a munkavállalókkal kapcsolatos személyes adatok is tárolásra kerülnek. Mivel ez esetben a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja szerinti szervezetnek minősül, az EIR-ben bekövetkezett, illetve a tudomásra jutott olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is –, amelyek a szervezet működésében vagy az általa végzett szolgáltatásnyújtásban súlyos zavart vagy vagyoni hátrányt okoz, illetve jelentős vagyoni vagy nem vagyoni kárt okoz más természetes vagy jogi személyek számára, köteles a vállalat bejelenteni a nemzeti kiberbiztonsági incidenskezelő központ részére[92], indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül.[93]

A személyes adat, mint kockázati tényező a NIS 2-ben

A NIS 2 nem adatvédelmi norma, de:

- rögzíti, hogy „tiszteletben tartja az alapvető jogokat, és figyelembe veszi különösen a Charta által elismert elveket, mindenekelőtt a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot, a személyes adatok védelméhez való jogot, a vállalkozás szabadságát, a tulajdonhoz való jogot, a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét, valamint a védelemhez való jogot”[94],
- előírja a megfelelő technikai és szervezési intézkedéseket, mint védelmi intézkedéseket,
- az adatvédelmi megfelelőségből ismert adatvédelmi és adatbiztonsági szabályzat, az adatvédelmi incidens kezelésére vonatkozó eljárás megléte, az adatvédelmi hatásvizsgálat megtörténte, a hozzáférés-kezelés, valamint a naplózás gyakorlata egyben az információbiztonsági megfelelés mércéje is.

A GDPR-alapú érettség éppen ezért jelentősen segíti a NIS 2-megfelelést. Ebben az esetben a párhuzamos megfelelés nem opcionális, hanem kötelező, amelynek biztosítása összehangolt szabályzatok, eljárásrendek és auditok alkalmazásával valósítható meg.

A NIS 2 és a GDPR ütközése

A NIS 2 és a GDPR nem mondanak ellent egymásnak, de

- más célt követnek (egyik az érintetti jogokat, a másik az információbiztonságot védi),
- más logikával közelítik meg ugyanazt az eseményt (pl.: adatvesztést vagy kiberbiztonsági incidenst),
- mást várnak el a szervezettől, mint követendő magatartásforma. Például míg a GDPR megköveteli az adattakarékosságot és célhoz kötöttséget az adatok gyűjtése során, addig a NIS 2 minél szélesebb körű elvárása a naplózás, monitorozás, loggyűjtés, ami könnyen nagy mennyiségű személyes adat technikai tárolásához, illetve céltól eltérő kezeléséhez vezethet.

92 2024. évi LXIX. törvény Magyarország kiberbiztonságáról 66.§ (2) bek.

93 418/2024. (XII. 23.) Kormány rendelet, 77. § (1) bekezdés

94 AZ EURÓPAI PARLAMENT ÉS a TANÁCS (EU) 2022/2555 IRÁNYELVE (143) preambulumbekezdés

Az ütközések feloldása a gyakorlatban az alábbi módokon keresztül valósítható meg:

- az információbiztonsági kockázatértékelések és az adatvédelmi hatásvizsgálat (GDPR) összehangolása
- a belső szabályzatok (naplózás, hozzáférés, adattovábbítás stb.) kialakítása oly módon, hogy azok nemcsak az MK rendelet kötelező védelmi intézkedésekkel kapcsolatos előírásait, hanem a GDPR alapelveit, illetve adott esetben a Munka törvénykönyvének[95] előírásait is figyelembe veszik
- az IBF és a DPO együttműködésének nemcsak előírása, hanem tényleges érvényesítése.

Védelmi intézkedés a gyakorlatban: munkavállalók ellenőrzése, illetve háttérellenőrzése

A NIS 2 szerinti biztonsági megfelelés a munkavállalók esetében gyakran igényel megbízhatósági, biztonsági, alkalmassági vizsgálatokat („háttérellenőrzés”), különösen jelentős vagy magas EIR-hez való hozzáférésük előtt. Azonban a GDPR, valamint az Mt. egyértelmű korlátokat állít a személyes adatok célhoz kötött, arányos és jogszerű kezelésére – különösen alkalmasságra, büntetett előéletre, magánéletre vonatkozó adatgyűjtés esetén (lásd pl.: erkölcsi bizonyítvány bekérésének korlátai).[96]

Példa: célhoz kötöttség elvének sérelme[97]
Egy beszerzési projekt során a beszerzés bejárást tart az üzemi területen, de a beszerzési munkatárs elfelejtette jelenléti íven dokumentálni a bejáráson résztvevőket. Ezért utólag úgy dönt, hogy lekéri a beléptetési rendszerből az aznapi mozgási adatokat, hogy igazolja, kik vettek részt ténylegesen a bejáráson.
Miért sérelmes?

- A beléptetési adatokat eredetileg biztonsági és beléptetési, valamint a területen a személyek mozgásának megfigyelése céljából gyűjtöttük,
- nem adminisztratív bizonyításhoz → célhoz kötöttség elve sérül
- Nincs jogalap a cél utólagos megváltoztatására (pl.: a beszerzés az adatkezelés jogalapját nem dokumentálta, pl.: hozzájárulás, szerződéses kötelezettség, jogos érdek)
- A munkavállalók és a látogatók nem számíthatnak arra, hogy beléptető rendszerben gyűjtött adatok más célra kerülnek felhasználásra (pl.: a beszerzés compliance megvalósításának alátámasztására)
- Helyes megoldás lehetett volna, ha a bejáráson résztvevők nevét helyben, jelenléti íven rögzíti a bejárás szervezője. Amennyiben ez elmaradt, a beléptetési adatokat csak akkor lehetett volna felhasználni, ha azt a belső szabályzat kifejezetten lehetővé teszi adminisztratív célból, a jogalap és az érintetti tájékoztatás dokumentálásával.

95 2012. évi LXXXVI. törvény a munka törvénykönyvéről (Mt.)

96 2012. évi LXXXVI. törvény a munka törvénykönyvéről (Mt.) 11. § (3)-(4) bekezdés

97 „a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon”. GDPR 5. cikk (1) bekezdés b) pont

Melyek a NIS 2 és a GDPR ütközési pontjai a háttérellenőrzés esetében?

Szempont	NIS 2 (hazai végrehajtás)	GDPR
Elvárás	az EIR-hez csak megbízható személy férjen hozzá[81]	Csak célhoz kötötten, jogalappal kezelhető személyes adat (pl.: erkölcsi bizonyítvány, múltbeli munkaviszony, pénzügyi helyzet stb.)
Cél	Rendszerbiztonság, humán kockázatok csökkentése	Magánélet védelme, emberi méltóság tisztelete
Kockázat	Elmaradt háttérellenőrzés → rendszerszintű sérülékenység	Túlzott háttérellenőrzés → jogszerűtlen adatkezelés, az érintettek jogainak és szabadságainak sérelme

81 7/2024 (VI.24) MK rendelet, 2. melléklet 14.3. védelmi intézkedés

Táblázat: NIS 2 és GDPR szempontok a munkavállalók háttérellenőrzésénél

Egy IT-biztonsági cég a NIS 2-re hivatkozva minden új IT szakembertől bekéri az erkölcsi bizonyítványát és az előző 3 munkahely referenciáját, ellenőrzi a közösségi média fiókjait, valamint egy külső céget megbíz titokban rögzített „megbízhatósági interjúval". Következmény: súlyos adatvédelmi sérelem, munkavállalói bizalomvesztés, esetleges NAIH-vizsgálat, személyiségjogi per

Hogyan érhetjük el a NIS 2 és a GDPR közötti összhangot?

A NIS 2–GDPR összhang négy alapelve:

1. Arányosság: a biztonsági kontroll adatvédelmi szempontból is indokolható, szükséges és arányos legyen, valamint megfeleljen a fokozatosság elvének is.
2. Átláthatóság: monitoringról, naplózásról, a gyűjtött információk az eredeti céltól eltérő célra használatáról megfelelő tájékoztatást kapjanak az érintettek, tekintettel a GDPR előírásaira
3. Dokumentáltság: a döntések és a mérlegelések igazolhatóak legyen, összhangban az elszámoltathatóság elvével
4. Integrált incidenskezelés: egy esemény, egy koordinált jogi reakció mindkét jogág előírásainak megfelelve.

A NIS 2 és a GDPR közötti összhang nem technikai, hanem irányítási kérdés, mely megköveteli a szervezettől, hogy

- a DPO és a CISO/IBF együttműködése ne csak opcionális/alkalomszerű legyen,
- legyen kialakítva megfelelő közös kockázatelemzési fórum,
- az adatvédelmi hatásvizsgálat (DPIA) és az információbiztonsággal kapcsolatos kockázatértékelés összehangolása megtörténjen (ezt a célt szolgálja az NKI törekvése az adatvédelmi kockázatelemzés beemelése a rendszerbiztonsági tervbe)

- az incidenskezelési folyamat integrált legyen.

Ha a két terület nincs összehangolva, a szervezet egyszerre két hatóság előtt állhat, amelyek eltérő jogi logikával, ugyanazon esemény miatt vizsgálódhatnak és büntethetnek.

A NIS 2 és a GDPR nem versengő szabályrendszerek, hanem a szervezet életében egymást korlátozó és kiegyensúlyozó normák, amelyeket követnie kell. Éppen ezért a szervezet érettségét nem az mutatja, hogy melyiknek felel meg jobban, hanem az, hogy képes-e a kettőt egyensúlyban tartani.

IBF és DPO közötti hatásköri összeütközés

A GDPR-NIS 2 kontextusban gyakorlati problémaként merülhet fel az a kérdés, hogy a DPO és IBF pozíciót betöltheti-e ugyanazon személy. E körben expressis verbis jogszabályi tilalom nincs, azonban több körülmény értékelése alapján levezethető, nem javasolt az, hogy ezt a két pozíciót ugyanaz a személy töltse be.

Az általános adatvédelmi rendelet 38. cikk (6) bekezdése mondja ki azt, hogy a DPO nem tölthet be olyan pozíciót, melyben az adatkezelés céljait és elveit meghatározná. E körben az összeférhetetlenség fogalmát a WP29 munkacsoport WP243 rev.01[98] számú iránymutatása részletezi: összeférhetetlenség esete akkor áll fenn, ha a DPO olyan pozícióban van, amely során az adatkezelés céljairól és eszközeiről dönt. Ilyen pozícióként a dokumentum példaként említi az ügyvezetőt, a HR-vezetőt, az IT-vezetőt vagy a marketing-vezetőt. Ezzel összefüggésben tehát azt kell mérlegelni a szervezeteknek, hogy adatkezelési célokat meghatározó döntési pozícióba kit jelöl ki.

Az IBF vonatkozásában Kiberbiztonsági tv. 11.§ (4) bekezdése kimondja, hogy az elektronikus információs rendszer biztonságáért felelős személyként – az (5) bekezdésben foglalt kivétellel – nem jelölhető ki vagy bízható meg a szervezet gazdasági vezetői feladatait ellátó személy vagy az a személy, aki a szervezeten belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el, illetve ilyen személy közvetlen alárendeltségébe tartozik. Ebből az következik, hogy az IBF az operatív biztonságért felelős, így az informatikai üzemeltetésben nem vehet részt.

Ha ugyanaz a személy tölti be a két szerepet, akkor előfordulhat, hogy ő alakítja ki a biztonsági kontrollokat (IBF), majd ezt követően ő ellenőrzi azok megfelelőségét adatvédelmi szempontból (DPO). Ez tipikus olyan ellenőrzési konfliktus, melyet célszerű elkerülni.

A magyar gyakorlat szerint több szervezetnél előfordul ez a megoldás, de az általánosan elfogadott álláspont az, hogy ez csak kisebb szervezeteknél fogadható el, de csak abban az esetben, ha a szerepek szétválasztása és a szervezeti függetlenség biztosított marad.

Az ISO 27001 alapján a szerepkörök szétválasztása ezen esetre is megoldást kínál, így a 27001 szerinti információbiztonsági irányítási rendszernél ezen szerepkörök elkülönülnek.

Információbiztonsági és adatvédelmi tudatosság növelés

Az európai hatóságok és az ENISA egyaránt hangsúlyozzák, hogy a NIS 2 és a GDPR követelményeinek összehangolása az egyik legnagyobb kihívás a szervezetek számára, különösen a személyes adatokat kezelő kritikus rendszerek

védelme során, és ez különösen igaz a tudatossággal kapcsolatos képzések esetében.

Mind a két jogszabályi környezet elvárja, hogy a szervezet/adatkezelő felkészítse mindazokat a személyeket, akik hozzáférnek a rendszerekhez, illetve a rendszereiben adatokat kezelnek. Éppen ezért célszerű ezen oktatásokkal kapcsolatos stratégiát egyeztetni, illetve a tartalmakat

98 https://ec.europa.eu/newsroom/article29/items/612048

összehangolni, különös tekintettel a vonatkozó kockázatelemzések megállapításaira, a megtörtént incidensekre, a jogszabályi és jogalkalmazási változásokra, valamint a szervezetünk információbiztonsági és adatvédelmi szakembereinek (CISO, IBF, DPO stb.) véleményére.

A két szabályozás közötti összhang nemcsak jogszabályi követelmény, hanem a szervezeti bizalom és a kockázatok minimalizálásának kulcsa is.

Kvantumfenyegetések a NIS 2 korában

A NIS 2 irányelv célja, hogy az Európai Unió tagállamait felkészítse a legmodernebb klasszikus kiberfenyegetésekre. Ugyanakkor alulértékeli a kvantumszámítógépek jelentette forradalmi kockázatokat, amelyek a következő évtizedben alapjaiban változtathatják meg a digitális biztonság környezetét. A jelenlegi szabályozási keretek – ideértve a titkosítási szabványokat, mint az RSA és ECC, valamint az incidensjelentési időkereteket – technológiailag elavultnak számítanak egy olyan korszakban, amikor a Shor-algoritmus percek alatt képes feltörni a nyilvános kulcsú titkosítást, a Grover-optimalizált brute-force támadások érvénytelenítik a jelenlegi jelszó- és session-kulcsokat, míg a kvantum–AI konvergencia, például RDSI deepfake támadások, lehetetlenné teszi a digitális tartalmak hitelesítését. Ahogy a DARPA Quantum Shield Program 2025-ben megállapította: „A NIS 2 hiányosságai nem technológiai korlátok, hanem stratégiai vakfoltok."

A kvantumtámadások kockázata már most kézzelfogható, és a NIS 2 szabályozásában számos rés mutatható ki. Példaként az SSH-Q (szub-szekundumos Secure Shell eltérítés) a valós idejű észlelés hiányát használja ki, lehetővé téve adminisztratív VPN-ek kompromittálását mindössze 15 másodperc alatt, nyom nélkül. A CAQI (tanúsítványkiadó kvantum megszemélyesítés) az elavult RSA/ECC követelmények miatt képes hamisított eIDAS tanúsítványokkal állami domainek átvételére. A QCC (kvantum lánc-összeomlás) pedig a blokklánc integritásvédelmének hiányát kihasználva akár 14,2 milliárd eurós veszteséget okozhat központi banki digitális valutákban 2030 előtt.

A szabályozás frissítése három kiemelt területet érint. Először is, a posztkvantum kriptográfia (PQC) kötelezővé tétele elengedhetetlen. Ennek részeként a NIS 2 mellékleteiben olyan algoritmusokat kellene előírni, mint a CRYSTALS-Dilithium vagy a Kyber-1024, követve az EU eIDAS 2.1 példáját, amely 2027-től betiltja az RSA-2048-at. Másodszor, be kell vezetni a kvantumérzékeny incidensjelentést, amely a jelenlegi 24/72 órás határidők helyett szub-másodperces anomáliadetektálást alkalmazna, például entropiaesés-mintázatok alapján. Harmadszor, a beszállítói lánc kvantumbiztosítása szükséges, amely a kulcsfontosságú Tier 1 beszállítókat PQC-támogatásra képes HSM-eszközök használatára kötelezné.

A nem megfelelő időben történő intézkedés rövid távon (2025–2027) már komoly gazdasági hatásokkal járna. Az ENISA becslése szerint 23,4 milliárd eurónyi veszteség lenne elkerülhető, amely magában foglalja a QCC támadásokból eredő digitális valuta lopásokat, a CAQI típusú tanúsítvány-hamisításokból származó hamis SWIFT tranzakciókat, valamint az RDSI deepfake csalások okozta, akár 920 millió eurós veszteségeket 2026-ban. Hosszabb távon (2028–2030) rendszerszintű összeomlás veszélye fenyeget, például kvantum-időmanipuláció (TQNI) miatti energiahálózati blackoutok, amelyek napi 49 milliárd eurós kárt okozhatnak, vagy biometrikus hamisítások (BQSA) révén több ezer illegális határátlépés történhet. Ezek mellett a jogi következmények is súlyosak lennének: a NIS 2 bírságok értelmüket veszítenék, mivel a támadók láthatatlanok maradnának. Ahogy az EU Cyber Council 2026-ban fogalmazott: „A kvantumtámadások nem hagynak nyomot – csak kárt."

Az ajánlott stratégiai lépések három időtávban határozhatók meg. Rövid távon (2024–2026) szükséges a teljes PQC migráció a kritikus infrastruktúrákban, valamint kvantum-Red Team gyakorlatok bevezetése az NIS 2 által érintett szervezetek számára. Középtávon (2027–2029) a kvantumbiztos tanúsítványok – például SPHINCS+ vagy FALCON-1024 – kötelezővé tétele, valamint a Five Eyes típusú együttműködések erősítése a kvantumtámadási benchmarkok megosztása érdekében lenne célszerű. Hosszú távon (2030-tól) pedig a kriptográfiai agilitás, vagyis a 24 órán belüli algoritmusváltás kötelezővé tétele, illetve kvantum-SIEM rendszerek bevezetése lenne szükséges, amelyek Grover-rezisztens anomáliadetektálást alkalmaznak.

A kvantumfenyegetések nem spekulációk: ma is létező képességek, amelyeket állami szereplők fejlesztenek. A NIS 2 frissítése ezért nem opció, hanem létkérdés. A késlekedés ára nemcsak pénzügyi veszteséget, hanem stratégiai önpusztítást is jelenthet a digitális ökoszisztémában.

17

Információ-biztonsági architektúra

A NIS 2 irányelv kockázatalapú biztonsági intézkedéseket ír elő, de nem határozza meg, hogy a szervezeteknek milyen információbiztonsági architektúrát vagy módszertant kell alkalmazniuk. A magyar végrehajtás sem követel meg konkrét architektúra keretrendszert, ugyanakkor az auditorok tapasztalatai azt mutatják, hogy a megfelelési hiányosságok jelentős része nem technológiai, hanem az információrendszerek átláthatatlanságából, a kontrollok elszigetelt alkalmazásából és a hiányos dokumentációból ered. A strukturált, architektúra alapú megközelítés ezért nem önmagáért fontos, hanem azért, mert támogatja a kockázatok kezelését, az auditálhatóságot és a biztonsági intézkedések hosszú távon is fenntartható működését.

17. Információbiztonsági architektúra a NIS2 megfelelési programban

Írta: Molnár Bálint, Dr. Váczi Dániel

17.1 Az információbiztonsági architektúra szerepe és fogalma

Az architektúra a rendszerek alapvető szervezeti felépítését jelenti, amely meghatározza az alkotóelemek közötti kapcsolatokat és azok működési elveit. A szervezeti informatikai architektúra olyan tervezési elvek összessége, amelyek az információk, információrendszerek és a technológiai infrastruktúra egymáshoz való viszonyát írják le.

Az architektúra elsődleges célja az információrendszerek közötti együttműködés biztosítása, a technológiai környezet egységesítése, valamint az üzleti célok és az informatikai működés összehangolása. Ennek révén a szervezet működése átláthatóbbá és strukturáltabbá válik.

Információbiztonsági szempontból az architektúra kiemelt jelentőségű, mivel meghatározza az információs vagyon struktúráját, kijelöli a biztonsági kontrollok helyét, és lehetővé teszi a kockázatok strukturált kezelését. Ennek megfelelően az információbiztonsági architektúra a szervezet információs rendszereinek és biztonsági intézkedéseinek egységes modellben történő leírását jelenti, amely átfogó képet ad a rendszerek működéséről, valamint a biztonsági kontrollok elhelyezkedéséről és összefüggéseiről.

Az architektúra több, egymással összefüggő rétegből áll, amelyek a szervezet működésének különböző aspektusait fedik le:

- Szervezeti architektúra: a szervezet céljai, működése és irányítása,
- Információ architektúra: az információk szerkezete és az információigények,
- Információrendszer architektúra: az információrendszerek struktúrája és kapcsolatai,
- Műszaki architektúra: az infrastruktúra, platformok és technológiák,
- Alkalmazási architektúra: az alkalmazások és szolgál tatások szerkezete.

Ezek a rétegek együtt biztosítják az információrendszerek integrált, biztonsági szempontból is értelmezhető megközelítését.

17.2 Architektúra keretrendszerek

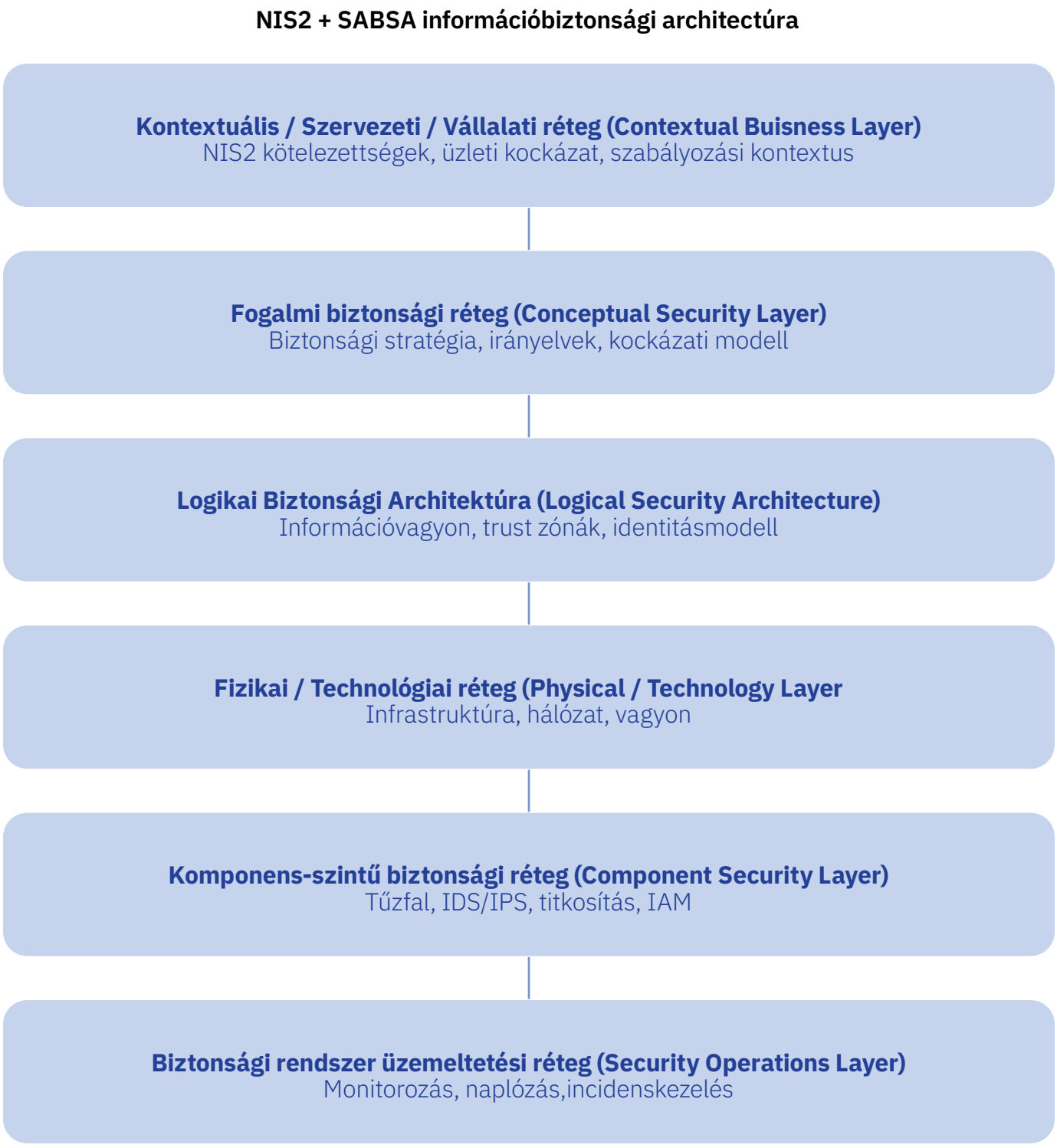
Az információbiztonsági architektúra kialakítására több, nemzetközileg elfogadott keretrendszer áll rendelkezésre, amelyek strukturált módszertant biztosítanak a tervezéshez és a dokumentáláshoz.

SABSA

A SABSA (Sherwood Applied Business Security Architecture) egy üzleti célokra épülő biztonsági architektúra keretrendszer, amely a szervezeti célokból kiindulva vezeti le a biztonsági kontrollokat. A megközelítés lényege, hogy a biztonsági intézkedések nem önálló technológiai döntésekként jelennek meg, hanem közvetlenül a szervezeti célokból, kockázatokból és működési követelményekből származnak.

A modell több egymásra épülő réteget különböztet meg:

- Kontextuális architektúra,
- Fogalmi architektúra,
- Logikai architektúra,
- Fizikai architektúra,
- Komponens architektúra,
- Szolgáltatásmenedzsment architektúra.



6. Ábra. NIS 2 információbiztonsági architektúra SABSA modell alapján.

Az alábbi ábra a SABSA modell NIS2 kontextusban történő értelmezését mutatja be:

A rétegek a szervezeti céloktól a biztonsági működésig mutatják be a kontrollok elhelyezkedését, ezáltal biztosítva a stratégiai és operatív szintek közötti kapcsolatot. Ez a felépítés jól illeszkedik a NIS2 követelményrendszeréhez, amely szintén kockázatalapú megközelítést alkalmaz, és elvárja, hogy a biztonsági intézkedések a szervezeti működéshez igazodjanak.

A SABSA modell egyik kulcseleme a MI–MIÉRT–HOGYAN–KI–HOL–MIKOR dimenzió, amely strukturált módon támogatja az architektúra leírását és a kontrollok indokoltságának visszavezethetőségét. Ez különösen fontos a NIS2 auditok során, ahol a kontrollok megléte mellett azok indokoltságát és megfelelőségét is igazolni szükséges.

SABSA réteg	Architektúra szint	NIS2 értelmezés
Kontextuális	Üzleti és szabályozási szint	szervezeti célok, szolgáltatási kötelezettségek, NIS2 megfelelés
Fogalmi	iztonsági stratégia	kockázati stratégia, biztonsági elvek
Logikai	Biztonsági modell	információvagyon, hozzáférési modellek
Fizikai	Technológiai architektúra	infrastruktúra és védelmi mechanizmusok
Komponens	Technológiai implementáció	konkrét biztonsági eszközök
Szolgáltatás	Biztonsági működés	monitorozás, incidenskezelés

Az alábbi táblázat szemlélteti a különböző architektúra rétegek és a megfelelési követelmények közötti kapcsolatot.

Zachman keretrendszer

A Zachman keretrendszer egy ontológiai modell, amely a szervezeti architektúra különböző nézőpontjait rendszerezi. A modell hat alapvető kérdés köré szerveződik: Mit? Hogyan? Hol? Ki? Mikor? Miért? Ezek a kérdések különböző szervezeti nézőpontokkal kombinálva strukturált architektúra-leírást eredményeznek.

A NIS 2 magyar implementációja, amely jelentős mértékben támaszkodik az NIST 800-53 Rev.5 kontrollrendszerére, megköveteli az információs rendszerek, adatáramlások és felelősségek egyértelmű azonosítását. A Zachman modell ebben hatékony támogatást nyújt, mivel strukturált keretet biztosít annak meghatározására, hogy milyen információk, folyamatok és szereplők vesznek részt az egyes rendszerek működésében.

Ez a megközelítés különösen hasznos lehet az auditokra való felkészülés során, mivel segíti az információk rendszerezését és az architektúra különböző nézőpontok szerinti bemutatását. Ez elősegíti a kontrollok megfelelőségének átláthatóbb és konzisztens értelmezését.

ISO/IEC 42010 architektúra szabvány

Az ISO/IEC 42010 szabvány az architektúra leírásának alapelveit határozza meg, és egységes keretet biztosít az architektúra dokumentáció kialakításához. A szabvány három kulcsfogalmat

vezet be: architektúra, architektúra nézet és nézőpont, amelyek lehetővé teszik a rendszer különböző érintettek szerinti értelmezését.

A NIS2 követelmények teljesítése során különösen fontos, hogy az architektúra dokumentáció különböző célcsoportok (például vezetők, üzemeltetők és auditorok) számára is értelmezhető legyen. Az ISO/IEC 42010 megközelítése ezt támogatja azzal, hogy elkülöníti az egyes nézőpontokat, és strukturált módon kezeli az architektúra leírását.

A szabvány alkalmazása hozzájárul a dokumentáció következetességéhez és auditálhatóságához, amely kulcsfontosságú a NIS 2 megfelelés során. Ez különösen a széles spektrumú kontrollkörnyezet esetében jelent előnyt, ahol a kontrollok különböző rendszerszinteken és érintetti nézőpontok mentén jelennek meg.

17.3 Az információbiztonsági kontrollok architektúrája

Az információbiztonsági architektúra egyik központi eleme a biztonsági kontrollok strukturált és tudatos elhelyezése. A kontrollok nem önálló, izolált intézkedések, hanem az architektúra különböző rétegeiben megjelenő, egymással összefüggő elemek, amelyek együttesen biztosítják a szervezet védelmét.

A kontrollok több formában jelennek meg, ideértve a szabályzatokat, eljárásrendeket, technológiai megoldásokat és szervezeti intézkedéseket. Ezek célja a szervezeti működés támogatása, a nem kívánt események megelőzése, az incidensek felismerése és kezelése, valamint a működés helyreállítása. A NIS 2 követelményrendszer elvárja, hogy ezek a kontrollok ne elszigetelten, hanem egymásra épülő, kockázatalapú rendszerként kerüljenek kialakításra.

A kontrollok alapvetően megelőző, észlelő és helyreállító kontrollokba sorolhatók. Ezek együttesen alkotják a szervezet védelmi képességét, amely a támadások megelőzésétől kezdve az események észlelésén át egészen a helyreállításig lefedi a teljes biztonsági életciklust. A hatékony architektúra biztosítja, hogy ezek a kontrolltípusok kiegyensúlyozott módon, egymást erősítve jelenjenek meg.

Az architektúra érettsége különböző szinteken értelmezhető, az ad hoc megoldásoktól az integrált, majd adaptív biztonsági architektúráig. A magasabb érettségi szintek jellemzője, hogy a biztonság nem különálló elemként, hanem a szervezet működésébe beépítve jelenik meg, és folyamatos visszacsatolással, monitorozással és kockázatalapú döntéshozatallal működik.

Az alábbi modell összefoglalja a biztonsági architektúra érettségi szintjeit:

Szint	Megnevezés	Jellemzők
1	Ad-hoc biztonság	elszigetelt technológiai megoldások
2	Dokumentált kontrollok	IBSZ és alap kontrollok
3	Strukturált architektúra	információrendszer-leltár és kockázati modell
4	Integrált biztonsági architektúra	biztonság az architektúrába építve
5	Adaptív biztonsági architektúra	folyamatos monitorozás és kockázatalapú működés

táblázat: NIS2 biztonsági architektúra érettségi modell

17.4 Az információbiztonsági architektúra technológiai elemei

Az információbiztonsági architektúra technológiai rétege a biztonsági kontrollok gyakorlati megvalósítását biztosító informatikai megoldások összessége. Ezek az eszközök az architektúra különböző szintjein jelennek meg, és együttesen támogatják a megelőzési, észlelési és reagálási képességeket.

A technológiai kontrollok az alábbi fő területek mentén értelmezhetők:

- Hálózatbiztonsági megoldások: tűzfalak (NGFW), mikro-szegmentáció, hálózati hozzáférés-szabályozás (NAC), VPN és IPsec alapú titkosított kommunikáció, DDoS védelem, hálózati forgalom analízis (NTA/NDR)
- Behatolásészlelés és fenyegetésdetektálás: IDS/IPS rendszerek, hálózati és host alapú szenzorok, anomália-alapú detektálás, threat intelligence integráció, sandboxing megoldások
- Végpont- és eszközvédelem: EDR/XDR megoldások, mobil eszközmenedzsment (MDM/MAM), eszközkonfiguráció és hardening, alkalmazásvezérlés (application whitelisting)
- Identitás- és hozzáférés-kezelés (IAM): központi identitáskezelés, többtényezős hitelesítés (MFA), szerepkör alapú (RBAC) és attribútum alapú (ABAC) jogosultságkezelés, privilegizált hozzáférések kezelése (PAM), single sign-on (SSO)
- Naplózás, monitorozás és incidenskezelés: központi naplógyűjtés, SIEM rendszerek, SOAR megoldások, biztonsági események korrelációja, automatizált riasztáskezelés, Security Operations Center (SOC) képességek
- Sebezhetőség- és konfigurációkezelés: sérülékenységvizsgálati eszközök, folyamatos sebezhetőség menedzsment, patch management, konfigurációs megfelelőség ellenőrzése (CIS baseline-ok)
- Adatvédelem és adatbiztonság: titkosítás (at rest / in transit), kulcsmenedzsment (KMS/HSM), adatvesztés-megelőzés (DLP), adatmaszkolás, mentési és helyreállítási megoldások (backup, disaster recovery)
- Felhő- és virtualizációs biztonság: CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), konténerbiztonság (Kubernetes security), infrastruktúra mint kód (IaC) biztonsági ellenőrzése
- Alkalmazásbiztonság és fejlesztési biztonság: SAST/DAST eszközök, DevSecOps folyamatok, kódelemzés, dependency scanning, API biztonság
- OT és ipari rendszerek biztonsága (ahol releváns): ipari protokollok monitorozása, hálózati szegmentáció IT/OT között, passzív forgalomelemzés, biztonságos távoli hozzáférés, speciális ICS/SCADA védelmi megoldások

Ezek az elemek elsősorban az architektúra fizikai és komponens szintjén jelennek meg, és kulcsszerepet játszanak a NIS 2 által előírt technológiai kontrollok megvalósításában. Fontos azonban hangsúlyozni, hogy ezek a megoldások önmagukban nem biztosítanak teljes körű védelmet. Hatékonyságuk akkor érvényesül, ha egymással integrált módon, az architektúra részeként, megfelelő szervezeti szabályozással és működési folyamatokkal együtt kerülnek kialakításra.

17.5 Információbiztonsági architektúra a NIS2 megfelelésben

A NIS 2 irányelv kockázatalapú biztonsági intézkedések bevezetését írja elő, amelyek többek között a kockázatkezelés, incidenskezelés, üzletmenet-folytonosság, ellátási lánc biztonsága, valamint a monitorozás és naplózás területeit érintik. Az architektúra alapú megközelítés biztosítja, hogy ezek az intézkedések a szervezet információs rendszereinek különböző szintjein következetesen és egymással összhangban jelenjenek meg.

Az audit tapasztalatok alapján az egyik nagy kihívás az információrendszerek átláthatóságának hiánya. Az architektúra szemlélet támogatja az információrendszerek azonosítását, a függőségek feltárását, a kritikus rendszerek meghatározását, valamint a biztonsági kontrollok megfelelő elhelyezését. A jól definiált architektúra különösen fontos az incidenskezelés, a kockázatelemzés, az auditok lebonyolítása, valamint az információbiztonsági program irányítása során.

Az információbiztonsági architektúra kialakításának lépései a NIS 2 megfelelésben

A NIS 2 követelményeinek való megfelelés nem csupán technológiai intézkedések bevezetését jelenti, hanem egy átfogó információbiztonsági architektúra kialakítását. Az architektúra célja, hogy strukturált módon írja le a szervezet információvagyonát, információrendszereit és az azokat támogató technológiai környezetet, valamint ezek biztonsági védelmét. A gyakorlati tapasztalatok alapján az információbiztonsági architektúra kialakítása egy többlépcsős folyamat, amely az alábbi fő lépésekből áll:

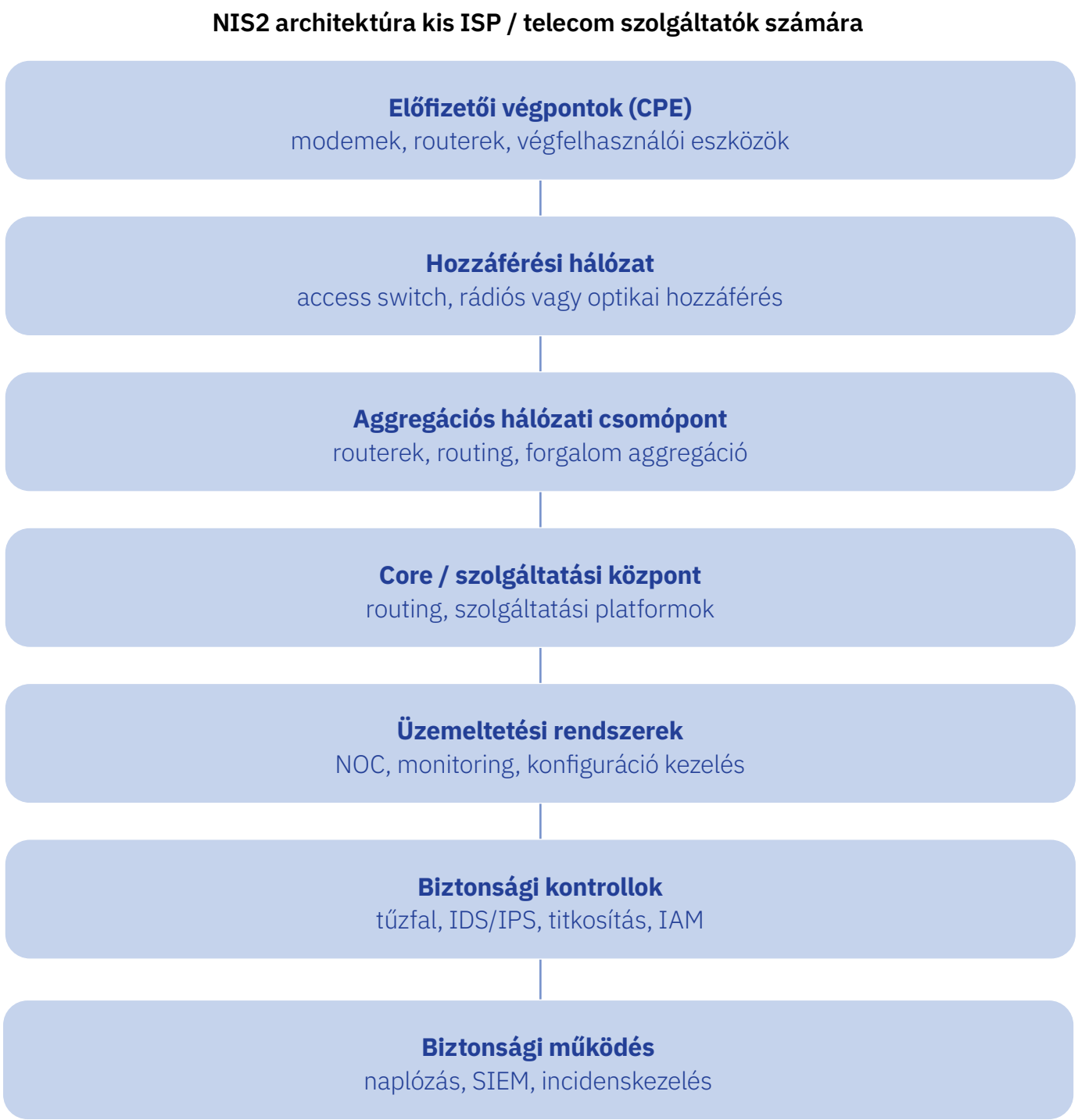
1. A szervezeti környezet és a kulcsfontosságú szolgáltatások azonosítása: Az architektúra kialakításának első lépése a szervezet működésének megértése. Ebben a lépésben az alábbi kérdések kerülnek meghatározásra: milyen szolgáltatásokat nyújt a szervezet, melyek a kritikus üzleti folyamatok, milyen jogszabályi és szabályozási kötelezettségek vonatkoznak a működésre, mely szervezeti egységek és szerepkörök vesznek részt az információfeldolgozásban. Ez a szint a szervezeti vagy üzleti architektúra szintjének felel meg.
2. Az információvagyon és az információáramlások feltérképezése: A következő lépés az információ architektúra kialakítása. Ennek során a szervezet azonosítja az információs vagyont, meghatározza az adatkategóriákat, feltérképezi az információáramlásokat, azonosítja az adatok feldolgozásában részt vevő rendszereket. Ez a lépés biztosítja a kockázatelemzés és a biztonsági intézkedések alapját.

3. Az információs rendszerek és alkalmazások azonosítása: Ebben a lépésben a szervezet azonosítja azokat az információs rendszereket, amelyek az információk feldolgozásában részt vesznek. Ide tartoznak például az üzleti alkalmazások, adatbázis rendszerek, integrációs rendszerek, szolgáltatási platformok. Ez az információrendszer architektúra szintje, amely az információ és a technológia közötti kapcsolatot írja le.
4. A technológiai infrastruktúra feltérképezése: A műszaki architektúra szintjén kerül sor az informatikai infrastruktúra elemeinek azonosítására. Ez a hálózati infrastruktúrát, szervereket és platformokat, operációs rendszereket, virtualizációs és felhő környezeteket és a kommunikációs protokollokat foglalja magába. Ez a lépés segíti az infrastruktúra szintű kockázatok feltárását.
5. Biztonsági kontrollok elhelyezése az architektúrában: A biztonsági architektúra kialakításának kulcsfontosságú eleme a kontrollok megfelelő elhelyezése. A kontrollok különböző szinteken jelennek meg úgy mint szervezeti szinten (szabályzatok, irányelvek), folyamat szinten (eljárásrendek) és technológiai szinten (biztonsági eszközök). A kontrollok célja a kockázatok csökkentése, az incidensek megelőzése, az események észlelése, a működés helyreállítása.
6. Monitorozás és folyamatos fejlesztés: Az információbiztonsági architektúra nem statikus modell. A NIS 2 követelményeinek megfelelően a szervezeteknek folyamatosan figyelniük kell a biztonsági eseményeket, a működési kockázatokat, a technológiai változásokat, a szabályozási környezet alakulását. Ennek érdekében a szervezetek biztonsági monitorozási és incidenskezelési folyamatokat alakítanak ki.

17.6. Esettanulmány – mikro és KKV szolgáltatók architektúrája

A mikro- és kisvállalkozások esetében az információbiztonsági architektúra jellemzően egyszerűbb felépítésű, ugyanakkor alapvető strukturáltság nélkül ezek a környezetek is nehezen áttekinthetővé és védhetővé válnak. A NIS 2 megfelelés szempontjából ezért különösen fontos, hogy még korlátozott erőforrások mellett is kialakításra kerüljön egy jól értelmezhető, rétegzett architektúra-modell.

Az első ábra egy tipikus kis- és közepes szolgáltató referencia-architektúráját szemlélteti, amely a szolgáltatási infrastruktúrát, az üzemeltetési rendszereket, valamint a biztonsági kontrollokat egységes rendszerként mutatja be. Az architektúra logikai felépítése az előfizetői végpontoktól indul, és a szolgáltatási központi rendszerekig, majd az üzemeltetési és biztonsági funkciókig terjed.



7. Ábra. Referencia architektúra kis és közepes szolgáltatók NIS 2 biztonsági modelljéhez

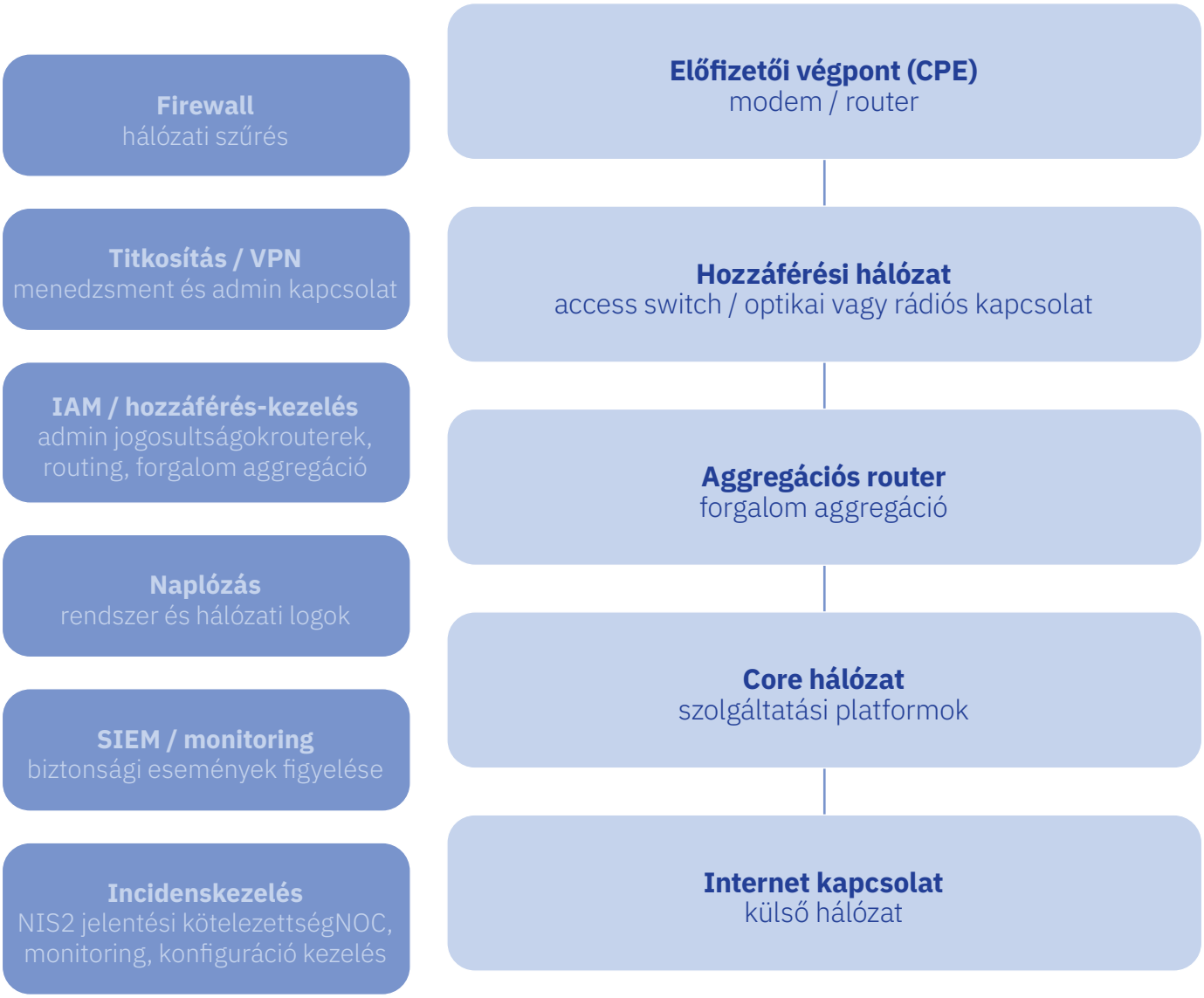
A modell alsó rétegét az előfizetői végpontok (CPE-k), valamint a hozzáférési hálózat alkotja, amely magában foglalja a hozzáférési eszközöket, vezetékes és vezeték nélküli kapcsolati technológiákat. Ezt követik az aggregációs hálózati csomópontok, ahol a forgalom koncentrálása és irányítása történik, majd a core vagy szolgáltatási központ, amely a routing funkciókat és az üzleti szolgáltatásokat biztosító platformokat tartalmazza.

Az infrastruktúra felett helyezkednek el az üzemeltetési rendszerek – például a hálózatfelügyeleti (NOC), monitoring és konfigurációkezelő rendszerek –, amelyek a működés fenntartásához és felügyeletéhez szükségesek. Ezekhez szorosan kapcsolódnak a biztonsági kontrollok, mint a tűzfalak, behatolás észlelő rendszerek, titkosítási megoldások és hozzáférés-kezelési mechanizmusok.

A modell legfelső szintjén a biztonsági működés jelenik meg, amely magában foglalja a naplózást, a biztonsági események monitorozását (SIEM), valamint az incidenskezelési folyamatokat. Ez a réteg biztosítja a folyamatos felügyeletet és a reagálási képességet.

Az architektúra egyik fontos jellemzője, hogy nem csupán komponensek halmaza, hanem olyan rendszer, amelyben az adatáramlások és a biztonsági kontrollok egymással összefüggésben értelmezhetők.

A következő ábra ezt a működést egy konkrétabb nézőpontból mutatja be, a hálózati adatút és a hozzá kapcsolódó biztonsági kontrollpontok mentén. A szolgáltató tipikus adatútja az előfizetői végponttól indul, a hozzáférési hálózaton és az aggregációs rétegen keresztül a core hálózatig, majd az internetkapcsolatig vezet. Ez a lánc jól definiálható, és minden pontján azonosíthatók azok a helyek, ahol biztonsági kontrollok alkalmazása szükséges.



8. Ábra: NIS 2 biztonsági kontrollpontok egy kis internet- és távközlési szolgáltató hálózati architektúrájában

A NIS 2 követelmények szempontjából ezek a kontrollpontok különösen fontosak. Ilyen például a hálózati határokon elhelyezett tűzfalak alkalmazása, a kommunikáció titkosítása VPN vagy egyéb kriptográfiai megoldások segítségével, a hozzáférések szabályozása identitás- és jogosultságkezelési rendszerekkel, valamint a naplózás és a biztonsági események folyamatos monitorozása.

Az incidenskezelés szintén kulcselemként jelenik meg, amely összekapcsolja a technológiai kontrollokat a szervezeti folyamatokkal. A jól kialakított architektúra lehetővé teszi, hogy egy biztonsági esemény észlelése, elemzése és kezelése gyorsan és strukturált módon történjen.

Ez az esettanulmány rávilágít arra, hogy még viszonylag egyszerű infrastruktúra esetén is elengedhetetlen az architektúra alapú megközelítés. A rétegzett felépítés és a kontrollpontok tudatos kijelölése biztosítja, hogy a biztonsági intézkedések ne elszigetelten, hanem egymással összhangban működjenek, támogatva ezzel a NIS2 követelmények teljesítését.

17.7 NIS2 audit tapasztalatok

A NIS2 auditok során visszatérően hasonló típusú hiányosságok kerülnek azonosításra, amelyek jelentős része nem technológiai, hanem architekturális és szervezeti jellegű. A tapasztalatok azt mutatják, hogy a megfelelési problémák gyakran nem egy-egy konkrét kontroll hiányából fakadnak, hanem abból, hogy a szervezetek nem rendelkeznek átlátható és strukturált információbiztonsági architektúrával.

A gyakran azonosított hiányosságok közé tartoznak az információrendszer-leltár hiánya, a dokumentálatlan adatáramlások, a naplózás és monitorozás hiányosságai és a szervezeti felelősségek tisztázatlansága. Ezek a problémák közvetlenül befolyásolják a kockázatelemzés minőségét, a biztonsági kontrollok hatékonyságát, valamint az incidenskezelési képességeket.

A NIS 2 bevezetésével a kritikus és fontos szolgáltatásokat nyújtó szervezetek számára jelentősen szigorodtak a kiberbiztonsági követelmények. A mikro- és kisvállalkozások ugyanakkor méretükből és erőforrásaik korlátozottságából adódóan eltérő kihívásokkal szembesülnek, mint a nagyobb szervezetek, ami különösen az architektúra és a szervezeti működés területén jelentkezik.

Az auditok és felkészítési projektek tapasztalatai alapján megállapítható, hogy a megfelelési hiányosságok jelentős része megfelelő architekturális szemlélettel és strukturált megközelítéssel kezelhető lenne. Az architektúra dokumentáció megléte önmagában is jelentősen megkönnyíti a megfelelési ellenőrzések lebonyolítását, mivel átláthatóvá teszi az információrendszerek működését, az adatáramlásokat és a biztonsági kontrollok elhelyezkedését.

Az alábbiakban összefoglaljuk a leggyakrabban tapasztalt problémákat és a bevált megoldási megközelítéseket.

Az információrendszerek átláthatóságának hiánya

Az auditok egyik gyakori megállapítása, hogy a szervezetek nem rendelkeznek teljes körű áttekintéssel az általuk üzemeltetett információs rendszerekről. Ez különösen igaz kis szolgáltatók esetében, ahol a rendszerek gyakran fokozatosan, több év alatt alakultak ki. Tipikus problémák a hiányos rendszerleltár, a dokumentálatlan integrációk, nem azonosított adatáramlások és az információs vagyon nyilvántartás hiánya. Ez megnehezíti a kockázatelemzés és a biztonsági intézkedések megfelelő tervezését. Az architektúra alapú megközelítés segíthet az információrendszerek strukturált feltérképezésében.

A biztonsági kontrollok elszigetelt alkalmazása

Sok szervezetben a biztonsági intézkedések különálló technológiai megoldások formájában jelennek meg (például: tűzfal telepítése, vírusvédelem alkalmazása, naplózás bevezetése). Ezek azonban gyakran nem alkotnak integrált biztonsági rendszert. Az auditok során gyakran kiderül, hogy a naplókat nem ellenőrzik rendszeresen, a riasztások feldolgozása nem definiált, vagy az incidenskezelési folyamat nem működik a gyakorlatban. A tapasztalatok szerint a kontrollok hatékonysága jelentősen javul, ha azok az információbiztonsági architektúra részét képezik.

Monitorozás és eseménykezelés hiányosságai

A NIS 2 egyik alapvető követelménye a biztonsági események folyamatos monitorozása és kezelése. A gyakorlatban azonban a következő problémák gyakran előfordulnak:

- A biztonsági naplózás nincs megfelelően konfigurálva,
- A naplóadatok elemzése nem történik meg,
- Az incidensek kezelésére nincs dokumentált eljárás,
- A monitoring rendszerek nem fedik le a teljes infrastruktúrát.

Ez különösen problémás lehet hálózati szolgáltatók esetében, ahol a szolgáltatás folytonossága kulcsfontosságú.

NIS2 Capability Map – kis ISP / telecom szolgáltatók

Governance IBSZ, felelősségek, megfelelőség	**Risk Management** kockázatelemzés, kockázatkezelés
Asset Management EIR leltár, információvagyon	**Security Architecture** architektúra modell, trust zónák
Network Security tűzfal, szegmentáció	**Identity & Access Management** felhasználók, admin hozzáférések
Logging & Monitoring naplózás, SIEM, eseményfigyelés	**Incident Response** incidenskezelés, jelentés
Business Continuity mentések, helyreállítás	**Audit & Improvement** ellenőrzés, fejlesztés

Az architektúra dokumentáció hiánya

Az auditok során az egyik legfontosabb hiányosság az információbiztonsági architektúra dokumentációjának hiánya. Sok szervezet rendelkezik szabályzatokkal, eljárásrendekkel és technológiai megoldásokkal, de hiányzik az a dokumentáció, amely bemutatja az információs rendszerek kapcsolatát, az adatáramlásokat és a biztonsági kontrollok elhelyezkedését. Ez megnehezíti az információbiztonsági program átlátható működtetését.

Bevált gyakorlatok

A felkészítési projektek során több olyan megközelítés is azonosítható volt, amely jelentősen megkönnyítette a NIS 2 megfelelést.

- Architektúra alapú megközelítés: A szervezetek először feltérképezik az információs rendszerek architektúráját.
- Kockázatalapú biztonsági modell: A biztonsági intézkedések a kockázatelemzés eredményeire épülnek.
- Egyszerű, de működő folyamatok: A kis szervezetek számára a túlzottan komplex biztonsági rendszerek nem fenntarthatók.

A NIS 2 audit tapasztalatai azt mutatják, hogy a sikeres megfelelés kulcsa nem kizárólag a technológiai megoldásokban rejlik. A legfontosabb tényezők a szervezet információs architektúrájának megértése, a biztonsági kontrollok strukturált elhelyezése, a felelősségek egyértelmű meghatározása és a a működő monitorozási és incidenskezelési folyamatok.

Az architektúra alapú megközelítés különösen fontos a mikro- és kisvállalkozások számára, mert lehetővé teszi a rendelkezésre álló erőforrások hatékony felhasználását.

17.8 Ajánlások mikro és KKV szervezetek számára

A NIS 2 magyar implementációja által előírt követelményeinek teljesítése különösen nagy kihívást jelent a mikro- és kisvállalkozások számára, amelyek gyakran korlátozott technológiai és humán erőforrásokkal rendelkeznek. A felkészítési projektek és auditok tapasztalatai alapján az alábbi tíz ajánlás segítheti a szervezeteket abban, hogy hatékony és fenntartható információbiztonsági architektúrát alakítsanak ki.

Az információbiztonságot architekturális kérdésként kell kezelni

Az információbiztonság nem csupán technológiai eszközök alkalmazását jelenti, hanem a szervezet működésének strukturált részét képezi. A biztonsági intézkedéseknek a szervezet információs architektúrájába kell illeszkedniük, mivel csak így biztosítható az információrendszerek átláthatósága, a kontrollok megfelelő elhelyezése és a kockázatok következetes, rendszerszintű kezelése. Az egyik legfontosabb lépés az összes információrendszer azonosítása. Ez magában foglalja az alkalmazások, adatbázisok, hálózati infrastruktúra és felhőszolgáltatások. A rendszerleltár a kockázatelemzés és a biztonsági architektúra alapja.

Az információs vagyon azonosítása

A szervezeteknek egyértelműen meg kell határozniuk, hogy mely információk kritikusak a működésük szempontjából. Ide tartozhatnak például az előfizetői adatok, hálózati konfigurációk, szolgáltatási adatok vagy működési naplók. Az információs vagyon pontos azonosítása nélkül a kockázatok nem értelmezhetők és nem kezelhetők megfelelően.

Az információáramlások feltérképezése

A biztonságos működés alapja annak megértése, hogy az adatok hogyan mozognak a rendszerek között. Az információáramlások dokumentálása lehetővé teszi a kritikus adatkapcsolatok, integrációs pontok és potenciális biztonsági kockázatok azonosítását. Az adatáramlási modellek az architektúra dokumentáció kulcsfontosságú elemei.

A biztonsági kontrollok architekturális elhelyezése

A biztonsági intézkedéseknek az architektúra különböző szintjein kell megjelenniük. A hálózati szinten alkalmazott védelmi megoldások, a rendszer szintű hozzáférés-kezelés, az alkalmazási szintű hitelesítés és naplózás, valamint a szervezeti szintű irányelvek és eljárásrendek együttesen biztosítják a védelem hatékonyságát.

Monitorozási és naplózási rendszer kialakítása

A biztonsági események folyamatos monitorozása a NIS2 egyik alapvető követelménye. Ennek része a naplózási mechanizmusok kialakítása, a hálózati és rendszeresemények figyelése, a riasztások kezelése, valamint az incidensek elemzése. A megfelelő monitorozási képesség nélkül a szervezet nem képes időben reagálni a biztonsági eseményekre.

Hozzáférés-kezelés és jogosultságok kontrollja

A hozzáférések szabályozása kulcsszerepet játszik az információbiztonságban, különösen az adminisztrátori jogosultságok esetében. A szervezeteknek biztosítaniuk kell az egyedi felhasználói azonosítást, a szerepkör alapú jogosultságkezelést, valamint a kritikus tevékenységek naplózását és ellenőrizhetőségét.

A biztonsági architektúra dokumentálása

A jól strukturált architektúra dokumentáció alapvető feltétele a működés átláthatóságának. Az architektúra ábrák, adatáramlási modellek és kontrolltérképek nemcsak a belső működést teszik követhetővé, hanem az auditokra való felkészülést és a változások kezelését is jelentősen támogatják.

Folyamatos felülvizsgálat és fejlesztés

Az információbiztonsági architektúra nem statikus, hanem folyamatosan fejlődő rendszer. A szervezeteknek rendszeresen felül kell vizsgálniuk a kockázatokat, a technológiai környezet változásait és a kontrollok hatékonyságát annak érdekében, hogy a biztonsági intézkedések lépést tartsanak a változó fenyegetési környezettel.

A NIS 2 megfelelés nem kizárólag a szabályozási követelmények teljesítéséről szól. A szabályozás célja, hogy a szervezetek olyan információbiztonsági architektúrát alakítsanak ki, amely hosszú távon biztosítja az információs rendszerek megbízható és biztonságos működését. Az architektúra alapú megközelítés különösen fontos a kis- és közepes szervezetek számára, mert lehetővé teszi a korlátozott erőforrások hatékony felhasználását és a biztonsági intézkedések fenntartható működtetését.[99,100]

---

99 Molnár Bálint: Információbiztonsági program Információbiztonsági architektúrák információs rendszerekben,May 2014,Publisher: Nemzeti Közszolgálati egyetem, https://www.researchgate.net/publication/317606511_Informaciobiztonsagi_program_Informaciobiztonsagi_architekturak_informacios_rendszerekben

100 **Molnár Bálint, Kő Andrea: Információrendszerek auditálása Az informatika és az információrendszerek ellenőrzési és irányítási módszerei Corvinno Technology Transfer Kft., 2009,** https://www.researchgate.net/publication/401734621_Informaciorendszerek_auditalasa_Az_informatika_es_az_informaciorendszerek_ellenorzesi_es_iranyitasi_modszerei_Corvinno_Technology_Transfer_Kft

18

Kommunikáció a menedzsmenttel

A NIS 2 irányelv és a hazai végrehajtó hazai szabályozás számos olyan kötelezettséggel jár, amelyek nem csupán technikai vagy jogi kérdések, hanem erőforrásigényes stratégiai feladatok. a NIS 2 azonban nemcsak IT-feladatok halmaza, hanem üzletfolytonossági és jogi kockázatok kezelése is. Éppen ezért a vezetőség támogatása kulcsfontosságú olyan területeken, mint a költségvetés biztosítása, a szervezeti változások jóváhagyása, valamint a döntések meghozatala nemcsak a jogszabályok által megkövetelt esetekben, hanem egyéb érzékeny kérdésekben is (pl.: háttérellenőrzés, monitoring).

18. Kommunikáció a menedzsmenttel

Írták: dr. Albert Ágota, Kovács György Attila

18.1. Hogyan és mit mondjunk a vezetőségnek?

Minden sikeres projekt bevezetésének alapja a rendszeres, korrekt, nyílt kommunikáció a menedzsmenttel, melynek célja nemcsak a tájékoztatás, hanem azoknak a döntéseknek az előkészítése, amelyek az anyagi, személyi és szervezeti erőforrásokat biztosítják. a szervezetünkre váró feladatokat egyszerűen kell megfogalmaznunk, mert nem biztos, hogy a döntéshozó személy informatikai vénával rendelkezik. Az ENISA ajánlása szerint tudatosítani kell a vezetőséggel, hogy *„felelősek a kiberbiztonsági intézkedések jóváhagyásáért*[101]*, és el kell végezniük a kiberbiztonsági képzést”* [102].

De hogyan és mit mondjunk a vezetőségnek? Az a tájékoztatás, miszerint *„a NIS 2 hatálya alá tartozó szervezetként megfelelő és arányos műszaki, üzemeltetési és szervezeti intézkedéseket kell hoznunk azon hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, amelyeket működésünkhöz vagy szolgáltatásaink nyújtásához használunk, valamint annak érdekében, hogy az incidenseknek a szolgáltatásainkat igénybe vevőkre és más szolgáltatásokra gyakorolt hatást megelőzzük vagy minimalizáljuk”,* nem biztos, hogy nyitott fülekre talál, illetve a „mondd meg az igazat[103] és fuss” taktikát sem biztos, hogy érdemes direktben alkalmaznunk.

Gondolkodjunk „üzletben” és „kockázatban”. a vezetőség nem technikai részleteket akar hallani (pl.: tűzfal-konfiguráció), hanem azt, hogy milyen kockázat fenyegeti az üzleti működést, mi történhet, ha NIS 2 követelményeknek nem felel meg a cég, valamint egy esetleges incidens mekkora pénzügyi és reputációs kárt okozhat. Ne csak a hátrányokat (mennyibe kerül), hanem az eredményt is mutassuk be, például „a NIS 2 megfelelés azt szolgálja, hogy a szervezetünk ellenálló legyen a kibertámadásokkal szemben, és akkor is tovább tudjunk működni, ha megtámadnak minket”. a kommunikációban segítséget nyújthat, ha a következő három kérdés mentén gondolkodunk:

- Mi a probléma?
- Milyen következménye lehet?
- Hogyan csökkenthetjük a kárt?

A prioritásokat mutassuk be, és lehetőleg ne öntsünk mindet egyszerre a vezetőségre. Érdemes például időben rangsorolni, például mi az, ami rövid távon megoldandó/kötelező (pl.: jogszabályi határidők, az audit mikorra várható, mely szabályzatokat kell elkészítenünk stb.), mivel szükséges középtávon foglalkozni (pl.: fejlesztések, amivel költséget spórolhatunk meg vagy megkönnyíthetjük a későbbi auditoknak megfelelést), illetve mi illeszthető be a hosszú távú stratégiánkba (pl.: kiberbiztonsággal

101 lásd pl.: 2024. évi LXIX. törvény Magyarország kiberbiztonságáról. 6.§, 8.§, 10.§ (2) bekezdés

102 ENISA: MAPPING NIS 2 OBLIGATIONS TO ECSF June 2025, doi: 10.2824/8870995.

103 pl.: Kiberbiztonsági tv. 30. § (3) bekezdés alapján ha „a szervezet vezetője a jogszabályban előírt kötelezettségének nem tesz eleget, a nemzeti kiberbiztonsági hatóság az eset összes körülményének mérlegelésével kormányrendeletben meghatározott mértékű bírsággal sújthatja, ismételt jogsértés esetén sújtani köteles” , illetve adott esetben a (6) bekezdés b) pontja alapján „kezdeményezheti a cégbíróságnál az alapvető szervezet vezetőjének az adott szervezetben betöltött vezető tisztségviselői feladatainak ellátásától való ideiglenes eltiltását”.

kapcsolatos tudatossági kultúra kiépítése és folyamatos karbantartása).

Kommunikáljunk egyszerűen és adjunk számokat is, például mekkora az audit várható közvetlen költsége, egy napi termeléskiesés milyen költséggel jár, milyen versenyképességi hátrányt okozhat a gyakorlatban nem megfelelés (pl.: egy zsarolóvírusos támadás mivel járhat), adott esetben mennyi lehet a bírság.

A szervezet vezetője a tájékoztatónk alapján dönt a következő lépésekről és a szükséges erőforrások bevonásáról, éppen ezért fontos, hogy a felmerülő problémákról objektíven tájékoztassuk. Nagy valószínűséggel a vállalat vezetője tőlünk, mint az adott téma felelősétől várja el a megoldást is, ezért kínáljunk fel több alternatívát, ami számára választási lehetőséget biztosít. Ez nemcsak a probléma átbeszélésre és mérlegelésre készteti a vezetőt, hanem a döntés érzését is biztosítja, valamint segít a felelősséget tudatosítani. Éppen ezért már a NIS 2 projekt bevezetésének elején tisztáznunk kell, hogy ez egy idő- és erőforrás igényes feladat.

18.2. Riportolási lehetőségek

A projektvezetőnek a cég szervezeti kultúrájának megfelelő (heti, kétheti, maximum havi) gyakorisággal kell a felső vezetést röviden informálnunk a felkészülés helyzetéről, valamint azokról a felmerülő új problémákról, amelyekben a felső vezetés segítségére van szükségünk, mint például a kiemelt kockázatok kezelése, a közelgő határidőkből adódó feladatok, valamint a már elvégzett és a tervezett intézkedések.

Az is előfordulhat, hogy incidens esetén kell gyors jelentést adnunk a vezetőségnek. Ebben célszerű röviden, tömören megfogalmaznunk azt, hogy mi történt, az milyen hatással lehet az üzletmenetre, illetve a szervezetünk reputációjára, mi a javasolt azonnali intézkedés, mikorra várható helyreállás, valamint milyen jelentési kötelezettségeink vannak a kiberbiztonsági és adatvédelmi incidens protokolljaink alapján.

Be kell számolnunk a NIS 2 audittal kapcsolatban is. Előtte érdemes kiemelnünk a várható kötelezettségeket és a hiányosságainkat, utána pedig beszámolnunk az audit megállapításairól, valamint a javasolt intézkedésekről.

18.3. Legfontosabb költségtételek

A költségvetés tervezésénél két tételt, az éves kiberbiztonsági felügyeleti díjat, valamint a kiberbiztonsági audit legmagasabb díját jogszabályok határozzák meg[104].

A NIS 2 bevezetés költsége függ a szervezet méretétől, a bevezetésben részt vevő munkatársak számától, az esetleges külső tanácsadó(k) díjazásától, valamint a GAP analízis során felfedezett hiányosságok megszüntetéséhez szükséges új informatikai eszközök költségétől is, ezért a költséget minden szervezet esetében egyedileg lehet meghatározni.

18.4. Nem választás, hanem kötelesség – A vezetőség feladatai és a várható kihívások

A vezetőség felé egyértelműen kell azt az alapgondolatot kommunikálni, hogy a NIS 2 megfelelés az érintett szervezet számára kötelező: olyan, mint a hatályos adójogszabályoknak vagy munkavédelmi előírásoknak megfelelés. Nem lehet kibújni alóla.

104 Az éves felügyeleti díjat lásd a 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díjról. Az audit díját az SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról 3. melléklete alapján lehet kiszámolni.

A szervezetre váró feladatokat két jogszabályban[105] megfogalmazott követelmények részletes GAP elemzését követően tudjuk meghatározni.

A GAP analízis eredménye többek között új szabályzatok kiadása, a meglévő szabályzataink, valamint folyamataink (eljárásrendjeink) módosítása, valamint új informatikai hardver és szoftver eszközök vásárlását is jelentheti. Ez az eredmény nagymértékben függ a szervezet információbiztonsági felkészültségétől.

Milyen ellenvetésekre számíthatunk?

- „Ez nálunk úgysem történik meg" – cáfoljunk konkrét példákkal.
- „A szervezetnek nincs rá pénze" – mutassuk be a lehetséges bírságok vagy károk nagyságrendjét, például a közelmúlt zsarolóvírusos támadásainak költségét, illetve a támadások miatti bírságok összegét.
- „Akkor inkább ne dokumentáljunk semmit" – világítsunk rá, hogy mind az auditor, mind a hatóság mindig a dokumentációt kéri először.

Általánosságban elmondható, hogyha egy szervezet már rendelkezik valamilyen információbiztonsághoz kapcsolódó tanúsítvánnyal (pl.: ISO27001, TISAX), akkor az új, NIS 2 bevezetésére tekintettel készítendő szabályzatok és eljárásrendek száma megközelítheti a húszat, ha azonban teljesen kezdők vagyunk ezen a területen, akkor a jogszabályok által megkövetelt dokumentumok száma bőven meghaladja az ötvenet.

A hiányzó dokumentumok elkészítése jelentős erőforrás ráfordítást igényel, akárcsak a hiányzó informatikai megoldások beszerzése. a megfelelősség biztosítása költséges és időigényes feladat, amiről a vezetőségnek már a projekt indulásakor feltétlenül tudnia kell.

Amennyiben nemzetközi léptékben szükséges elmagyaráznunk a szervezetünkre háruló feladatokat, az ENISA által kiadott NIS 2 technikai végrehajtási útmutató segítséget nyújthat ebben, különösen az útmutató „mapping table" verziója[106].

105 Ezek a következő jogszabályok:
1. 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről.
2. 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról 7. mellékletében megfogalmazott követelmények

106 ENISA: NIS 2 Technical Implementation Guidance és Technical Implementation Guidance Mapping table. June 26, 2025.

19

Megérteni és megértetni

Az információbiztonság – a közvélekedés ellenére – nem kizárólag technikai kérdés, hanem szervezeti kultúra és a működés szerves része is. Az MK rendelet, valamint a NIS 2 irányelv alapján a szervezeteknek biztosítaniuk kell, hogy a biztonsági követelmények ne csak a szabályzatokban, eljárásrendekben és egyéb dokumentumokban, hanem a napi működésükben is megjelenjenek. Ennek érdekében szükséges belső koordinációs munkacsoportok kialakítása, valamint a felhasználók rendszeres, célzott tájékoztatása és oktatása is.

Ez a fejezet bemutatja a szervezeten belül létrehozott munkacsoportok szerepét az információbiztonság menedzselésében, valamint a tudatos felhasználói magatartás kialakítására irányuló intézkedéseket, ideértve a képzéseket, a kommunikációs csatornákat és a visszajelzési mechanizmusokat is.

19. Megérteni és megértetni

Írták: dr. Albert Ágota, Kovács György Attila

19.1. Belső munkacsoportok, felhasználók bevonása

Projektindítás és vezetői elköteleződés

Egy NIS 2 által érintett szervezetnél a legelső és legfontosabb lépés a cégtulajdonos/ügyvezető megkeresése. a NIS 2 esetében – akárcsak a klasszikus tanúsítási rendszereknél – alapvető fontosságú a vezetői elkötelezettség, amely számos szempontból elengedhetetlen, mindenekelőtt az erőforrások biztosítása miatt.

Belső munkacsoport struktúra és tagok kiválasztása

Ha megvan a vezetői támogatás, akkor első lépésként szükséges egy olyan személy kijelölése, aki képes projektvezetőként a felkészülés élére állni, illetve – tekintettel a szervezet struktúrájára – azonosítani kell azokat a szervezeti egységeket, amelyek képviselőit javasolt bevonni a felkészülést koordináló és végrehajtó projekt csapatba. Figyelembe véve az MK rendelet alapján kötelező védelmi intézkedéseket, a bevonásra javasolt területek (az elnevezés és méret szervezetenként eltérő lehet):

Informatika,

- Fizikai biztonság / Security,
- Információbiztonsági felelős (IBF) és az adatvédelmi tisztviselő (DPO),
- HR (személyzeti/munkaügyi feladatokat ellátó szervezeti egység),
- Oktatás, képzés (illetve, amelyik szervezeti egység felelős),
- Beszerzés,
- Minőségbiztosítás,
- Létesítmény üzemeltetés,
- Jogi / compliance csapat,
- EIR-tulajdonosok vagy a tulajdonosok képviselői,
- EIR üzemeltetésben résztvevő szerződéses partnerek képviselői,
- Információbiztonsággal összefüggő feladatokat ellátó szerződéses partnerek képviselői (pl.: SOC szolgáltató).

A szervezet belső dinamikájának függvényében célszerű lehet olyan személy(eke)t is bevonni, akik hosszabb távon befolyásolhatnak egyes döntéseket és szabályzat-tartalmakat, például informális véleményformálókat, vagy éppen az Üzemi Tanács képviselőit.

Fontos a bevont szakértők közvetlen felettesével előre tisztázni, hogy egy-egy szakértő számára a projektben való részvétel jelentős időráfordítást igényelhet, és szükség lehet a szakértő napi feladatainak átszervezésére.

Azt is el kell dönteni, milyen külső erőforrás bevonása szükséges, amennyiben szervezeten belül nem áll rendelkezésre megfelelő szakértelem. Ha a szervezet már rendelkezik valamilyen információbiztonsághoz kapcsolódó tanúsítvánnyal (pl.: ISO/IEC 27001:2022, TISAX), akkor ezen irányítási rendszerek bevezetése során szerzett tapasztalatok segíthetnek abban dönteni, hogy szükséges-e külső tanácsadó támogatása vagy sem.

Ha egy szervezet nem rendelkezik azzal a tapasztalattal, ami várhatóan szükséges az auditra történő felkészüléshez, akkor feltétlen javasolt egy külső, komoly szakértelemmel és releváns tapasztalattal bíró, megbízható tanácsadó bevonása.

Milyen kérdések merülhetnek fel már az első lépéseknél?

- Melyik szakterület képviselője milyen döntésbe vonható be? Javasolt stakeholder-mátrix készítése, ötletet a szervezeti és működési szabályzatból, az EIR-ek rendszerbiztonsági terveiből, valamint a belső szabályzatokból és eljárásrendekből lehet meríteni.
- Ki legyen a projekt vezetője? Javasolt olyan személyt választani, akinek van projektvezetői gyakorlata, horizontálisan és vertikálisa ismeri a szervezetet és legalább főbb vonalakban tisztában van a NIS 2 hazai implementálásából eredő követelményekkel. Ideális esetben az IBF lesz a projekt vezetője, de elképzelhető más megoldás is.
- Milyen rendszerességgel tartson megbeszéléseket a projektcsapat? Hogyan oszszák meg a feladat- és hatásköröket?
- Milyen akciótervet/akciólistát és milyen részletességgel vázoljon fel a projektcsapat?

Célszerű úgy kialakítani a kereteket, hogy a projektcsapat tagjai hetente egyszer, projekt státusz megbeszélésen beszámoljanak a rájuk bízott feladat elkészültségi szintjéről. a találkozók állandó napirendi pontjai a felmerülő új kérdések, problémák megvitatása, az akciólistára új akciópontok felvétele. Mindezek érdekében a projekt során végrehajtandó feladatok azonosításához az alábbi kérdések mentén célszerű gondolkodni:

- Hogyan építsük fel a projekttervünket? Milyen fázisokat tudunk azonosítani a végrehajtandó feladatok tekintetében?
- Milyen támogató eszközöket vegyünk igénybe? Például projektindító dokumentum (Project Charter), feladatnyilvántartó sablon (pl.: Gantt), kommunikációs protokoll a projektcsapaton belül (belső ticketing/ütemező eszköz) stb.
- Ki és mely területen végez gap analízist? Hogyan állítjuk össze az útvonaltervünket (intézkedési terveinket), ki határozza meg a kapcsolódó mérföldköveket, mi alapján fókuszáljunk a prioritásokra?
- Rendelkezünk-e a szükséges kockázatértékelésekkel mind az EIR-ek, mind az ellátólánc tekintetében? Ha hiányosságaink vannak ezen a téren, kiket vonjunk be ezek pótlására?
- Kinek melyik szabályzat, eljárásrend aktualizálása lesz a feladata, tekintettel a védelmi intézkedésekre, és ki hangolja össze ezek a szabályzatokat?
- Hogyan oldjuk meg majd a munkavállalók képzését, információbiztonsággal kapcsolatos tudásuk naprakésszé tételét?

A projektvezető feladata ebben az esetben nemcsak az, hogy a szakterületek képviselőit motiválja, hanem az is, hogy megfelelő párbeszédet teremtsen annak érdekében, hogy a felkészülés hatékony és időarányos legyen. A közös cél egy olyan információbiztonsági környezet kialakítása, amely megfelel az elvárásoknak és nem utolsó sorban, „élhető” a szervezet számára.

A projektvezetőnek a cég szervezeti kultúrájának megfelelő (heti, kétheti, maximum havi) gyakorisággal, a szükséges és elégséges elv mentén kell a felső vezetést röviden informálni a felkészülés helyzetéről, valamint azokról a felmerülő új problémákról, amelyekben a felső vezetés segítségére van szükség.

A teljes projekt során kiemelten célszerű kezelni a jogszabályi környezet által determinált kockázatokkal arányos védelem elvét, amelynek biztosítása érdekében már az egyes feladatok és fázisok ütemezése, de különösen a GAP elemzést követő prioritások meghatározása során figyelembe kell venni a rendszerek

és szolgáltatások vonatkozásában azonosított kockázatokat.

Az együttműködés nemcsak a jelenben, hanem a jövőben, illetve rendkívüli helyzetek esetében is fontos – éppen ezért a projekt során megfelelő hangsúllyal kell kezelni azokat a védelmi intézkedéseket, amelyek a különböző szakterületek együttműködését igénylik (különösen, de nem kizárólag üzletmenet-folytonosság, incidenskezelés, szervezeti kommunikáció stb.).

19.2. Szervezeten belüli együttműködés, szervezeti egységek bevonása

A jogszabályi környezetnek történő megfelelés biztosításával megbízott projektcsapat munkájának eredménye lesz több olyan szabályozóból álló keretrendszer, amely a szervezeten belül korábban nem létezett, vagy tartalmilag jelentős átdolgozást igényelt.

A védelmi intézkedések jelentős hányada a védelmi intézkedések megvalósításában részt vevő, valamint az EIR-ekhez hozzáférő munkavállalók, illetve nem munkavállaló státuszú személyeket is érint, éppen ezért a felkészülés során olyan területekre is gondolni kell, amelyek nem tartoznak a hagyományos kiberbiztonsági/információbiztonsági területek közé.

Szervezeti egységek szerepe, tájékoztatása és bevonása

Tisztázni kell az egyes szervezeti egységek szerepét, valamint feladatkörüket, különös tekintettel a védelmi intézkedések megvalósításában betöltött szerepükre, az EIR-ekhez történő hozzáférésük mértékére és kockázati szintjére.

Főbb területek (nem kizárólagos felsorolás) és kapcsolódó tevékenységek:

- Humán erőforrás menedzsment: munkavállalók ki- és beléptetésének, valamint szervezeten belüli mozgásának folyamataiba épített védelmi intézkedések végrehajtása (pl.: munkavállalók háttérellenőrzése, kilépő interjúk stb.), munkaköri leírások megfogalmazása, hozzáférési megállapodások, titoktartási megállapodások és összeférhetetlenségi nyilatkozatok kezelése, alapozó és haladó biztonságtudatossági képzések szervezése, fegyelmi eljárások koordinálása/lefolytatása stb.
- Jogi csapat: védelmi intézkedéseknek megfelelő záradékok beépítése a szerződésekbe (pl.: titoktartási nyilatkozatok, alvállalkozókkal szemben támasztott alapkövetelmények).
- Adatvédelmi tisztviselő: adatfeldolgozási megállapodások, közös adatkezelésre és adatmegosztásra irányuló megállapodások, nemzetközi adatáramlások adatvédelmi, adatbiztonsági és információbiztonsági megfelelősége, adatvédelmi incidenskezelés.
- Beszerzés: beszerzések során az információbiztonsági követelmények érvényesítése, a követelmények implementálása a szerződésekbe, kiírásokba/műszaki leírásokba.
- Biztonsági szolgálat: fizikai védelmi rendszerek összehangolása, az intézkedésekről az érintettek tájékoztatása, az intézkedések következetes érvényesítése.

A szervezeti egységeknek nemcsak a szokásos üzletmenet során kell megvalósítaniuk a védelmi intézkedéseket, hanem kritikus helyzetekben, például kiberbiztonsági és adatvédelmi incidens (pl.: reagálási terv készítése, kivizsgálás, kockázatelemzés, intézkedési tervben foglaltak végrehajtása, stb.), valamint üzletmenet-folytonossággal kapcsolatos problémák felmerülése és megoldása esetén is.

A szervezeti egységek tevékenységének összehangolása során figyelembe kell venni az összeférhetetlenségekkel kapcsolatos előírásokat is. a könnyebb áttekinthetőség érdekében célszerű

folyamatábrákat és felelősségi mátrixokat (pl.: RACI-táblákat) készíteni.

A szervezeti egységekre háruló feladatok áttekintését és számonkérését segíthetik például a kockázatelemzésen alapuló intézkedési tervek, a naprakész szervezeti és működési szabályzat, valamint a szervezet tényleges működéséhez igazodó belső szabályzatok, eljárásrendek és protokollok.

19.3. Felhasználók szerepe, tájékoztatása és bevonása

A felkészülés során be kell(ett) azonosítani, hogy a védelmi intézkedések közül melyek azok, amelyeket a szervezet minden munkatársának ismernie kell. Ezen szabályzatok (vagy szabályzat/eljárás kivonatok) megismertetését, a munkavállalók képzését – igazodva a szervezetünk képzési folyamataihoz – szervezett formában, tervezett módon biztosítani szükséges. a szabályok ismeretével egybekötött tudatosításra irányuló képzés mellett a helyben szokásos módszereket is fel lehet használni a mindenki számára szükséges információk átadására, például belső körleveleket, tudatosító plakátokat, valamint az erre a célra készített intranet oldalakat is. Fontos, hogy ezen tájékoztatások vegyék figyelembe a befogadó közeg jellegzetességeit (írásbeliség, internet és EIR-használat, nyelvi ismeretek stb.).

A biztonságtudatossági képzés hatékonnyá tétele érdekében fontos a felhasználók előzetes tudásmérése és a megszerzett ismeretekkel kapcsolatos utóellenőrzés is, például a biztonságtudatossági képzést követően érdemes rövid tudásfelmérést végezni az ismeretek rögzítése és mérhetősége érdekében.

Számos célirányos termék érhető el az információbiztonsági célú érzékenyítés, tudatosítás, és a belső szabályrendszerrel kapcsolatos ismeretek fejlesztése terén, ezért célszerű megfontolni az e-learning vagy blended learning lehetőségeket is, így kevesebb erőforrással is skálázhatjuk a tájékoztatást.

Fontos követelmény, hogy a képzések megtartásáról, az érintettek tájékoztatásáról, a tudásanyag megismertetésének tényéről és módszeréről naprakész, auditálható nyilvántartást kell vezetni, ezért célszerű olyan megoldást választani, amely nem csak az előkészítés, lebonyolítás, hanem a nyomonkövetés és dokumentálás funkcióját is biztosítja.

Az általános kiberbiztonsági ismereteken túl a munkavállalók szempontjából kiemelten fontos a szervezeti intézkedések, a hozzáférési megállapodások, a szabályzatba foglalt viselkedési szabályok, a titoktartási megállapodások, illetve a fegyelmi felelősség ismerete.

Összességében a következőkre célszerű fókuszálni:

- a biztonságtudatossági célú oktatásokat szerepkörök alapján szükséges kialakítani, amelynek elsődleges feltétele az egyes szerepkörök szabályozási szinten történő meghatározása – célszerű legalább vezető, felhasználó, IT üzemeltetési területen dolgozó, illetve fizikai biztonsággal foglalkozó szerepköröket elkülöníteni a kapcsolódó feladatok figyelembevételével;
- a képzések tartalmi elemeinek meghatározása során tekintettel kell lenni az adott szerepkörök felelősségi körére, valamint a potenciális veszélyeztető tényezőkre is (pl.: egy vezetőnek ismernie kell a szabályzatok által delegált, információbiztonságot érintő döntési felelősségét, illetve az emiatt fokozottan jellemző ún. BEC típusú támadások felismerhető jeleit, míg egy fizikai biztonságért felelős személynek a biztonsági zónákkal kell elsősorban tisztában lennie, illetve a tailgating típusú jogosulatlan belépés sajátosságait kell felismernie);
- nemcsak meg kell alkotni a belső szabályzatokat és eljárásrendeket, hanem ki kell

hirdetni és meg kell ismertetni azokat az érintettekkel;

- mindezt oly módon kell megtenni, hogy ennek ténye utólag bizonyítható legyen;
- az érintetteket a személyes adataik kezeléséről tájékoztatni kell (pl.: naplózás, ellenőrzések stb.).

Amennyiben adatfeldolgozók/közös adatkezelők, illetve az adatfeldolgozók/közös adatkezelők képviselői férnek hozzá az EIR-jeinkhez, valamint az abban tárolt személyes adatokhoz, az ő hozzáférésüket a GDPR előírásainak megfelelő megállapodásokban kell szabályozni.

Előfordulhat, hogy olyan személyek férnek hozzá a rendszerekhez, akik se nem munkavállalók, se nem adatfeldolgozók/közös adatkezelők, ebben az esetben szintén írásos módon kell dokumentálni azt, hogy milyen módon, milyen céllal és milyen mértékben férnek hozzá az adott rendszerhez („hozzáférési megállapodás"). Ilyen felhasználó lehet például a külsős IBF, DPO, könyvvizsgáló, ügyvéd, egyéb szakértők. Ezen felhasználóktól szintén meg kell követelni, hogy a viselkedési szabályokat nemcsak ismerjék, de tartsák is be.

A hatékony és eredmények biztonságtudatosságra fókuszáló keretrendszer kialakításához célszerű figyelembe venni jelen dokumentum 20. fejezetében taglaltakat.

20

„Quick Win” lista

A megfelelés sikeres megvalósítása átfogó szervezeti megközelítést igényel, amely magában foglalja a vezetőség aktív részvételét, dedikált szakértői támogatást és strukturált projektmenedzsmentet.

20. „Quick Win” lista

Írta: Máté Márk

Felsővezetés aktív részvétele és kereszt-funkcionális együttműködés

A NIS 2 irányelv egyik legjelentősebb újítása a vezetői szint közvetlen felelősségre vonása. a 20. cikk értelmében a felsővezetésnek jóvá kell hagynia és felügyelnie kell a kiberbiztonsági intézkedések végrehajtását. Ez fundamentális változást jelent, mivel a kiberbiztonsági kérdések már nem delegálhatók kizárólag az IT részlegre.

A compliance, IT és jogi területek bevonása kritikus fontosságú a kötelezettségek megvalósításában. a sikeres implementáció több szakterület szoros együttműködését igényli. Ez magában foglalja a rendszeres egyeztetések lebonyolítását a kulcsfontosságú érintettek között, a világos felelősségi körök és beszámolási útvonalak meghatározását, valamint a kiberbiztonsági tudatosság növelését minden szinten. Az integrált megközelítés részeként szükséges a jogi, informatikai és üzleti funkciók összehangolása, a közös irányítási struktúrák kialakítása, valamint az egységes incidenskezelési protokollok létrehozása.

- Dedikált felelős személy kijelölése: a Chief Information Security Officer (CISO) vagy más dedikált kiberbiztonsági felelős kijelölése elengedhetetlen. a Magyarország kiberbiztonságáról szóló Kiberbiztonsági tv. 6. § (3) 2. értelmében a szervezet vezetője ,,.kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt...”. Külső szakértőt is ki lehet nevezni az elektronikus információs rendszerek biztonságáért felelős személyként.
- Tanácsadói támogatás és képzés: a tapasztalt tanácsadók bevonása jelentősen felgyorsíthatja a megfelelőség elérését. a tanácsadók segíthetnek a jelenlegi érettségi szint felmérésében, a gap analízis elvégzésében, valamint a prioritások meghatározásában. a projektterv kidolgozása, a technikai megoldások kiválasztása és a folyamatok kialakítása területén is nyújthatnak támogatást.
- Adminisztratív, fizikai és technikai kontroll környezet kialakítás: a NIS 2 irányelv „all-hazards” megközelítést követel, amely magában foglalja a többszintű védelmet. Az adminisztratív kontrollok között szerepel a politikák és eljárások kidolgozása, a szerepkörök és felelősségek meghatározása. a fizikai kontrollok magukban foglalják a létesítmények védelmét, a hozzáférés-vezérlést, valamint a környezeti biztonsági intézkedéseket. a technikai kontrollok közé tartozik többek között a hálózatbiztonság, a titkosítás, valamint a monitoring és logging rendszerek.
- Meglévő tanúsítvány(ok) integrálása, ha van(nak): a meglévő pl.: ISO/IEC 27001:2022 tanúsítvány jelentős előnyt jelent a megfelelőség elérésében. a két követelményrendszer között számos átfedés található.
- Remediációs mérföldkövek: a strukturált implementáció kulcsfontosságú a sikeres megfelelőség eléréséhez. - Az előkészítési szakaszban történik a vezetői elkötelezettség biztosítása, a projektcsapat felállítása, valamint a jelenlegi állapot felmérése.
- - a tervezési szakasz magában foglalja a részletes gap analízis elvégzését, a remediációs terv kidolgozását, valamint az erőforrás-allokációt. - Az implementációs szakasz során kerül sor a technikai megoldások bevezetésére, a folyamatok kialakítására,

valamint a képzések lebonyolítására. - a tesztelési és finomhangolási szakasz tartalmazza az incidenskezelési gyakorlatok végrehajtását, a belső auditok lebonyolítását, valamint a folyamatos javítások implementálását. A haladás nyomon követése objektív mutatók alapján történik, úgymint az implementált kontrollok száma, a képzésben résztvevők aránya, az incidenskezelési reakcióidő, valamint az audit eredmények.

- Pre-audit és megfelelőség ellenőrzése: a rendszeres belső auditok biztosítják a folyamatos megfelelőséget. Az audit területek magukban foglalják a technikai kontrollok hatékonyságát, a folyamatok betartását, a dokumentáció megfelelőségét, valamint a képzési programok eredményességét. a független harmadik fél általi értékelés objektív képet ad a szervezet felkészültségéről. Ez magában foglalja a megfelelőségi állapot validálását, a további fejlesztési lehetőségek azonosítását, valamint az audit-készség felmérését.

A megfelelőség elérése komplex, de jól strukturált folyamat, amely a fenti quick win-ek követésével hatékonyan megvalósítható. a kulcs a vezetői elkötelezettség, a megfelelő szakértelem bevonása és a folyamatos fejlesztés kultúrájának kialakítása.

21

Szankciók és következmények

A NIS 2 irányelv és a kapcsolódó hazai jogszabályok megszegése nemcsak a kiberbiztonsági kockázatokat növeli, hanem jogi és pénzügyi következményekkel is járhat. a szankciók célja a jogkövető magatartás kikényszerítése, a megfelelő incidenskezelés ösztönzése és a hálózati, információs rendszerek biztonságának erősítése. a hatóság döntéseiben figyelembe veszi a jogsértés súlyát, ismétlődését és a szervezet együttműködési hajlandóságát is, ezáltal biztosítva az intézkedések arányosságát. a következmények így nemcsak elrettentő erőt képviselnek, hanem arra is ösztönzik a szervezeteket és az auditorokat, hogy a megfelelőség fenntartását folyamatos, stratégiai feladatként kezeljék.

21. Szankciók és következmények

Írták: Biró Gabriella, Robotka Árpád

21.1. Jogkövetkezmények a szervezettel és annak vezetőjével szemben

Ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és eljárási szabályokat nem teljesíti vagy nem tartja be, illetve valamely uniós tagállam kiberbiztonsági hatósága kölcsönös segítségnyújtás keretében megkeresést küld Magyarországra, a kiberbiztonsági hatóság jogkövetkezményeket alkalmazhat az érintett szervezettel szemben. a jogkövetkezmény lehet intézkedés vagy bírság.

A kiberbiztonsági hatóság a következő intézkedéseket alkalmazhatja:

- figyelmeztetheti a szervezetet a biztonsági követelmények és a kapcsolódó eljárási szabályok betartására;
- felszólíthatja a szervezetet megfelelő határidő tűzésével a biztonsági hiányosságok elhárítására, a megfeleléshez szükséges intézkedések meghozatalára, a jelentéstételi és adatszolgáltatási kötelezettségek teljesítésére;
- kötelezheti a szervezetet a jogsértő magatartás megszüntetésére, azonnali intézkedések megtételére és fegyelmi felelősség megállapítására is javaslatot tehet a munkáltatói jogkör gyakorlója felé;
- a szervezetet felügyelő szervhez vagy a tulajdonosi joggyakorlóhoz fordulhat és kérheti a közreműködését;
- jogosult a szervezet költségére információbiztonsági felügyelőt kirendelni.

Ha az alkalmazott intézkedések ellenére az érintett szervezet továbbra sem felel meg a kiberbiztonsági követelményeknek, a hatóság az eset összes körülményének mérlegelésével bírságot szabhat ki a szervezettel, valamint a szervezet vezetőjével szemben is.

A kiszabható bírság legmagasabb összege:

- alapvető szervezettel szemben 10 millió eurónak megfelelő forintösszeg vagy az előző év globális forgalmának 2%-a közül a magasabb összeg;
- fontos szervezettel szemben 7 millió eurónak megfelelő forintösszeg vagy az előző év globális forgalmának 1.4%-a közül a magasabb összeg;
- a szervezet vezetőjével szemben 15 millió forint személyi bírság.

Ezeken túl a kiberbiztonsági hatóság:

- kötelezheti a szervezetet a jogszabálysértés tényének és körülményeinek nyilvánosságra hozására;
- elrendelheti a szervezet által nyújtott szolgáltatásokat igénybe vevők tájékoztatását a potenciális fenyegetésekről;
- kiberbiztonsági incidens bekövetkezése esetén a honlapján tájékoztathatja a nyilvánosságot, illetve a szervezeteket határozatban kötelezheti tájékoztatásra;
- kötelezheti a szervezetet arra, hogy válságkezelési vagy veszélyhelyzet-kezelési intézkedés megtételének szükségessége esetén tájékoztassa a kiberbiztonsági hatóságot;
- nem közigazgatási szervnek minősülő alapvető szervezet esetében kezdeményezheti az illetékes hatóságnál az általa végzett tevékenységre vonatkozó tanúsítás vagy engedély ideiglenes felfüggesztését és kezdeményezheti a cégbíróságnál ezen szervezet vezetőjének ideiglenes

eltiltását a vezető tisztségviselői feladatok ellátásától;

- ha a hatósági kötelezést a szervezet figyelmen kívül hagyja vagy a javasolt védelmi intézkedéseket nem teljesíti és ezzel kiberbiztonsági incidenst vagy incidensközeli helyzetet teremt, a szervezetet a kiberbiztonsági hatóság az elhárításra fordított költségek megtérítésére kötelezheti.

Fentieken túl az SZTFH

- jogosult eltiltani az érintett szervezetet a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységtől;
- bírság kiszabása esetén tájékoztatja a szervezet tevékenységét engedélyező vagy felügyelő hatóságot a bírság kiszabásáról és a kiszabást megalapozó tényekről.

21.2. Jogkövetkezmények az auditorral szemben

Ha az auditor a jogszabályokban foglalt kiberbiztonsági követelményeket vagy a kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az SZTFH jogosult az auditort:

- figyelmeztetni a jogszabályok és az eljárási szabályok teljesítésére;
- határidő tűzésével kötelezni a megfeleléshez szükséges intézkedések megtételére;
- az auditori tevékenységtől ideiglenesen eltiltani.

Ha a fenti intézkedések ellenére az auditor a jogszabályi kötelezettségének nem tesz eleget, az SZTFH az eset összes körülményének mérlegelésével bírságot szabhat ki, amely nemteljesítés esetén megismételhető.

Ha az SZTFH az auditor tevékenységével kapcsolatban olyan jogsértést tár fel, amely hatással van az ellenőrzött szervezetre, arról értesíti a szervezet IBF-jét.

21.3. A jogkövetkez-mények alkalmazása

A kiberbiztonsági hatóság az egyes jogkövetkezményeket egymás mellett is alkalmazhatja, az alábbi szempontok figyelembevételével:

- a hiányosság, mulasztás súlya;
- a jogsértés időtartama;
- történt-e jelentős vagy nagyszabású kiberbiztonsági incidens vagy fennált-e annak veszélye?
- az incidens milyen hatással volt vagy lehetett volna az érintett vagy más szervezetre?
- okozott-e vagyoni vagy nem vagyoni kárt?
- az esemény egyedi vagy ismételt jellegű volt?
- az érintett szervezet korábban elkövetett releváns jogsértései;
- szándékos vagy gondatlan volt a jogsértés?
- az érintett szervezet magatartása, a kár megelőzésére vagy kárenyhítésre tett intézkedései;
- a jóváhagyott magatartási kódexek vagy jóváhagyott tanúsítási mechanizmusok betartása;
- az illetékes hatóságokkal való együttműködés szintje;
- a tervezett jogkövetkezmény hatékonysága, arányossága és visszatartó ereje.

Súlyos jogsértésnek minősülnek:

- az ismételt jogsértések;
- a jelentős események bejelentésének vagy orvoslásának elmaradása;
- ha a hatósági kötelezés után is elmarad a hiányosságok orvoslása;
- az ellenőrzési tevékenységek akadályozása;
- hamis vagy súlyosan pontatlan információk közlése.

21.4. Jogorvoslat

A kiberbiztonsági hatóság döntése ellen fellebbezés nem lehetséges. a végleges döntés ellen közigazgatási per indítható az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény szabályai szerint.

Ez azt jelenti, hogy ha valaki nem ért egyet a kiberbiztonsági hatóság döntésével, nem tud közvetlenül fellebbezni, hanem bírósági úton, közigazgatási per keretében kérheti a döntés felülvizsgálatát.

22

Biztonsági kultúra és tudatosság

A NIS 2 irányelv csak elvi szinten írja elő a „basic cyber hygiene practices and cybersecurity training”-et, illetve a vezetés kötelező képzését. Nem határoz meg óraszámot, szerepkör-bontást vagy formát. a magyar végrehajtás (Kiberbiztonsági tv., MK rendelet, 17/2025. EM rendelet stb.) ezzel szemben szerepkörökre és óraszámokra bont, részletesen szabályozza a képzések tartalmát, gyakoriságát, dokumentálását és a hatósági ellenőrzést. Bár a jogszabályi előírások szigorítása és akár a konkrét óraszámok meghatározása nagyon előremutató, de a tudatosság, mint viselkedési forma kialakulása nem egy olyan dolog, amit pusztán egy jogszabály életbe léptetése létre fog hozni.

©2025SOLEMOSÁKOS

22. Biztonsági kultúra és tudatosság

Írta: Solymos Ákos

Általános biztonságtudatosság

A világ erősen afelé halad, hogy egyre több feladatot látnak el automatizált entitások, hívhatjuk őket robotoknak, chatbotoknak, digitális asszisztenseknek, mégis a folyamatok végén egy ember áll, akinek a tudatossága meghatátozza az adott folyamat vagy döntés eredményét. Ez a tudatosság számos területre vonatkozhat és mindennek valamilyen hatása van. a környezettudatosság a környezetünk és a természet védelmére koncentrál, a tudatos nevelés a gyermekeink felelősségteljes felnőtté válását célozza, a biztonságtudatosság pedig az adott védendő értékek megóvásával kapcsolatos viselkedési formákra koncentrál.

A biztonságtudatosság is fakadhat családi gyökerekből, otthonról hozott és másolt viselkedésformákból, fakadhat transzgenerációs berögződésekből és hatással lehet rá a közvetlen környezet, akár a munkahely vagy egy közösség is. És ahogy szomorúan tapasztaljuk, sokszor egy-egy incidens, adatvesztés, kényelmetlen szituáció az, ami gondolkodásra és a viselkedésének megváltoztatására készteti a felhasználót vagy akár egy komplett szervezetet is (“. nekünk Mohács kell!”). a biztonságtudatosságot érdemes lenne már kisgyerekkortól beépíteni a nevelésbe, mivel ez jó alapot képezne a többi különböző tudatossági attitűd kialakulásához, azonban ennek a dokumentumnak nem célja ezen témák részletes kifejtése.

Összességében kijelenthető, hogy ha a felhasználó már alapjaiban véve is biztonságtudatosan gondolkodik és viselkedik, akkor sokkal könnyebb a szervezeti biztonsági szabályokat megértetni és elfogadtatni vele, és sokkal kisebb eséllyel fogja megpróbálni megkerülni vagy kijátszani a kontrollokat, védelmi intézkedéseket.

A biztonsági szabályok oktatása nem egyenlő a biztonságtudatosítással! Nem véletlen, hogy a vonatkozó jogszabályok is tudatosításként hivatkoznak erre a tevékenységre.

Gyakorlati aspektusok

Ebben a fejezetben olyan jó gyakorlatokat fogunk ismertetni, amelyek segítenek abban, hogy a szervezet ne csak megfeleljen a szabályozók előírásainak, hanem valóban hasznos szemléletformálás valósulhasson meg.

A biztonságtudatosság a szervezeti kultúra és a biztonsági kultúra része kell, hogy legyen. Ez persze jelentős erőforrásokat igényel kezdetben, de aztán olyan lesz az egész, mint a lendkerekes kisautó, ami megy magától és csak néha kell ismét lendületbe hozni, ami sokkal kisebb erőforrás, mintha megállna és újra el kellene indítani. Ha a biztonsági szabályok, a gyakorlatok, a különböző tesztek és az erre való felkészülés elindult és a felhasználók ezt már a mindennapok részeként élik meg, akkor az új dolgozók sokkal gyorsabban fogják tudni felvenni azt a sebességet, amivel ők is ennek a “lendkeréknek” a részei lesznek.

Terjedelmi okokból eltekintünk a konkrét jogszabályi hivatkozások idézgetésétől, de ami a lényeg, hogy a korábbi általános elvárásokhoz képest, miszerint “Legyen biztonsági oktatás évente egyszer”, a friss jogszabályok egy sokkal szofisztikáltabb, tervezett, szabályozott és mérhető tudatosítási és képzési rendszert írnak elő. a képzéseket általában és a biztonságtudatosítást is számos szempontból lehet és kell vizsgálni, ha valaki nem csak a kötelező minimumot akarja teljesíteni.

Hosszútávon javasolt a biztonságtudatosítási tevékenységet elkülönülten kezelni a szervezeti biztonsági szabályok megismertetésétől.

Időhorizont

Ha egy időhorizonton nézzük ezt a témakört, akkor érdemes felbontani (jogszabály szerint is így kell) a képzéseket újbelépő képzésekre és éves ismétlő képzésekre. a legszigorúbb módszer az, hogy addig nem is kaphat informatikai hozzáféréseket a felhasználó, amíg a szükséges előírt újbelépő képzéseken meg nem felelt.

Ennél enyhébb és némileg kockázatosabb, ha mondjuk havonta összevárják az újbelépőket és frontális oktatás jelleggel kapják meg az induló biztonsági ismereteket. Leszámítva azt, ahol egyáltalán nincsenek ismétlő képzések, a legkockázatosabb az, ha az új belépők megkapják a hozzáféréseiket és majd az éves ismétlő képzésen vesznek részt a régebbi kollégákkal. Ez azért rendkívül kockázatos, mert ebben az esetben a képzésig, ha a felhasználó közvetlenül az éves ismétlő képzés után érkezett, akár 11 hónap is eltelhet. Ilyenkor a felhasználó a kollégái tanácsai és a saját tapasztalásai alapján működik a szervezetben. Ez azért is a legrosszabb opció, mert mire a felhasználó eljut a képzésig, addig kialakulnak benne rossz gyakorlatok, félreértések, amelyek rossz esetben akár kiberbiztonsági incidensekhez is vezethetnek, ráadásul sokkal nehezebben fogja befogadni a valóban elvárt viselkedést és folyamatokat.

Képzések módja

A másik aspektus, ami általában erősen erőforrás és vezetői hozzáállás függő, az a képzés módja. Régebben, itt akár egy-két évtizeddel korábbra is gondolhatunk, a frontális, tantermi jellegű oktatás volt a jellemző, már ott, ahol volt egyáltalán. Mivel a felhasználók befogadási képessége eltérő, ez a képzési forma nem hatékony. Ráadásul sok esetben a Humán terület igyekszik optimalizálni a dolgozók értékteremtő folyamatokból való kiemelését. Vagyis jellemző, hogy van egy “oktatási nap”, amikor reggeltől estig a kollégák előadásokat hallgatnak mindenféle témában. Ebben egy a sok közül a biztonság. Az ilyen képzéseknek általában nagyon erőteljes a felejtési görbéje. Akár már órákkal később sem emlékeznek a felhasználók semmire, ami az előadáson elhangzott. Persze ez függ az előadótól, a témától és az előadás akár napon belüli időpontjától, így a hallgatóság fáradtságától, információ-telítettségétől is. Ráadásul szinte lehetetlen a teljes céget egy napra kivenni a folyamatokból.

Ennél hatékonyabb módszer az e-learning. Ez már komolyabb beruházás, mivel LMS-t (Learning Management System) kell működtetni/bérelni, tananyagokat kell készíteni, készíttetni vagy szintén bérelni és testreszabni. Ugyanakkor előnye, hogy a felhasználók szabad ütemezésben haladhatnak, mérhető a tudás és ismeretszerzés, akár vizsgáztatni is lehet, kevésbé probléma a nyelvi korlát és ami nagyon fontos időtől és tértől függetlenül elérhető és automatizálható. Ha az LMS kellően nagy tesztkérdés adatbázist használ, akkor a vizsgán vagy a tudásvisszaméréseken a csalás és “közösségi vizsgázás” kockázata is alacsony.

A leghatékonyabbak az olyan biztonságtudatosítási kampányok, amelyek, bár versenyeznek a szervezet többi területével, belső híreivel és oktatási anyagával, több területet, témát felölelve, egy hosszabb időhorizonton fejtik ki hatásukat, lehetőséget adva akár gyakorlatban is kipróbálni a biztonsággal kapcsolatos ismereteket (például social engineering kampányok, lockpicking, szabadulószoba stb.). Az ilyen biztonságtudatossági kampányokra már akár fél évvel a kampány előtt el kell kezdeni készülni. Az ilyen tevékenységet lehet színesíteni játékosítással (gamifikáció), versenyekkel, nyereményekkel is, amelyek növelhetik a bevonódást és így a tudás mélyebb rögzülését is. a kampányokat érdemes kiegészíteni valósághű szimulációkkal, ahol éles, de kontrollált támadásokkal kerülnek szembe a felhasználók. Az ilyen támadás szimulációkkal jól mérhető a képzések és a tudatosítási kampányok pozitív hatása.

Természetesen a tudatosítási kampányokon kívül is lehet tudatosítási tevékenységet végezni, akár egész évben, folyamatosan. Intranet hírek, céges rendezvényeken előadások vagy workshopok megtartása mind segíthet egy-egy fontos témát a felhasználók látókörében tartani.

Felhasználókat érintő képzéseket és kampányokat a szervezetek maguk is létre tudnak hozni, ha rendelkeznek megfelelő tapasztalattal, tudással és erőforrással, de hazai és nemzetközi biztonsági tanácsadó cégek is kínálnak ilyen szolgáltatásokat. Ami mindegyikben közös, az az, hogy rá kell szánni a felhasználók idejét, mivel a biztonságtudatosságot nem lehet tablettában bevenni.

Speciális területek – Információbiztonságért felelős vezetők és szervezeti vezetők képzései

Jelen dokumentum készítésének idején jelent meg a 17/2025. (VII. 24.) EM rendelet, amely egészen konkrét előírásokat fogalmaz meg a képzésekről és az elvárt végzettségekről nem csak az információbiztonságért felelős vezetők, hanem egyéb szervezeti szerepkörök számára is. Mindezek azért rendkívül fontosak, mert az elmúlt évek – évtizedek gyakorlata azt mutatta, hogy a biztonságtudatosítás és általában a biztonsági képzések a felsővezetőkre nem vonatkoztak. Még ha a belső szabályozás elő is írta a teljeskörűséget, a felsővezetők esetében már az is siker volt, ha az információbiztonsági vezető egy negyedórás idősávot kapott évente egyszer valamelyik felsővezetői értekezleten. De látjuk, tudjuk, hogy ez formalitás volt, valós hozzáadott értéket kis mértékben jelentett csak.

A jogszabály előírja, hogy az elektronikus információs rendszer biztonságáért felelős személynek évente legalább húsz órás, legalább három meghatározott tárgykörben (például kiberbiztonsági trendek; kockázatkezelés és szervezeti stratégiák; uniós és hazai jogszabályi változások; incidenskezelés; technológiai ismeretek; hatósági együttműködés; jó gyakorlatok megosztása; stb.) tartozó továbbképzésen kell részt vennie, ezzel folyamatosan bővítve szakmai tudását és megfelelve a 3. § (1)–(2) pontokban rögzítetteknek.

Üdvözlendő újdonság, hogy a szervezet vezetőjére vonatkozóan is meghatároz képzéseket kiberbiztonsági témakörben. a szervezet vezetőjének, a kinevezést követő egy éven belül legalább nyolc órás alapozó képzésen kell részt vennie, majd ezt követően évente legalább négyórás továbbképzést kell szervezni a kiberbiztonsági trendekről, kockázat- és stratégia alkotásról, jogszabályi kötelezettségek változásairól, incidenskezelési feladatokról, valamint jó gyakorlatok ismertetéséről a 4. § (1)–(2) bekezdés szerint.

Mindkét képzési kötelezettség esetén a programokat a felnőttképzésről szóló 2013. évi LXXVII. törvény szerinti, legalább hároméves szakmai tapasztalattal rendelkező, bejelentett felnőttképző intézménynek kell lebonyolítania, és a képzési programot – a 5. § (2)–(3) bekezdésben meghatározottak alapján – az Fktv. adatszolgáltatási rendszerébe fel kell tölteni. a rendelet hangsúlyozza, hogy a tananyag és a képzés formája – legyen az e-learning, workshop vagy gyakorlati szeminárium – legyen alkalmas a résztvevők aktív bevonására és a megszerzett ismeretek alkalmazására, mivel ez biztosítja a jogszabályban előírt folyamatos megfelelőséget és a hatósági ellenőrzés során igazolható tanúsítványok megszerzését.

Speciális területek – IT üzemeltetők és fejlesztők

Nem ejtettünk még szót egy speciális körről, az IT üzemeltető (ideértve a biztonsági infrastruktúrák üzemeltetését is) és fejlesztő kollégákról. a Kiberbiztonsági tv. és a nemrég megjelent képzettségekről szóló jogszabály sem említi külön őket, pedig meghatározó szerepük van a szervezet kiberbiztonsági ellenállóképességének megteremtésében. Az IT-s szerepkörökre vonatkozó

képzési kötelezettségek nem különülnek el teljesen az általános felhasználókat és a vezetőket érintő képzésektől. Ezért inkább az MK rendeletben kell keresnünk a rájuk vonatkozó előírásokat. a rendelet szerint minden, az elektronikus információs rendszerrel (EIR) közvetlenül foglalkozó kolléga – így az üzemeltetők és fejlesztők is – a szerepkörükhöz rendelt védelmi intézkedéseket és tudatossági kontrollokat kell, hogy megismerjék, majd képesnek kell lenniük ezen ismeretek gyakorlatba ültetésére is. Ez pedig speciális képzéseket igényel.

Konkrétan az MK rendelet 1. melléklete és a hozzá kapcsolódó EIR-útmutató kiemeli, hogy a fejlesztőknek és üzemeltetőknek a „Tudatosság és képzés" kontrollcsoporton belül nemcsak általános, hanem szerepkörspecifikus tartalmakat kell elsajátítaniuk – például a biztonsági tesztelés, a sebezhetőség-kezelés, a konfigurációk biztonsági megerősítése (hardening) és a naplózás elemzése terén. Ezekre pedig speciális, ráadásul az átlagos felhasználói biztonságtudatosítási képzéseknél jelentősen drágább és hosszabb képzéseken lehet szert tenni.

Ez tudatos tervezést igényel a képzési budget összeállításánál. Ilyen képzéseket a nagyobb szakmai szervezetek (ISC)², CompTIA, EC-Council, Offensive Security (OffSec)) képzései között kell keresni.

Összefoglalva a biztonságtudatosítás és képzés, egy nagyon fontos és nélkülözhetetlen kontrolterületté vált, amelyet már nem lehet egy jelenléti ív aláíratásával elintézni. Amely szervezetek továbbra is úgy gondolják, hogy nem éri meg képezni a kollégákat a megfelelő szinten, azok jelentős kockázatnak teszik ki magukat és ügyfeleiket. a kiberbiztonsági incidensek továbbra is jelentős részben a humán faktor képzetlenségéből és figyelmetlenségéből – vagy a biztonságtudatosság hiányából – fakadnak.

23. Rövidítés-jegyzék

ABAC – Attribute-Based Access Control; magyarul: Attribútum alapú hozzáférés-vezérlés

ACN – Agenzia per la Cybersicurezza Nazionale; magyarul: Nemzeti Kiberbiztonsági Ügynökség

AI – Artificial Intelligence; magyarul: mesterséges intelligencia

AI Act – Artificial Intelligence Act; magyarul: Mesterséges Intelligencia Rendelet

BCMS – Business Continuity Management System; magyarul: üzletmenet-folytonosság irányítási rendszer

BCP – Business Continuity Plan; magyarul: üzletmenetfolytonossági terv

BIA- Business Impact Analysis; magyarul: Üzleti Hatáselemzés

BM OKF – Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság

BMI – Bundesministerium für Inneres; magyarul: Szövetségi Belügyminisztérium

BPM – Business Process Management; magyarul: üzleti folyamatmenedzsment

BPR – Business Process Reengineering; magyarul: üzleti folyamatok újratervezése

BQSA – Blockchain-based Quantum-Safe Architecture; magyarul: Blockchain-alapú kvantumbiztos architektúra

BSI – Bundesamt für Sicherheit in der Informationstechnik; magyarul: Szövetségi Információbiztonsági Hivatal

BYOD – Bring Your Own Device; magyarul: „Hozd a saját eszközöd”

CAQI – Common Assurance and Quality Indicator; magyarul: Közös biztosítási és minőségi mutató

CCB – Centre for Cybersecurity Belgium; magyarul: Belgiumi Kiberbiztonsági Központ

CDN – Content Delivery Network; magyarul: tartalomszolgáltató hálózat

CER – Critical Entities Resilience Directive; magyarul: Irányelv a kritikus fontosságú szervezetek rezilienciájáról

CERT – Computer Emergency Response Team; magyarul: Számítógépes Vészhelyzetekre Reagáló Csoport

CIA – Confidentiality, Integrity, Availability; magyarul: bizalmasság, sértetlenség és rendelkezésre állás

CIP Security – Common Industrial Protocol Security; magyarul: Közös ipari protokoll biztonsági kiterjesztése

CMDB – Configuration Management Database; magyarul: konfigurációkezelési adatbázis

CyFun – CyberFundamentals Framework; magyarul: Kibervédelmi Alapelvek Keretrendszere

CSA CAIQ – Cloud Security Alliance Consensus Assessments Initiative Questionnaire; magyarul: Felhőbiztonsági Szövetség Konszenzusos Értékelési Kérdőív

CSA STAR – Cloud Security Alliance Security, Trust & Assurance Registry; magyarul: Felhőbiztonsági Szövetség Biztonsági, Megbízhatósági és Biztosítottsági Nyilvántartás

CSIRT – Computer Security Incident Response Teams; magyarul: Számítógépes biztonsági incidenskezelő csoport

DARPA – Defense Advanced Research Projects Agency; magyarul: Védelmi Fejlett Kutatási Projektek Ügynöksége (USA)

DEV környezet – Development environment; magyarul: fejlesztői környezet

DNP3 – Distributed Network Protocol 3; magyarul: Elosztott hálózati protokoll, 3-as verzió

DNS-szolgáltatás – Domain Name System szolgáltatás; magyarul: Tartománynév-rendszer szolgáltatás

DORA – Digital Operational Resilience Act; magyarul: Digitális Operatív Reziliencia Rendelet

DPIA – Data Protection Impact Assessment; magyarul: Adatvédelmi hatásvizsgálat

DRP – Disaster Recovery Plan; magyarul katasztrófaelhárítási terv

DSP – Digital Service Provider; magyarul: digitális szolgáltató

ECC – Elliptic Curve Cryptography; magyarul: Elliptikus görbéken alapuló kriptográfia

EDR – Endpoint Detection and Response; magyarul: végponti észlelés és reagálás

eIDAS – electronic IDentification, Authentication and trust Services; magyarul: elektronikus azonosítás, hitelesítés és bizalmi szolgáltatások

EIR – elektronikus információs rendszer

EK – Európai Közösség

ENISA – European Union Agency for Cybersecurity; magyarul: Európai Uniós Kiberbiztonsági Ügynökség

ENX – European Network Exchange

EU – European Union; magyarul: Európai Unió

EU-CyCLONe – European Cyber Crisis Liaison Organisation Network; magyarul: Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata

EUR – euró

FALCON-1024 – Fast Fourier Lattice-based Compact Signatures over NTRU (paraméter: 1024); magyarul: Gyors, Fourier-transzformációt használó, rácsalapú kompakt aláírás NTRU fölött (1024-es paraméterkészlettel)

GAP elemzés – eltérés elemzés

GDPR – General Data Protection Regulation; magyarul: Általános adatvédelmi rendelet

HKH – Honvédelmi Kiberbiztonsági Hatóság

HR – Human Resources; magyarul: emberi erőforrások

HSM – Hardware Security Module; magyarul: Hardveres biztonsági modul

HVAC – Heating, Ventilation, and Air Conditioning; magyarul: Fűtés, szellőztetés és légkondicionálás

IAM – Identity and Access Management; magyarul: Személyazonosság- és hozzáférés-kezelés

IB – információbiztonság

IBF – Információbiztonsági Felelős

IBSZ – Információbiztonsági Szabályzat

ICS – Industrial Control Systems, magyarul: Ipari irányító rendszerek

IDS – Intrusion Detection System; magyarul: Behatolás-észlelő rendszer

IEC – International Electrotechnical Commission; magyarul: Nemzetközi Elektrotechnikai Bizottság

IIoT – Industrial Internet of Things; magyarul: Ipari dolgok internete

IKT – információs és kommunikációs technológia

IPS – Intrusion Prevention System; magyarul: Behatolás-megelőző rendszer

ISO – International Organization for Standardization; magyarul: Nemzetközi Szabványügyi Szervezet

IT- Information Technology, magyarul: Információs Technológia

ITSM-rendszer – IT Service Management system, magyarul: IT-szolgáltatásmenedzsment-rendszer

K+F – kutatás és fejlesztés

Kiberbiztonsági tv. – 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

Kibertan. tv. – a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

KKV – Kis- és középvállalatok

Kormányrendelet – 418/2024. (X. 30.) Korm. rendelet,

KPI – Key Performance Indicator; magyarul: kulcs teljesítménymutató

KSH – Központi Statisztikai Hivatal

MAM – Mobile Application Management

MDM – Mobile Device Management

MFA – Multi-Factor Authentication; magyarul többtényezős hitelesítés

MI – Mesterséges Intelligencia

MK rendelet – 7/2024. (XI. 15.) MK rendelet

MKKR – Magyar Képesítési Keretrendszer

NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság

NBSZ – Nemzetbiztonsági Szakszolgálat

NCSC/CERT.LV – National Cyber Security Centre / Computer Emergency Response Team Latvia; magyarul: Lett Nemzeti Kiberbiztonsági Központ / Számítógépes Vészhelyzetekre Reagáló Csapat

NDR – Network Detection and Response; magyarul: hálózati észlelés és reagálás

NCC – Nemzeti Koordinációs Központ, az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) küldetésének és célkitűzéseinek támogatása érdekében nemzeti kapcsolattartó és koordinációs pontként szolgál. A magyar központ az NCC-HU.

NIS1 – Network and Information Systems Directive; magyarul: Hálózati és információs rendszerek irányelv (első változat)

NIS 2 – Network and Information Security Directive (version 2); magyarul: Hálózati és információs rendszerek biztonságáról szóló irányelv (második változat)

NISG – Netz- und Informationssystemsicherheitsgesetz; magyarul: hálózati és információbiztonsági törvény

NIST CSF – National Institute of Standards and Technology Cybersecurity Framework; magyarul: Nemzeti Szabványügyi és Technológiai Intézet Kiberbiztonsági Keretrendszer

NIST SP – National Institute of Standards and Technology Special Publication; magyarul: Nemzeti Szabványügyi és Technológiai Intézet Különkiadvány

NKI – Nemzeti Kiberbiztonsági Intézet

NMHH – Nemzeti Média- és Hírközlési Hatóság

OAuth – Open Authorization; magyarul: Nyílt jogosultságkezelési protokoll

OECD – Organisation for Economic Co-operation and Development; magyarul: Gazdasági Együttműködési és Fejlesztési Szervezet

OES – Operator of Essential Services; magyarul: alapvető szolgáltatást nyújtó szervezet

OLA – Operational Level Agreement; magyarul: Működési szintű megállapodás

OPC UA – Open Platform Communications Unified Architecture; magyarul: Nyílt platformú kommunikáció egységes architektúrája

OSCAL – Open Security Controls Assessment Language; magyarul: Nyílt Biztonsági Kontroll Értékelési Nyelv

OSDP – Open Supervised Device Protocol – Biztonságtechnikai iparági szabvány, amely a beléptető rendszerek kártyaolvasói és vezérlőpanelei közötti kommunikációt teszi biztonságosabbá és interoperábilissá (átjárhatóvá)

OT – Operational Technology; magyarul: ipari működtető technológia, üzemirányítási technológia

PAM – Privileged Access Management; magyarul: Kiemelt hozzáférés-kezelés

PCI DSS – Payment Card Industry Data Security Standard; magyarul: Fizetési Kártyaipari Adatbiztonsági Szabvány

PDCA – Plan – Do – Check – Act; magyarul: Tervezés – Végrehajtás – Ellenőrzés – Beavatkozás

PPT – (People, Process, Technology; magyarul: Személyek – Folyamatok – Technológia

PQC – Post-Quantum Cryptography; magyarul: Kvantum utáni (kvantumbiztos) kriptográfia

QCC – Quantum Communication Channel; magyarul: Kvantum kommunikációs csatorna

RBAC – Role-Based Access Control; magyarul: Szerepkör alapú hozzáférés-vezérlés

RACI – Responsible, Accountable, Consulted, Informed; magyarul: Felelős, Jóváhagyó, Konzultáló, Tájékoztatott

RBT – rendszerbiztonsági terv

RDSI – Réseau Numérique à Intégration de Services (Integrated Services Digital Network, ISDN); magyarul: Szolgáltatásintegrált digitális hálózat

RPO – Recovery Point Objective; magyarul: Helyreállítási Pont Célérték

RSA – Rivest–Shamir–Adleman; magyarul: Rivest–Shamir–Adleman nyilvános kulcsú titkosítási algoritmus

RTO – Recovery Time Objective; magyarul: Helyreállítási Idő Célérték

SaaS – Software as a Service; magyarul: szoftver mint szolgáltatás

SAB – Satversmes aizsardzības birojs; magyarul: Lett Alkotmányvédelmi Hivatal

SAML – Security Assertion Markup Language; magyarul: Biztonsági Nyilatkozati Jelölőnyelv

SIEM – Security Information and Event Management; magyarul: Biztonsági információ- és eseménykezelő rendszer

SIG-Full – Standardized Information Gathering Questionnaire (Full); magyarul: Szabványosított Információgyűjtő Kérdőív (teljes verzió)

SIS – Safety Instrumented System; magyarul biztonsági vezérlőrendszer

SL2 – Security Level 2; magyarul: 2. biztonsági szint

SLA – Service Level Agreement; magyarul: Szolgáltatási szint megállapodás

SMART – Specific, Measurable, Achievable, Relevant, Time-bound; magyarul: Konkrét – Mérhető – Elérhető – Releváns – Időhöz kötött

SMS – Safety Management System; magyarul: Biztonsági Irányítási Rendszer

SOC – Security Operation Center; magyarul: Biztonsági Műveleti Központ

SOC 2 – System and Organization Controls 2; magyarul: Rendszer- és Szervezeti Kontrollok 2. típusú jelentés

SPHINCS+ – Stateless Practical Hash-based Incredibly Nice Cryptographic Signature Plus; magyarul: Állapotmentes, gyakorlatban alkalmazható, hash-alapú kriptográfiai aláírásrendszer (Plus változat)

SPOC – Single Point of Contact; magyarul: egyablakos ügyintézési pont

SSH-Q – Secure Shell – Quantum-safe; magyarul: Kvantumbiztos Secure Shell protokoll

SSO – Single Sign-On; magyarul: Egyszeri bejelentkezés

SWIFT – Society for Worldwide Interbank Financial Telecommunication; magyarul: Nemzetközi bankközi pénzügyi telekommunikációs társaság

SZTFH – Szabályozott Tevékenységek Felügyeleti Hatósága

SZTFH rendelet – 1/2025. (I. 31.) SZTFH rendelet.

TCP/IP – Transmission Control Protocol / Internet Protocol; magyarul: átviteli vezérlő protokoll / internet protokoll, internetprotokoll-készlet

TISAX – Trusted Information Security Assessment Exchange; magyarul: Megbízható Információbiztonsági Értékelési Csereplatform

TLD – Top-Level Domain ; magyarul: legfelső szintű tartománynév

TOM – Technical and Organisational Measures; magyarul: technikai és szervezési intézkedések

TQNI – Trusted Quantum Network Infrastructure; magyarul: Megbízható kvantumhálózati infrastruktúra

UAT környezet – User Acceptance Testing environment; magyarul: felhasználói elfogadási tesztkörnyezet

USA – United States of America; magyarul: Amerikai Egyesült Államok

VBA – Visual Basic for Applications; magyarul nincs fordítás, a Microsoft Office-alkalmazásokba beépített programozási nyelv

VDA – Verband der Automobilindustrie; magyarul: Német Autóipari Szövetség

VDA ISA – VDA ISA – VDA Information Security Assessment; magyarul: VDA információbiztonsági értékelés

VLAN – Virtual Local Area Network; magyarul: Virtuális helyi hálózat

Mi változott a 2.0 verzióban?

Az alábbiakban összefoglaljuk a dokumentum 2.0 verziójában bevezetett legfontosabb változásokat és kiegészítéseket. A cél, hogy az első verziót már ismerő olvasók gyorsan áttekintést kapjanak az új tartalmakról, a jelentősen bővített fejezetekről, valamint azokról a finomításokról, amelyek az érthetőséget és a gyakorlati alkalmazhatóságot javítják.

#	Fejezet	Módosítás rövid leírása
1	Bevezető	Új bevezető fejezet készült.
2	Jogszabályi háttér	A 2.1 „A NIS2 célja”, a 2.3 „A NIS2 magyarországi jogszabályi háttere”, valamint a 2.2-höz kapcsolódó EU-s szabályozások és tanúsítási keretrendszerek a NIS2 kontextusában című fejezetek kiegészítésre és bővítésre kerültek.
3	Érintett szervezetek azonosítása	A fejezet kisebb pontosításokkal és finomhangolásokkal került frissítésre.
4	Szerepkörök és felelősségek	A fejezet kisebb pontosításokkal és finomhangolásokkal került frissítésre.
5	Kockázatkezelési keretrendszer kialakítása	Az 5.1 „A kockázatelemzési keretrendszer”, az 5.3 „Kockázatkezelés”, az 5.5 „Adatvagyon és BIA (üzleti hatáselemzés) szerepe”, valamint az 5.7 „A kockázatelemzés, figyelembe véve az ellátási lánc kockázatait” fejezetek bővítésre kerültek. Emellett új fejezetként bekerült az 5.8 „Compliance scoring és a folyamatos megfelelés mérése”.
6	Azonosított EIR-ek és rendszerelemek	A 6.1 „Mit tekintünk EIR-nek?” és a 6.3 „OT rendszerek sajátosságai” fejezetek kiegészítésre kerültek, míg a 6.2 „Biztonsági osztályba sorolás irányelvei” jelentős átdolgozáson és bővítésen esett át.
7	Nemzetközi kitettség és harmonizáció	A 7.1.3 „Franciaország” és a 7.1.6 „Németország” fejezetek frissítésre kerültek, valamint új fejezetként bekerült a 7.1.9 „Dánia” és a 7.1.10 „Bulgária”.
8	A hazai követelmények gyakorlati értelmezése és alkalmazása	A 8.3 „Szerződések kiegészítési javaslatai” fejezet kiegészítésre és pontosításra került.
9	Előkészítendő dokumentumok és nyilvántartások	A fejezet több ponton kisebb pontosításokkal bővült. Kiegészítésre került a 9.2 „Információbiztonsági szabályzat (IBSZ)” és a 9.7 „Rendszerbiztonsági terv” fejezet, valamint új alfejezetként bekerült a 9.5 „Személyi biztonsággal kapcsolatos dokumentumok”.
10	Auditálási folyamat	Kiegészítésre került a 10.7 „Összeférhetetlenség” fejezet, új fejezetként bekerült a 10.8 „Audit riport értelmezése (JSON)”, valamint a 10.9 „Eddigi audittapasztalatok”.
11	Ellátási lánc biztonsága	A 11.3 „Kockázatelemzés az ellátási lánc mentén” fejezet további kiegészítésekkel bővült.
12	Használható eszközök és automatizálási lehetőségek	Új fejezetként bekerült a 12.4 „Evidenciafeldolgozás nyelvi modellekkel: lehetőségek és korlátok”.

#	Fejezet	Módosítás rövid leírása
13	Incidens-kezelés és válságkommunikáció	A fejezet kisebb pontosításokkal és strukturális finomításokkal bővült. Új tartalomként bekerült a 13.1.3 „Gyakorlati szimulációk”, a 13.1.4 „Eddigi tanulságok”, a 13.5 „Digitális Omnibusz Package”, valamint kiegészítésre került a 13.2 „CSIRT jelentési kötelezettségek”.
14	Fizikai biztonsági intézkedések	A fejezet új alfejezetekkel bővült: 14.1 „A fizikai biztonság szintjei” és 14.2 „Biztonsági intézkedések”.
15	Folyamatos fenntartás és megfelelőség-menedzsment	Kiegészítésre került a 15.2 „Intézkedési tervek kialakítása”, valamint a 15.4 „IT, biztonság és üzlet súlyozása” fejezet.
16	Kapcsolódó feladatok és megfelelések	A 16.1 „NAIH kötelezettségek” és a 16.5 „A NIS2 és a GDPR” fejezetek kiegészítésre kerültek, továbbá a fejezet több pontján kisebb pontosítások történtek.
17	Információbiztonsági architektúra a NIS2 megfelelési programban	Teljesen új fejezetként került be a Whitepaperbe.
18	Kommunikáció a menedzsmenttel	Tartalmi módosítás nem történt.
19	Megérteni és megértetni	Tartalmi módosítás nem történt.
20	„Quick Win” lista	Tartalmi módosítás nem történt.
21	Szankciók és következmények	Tartalmi módosítás nem történt.
22	Biztonsági kultúra és tudatosság	Tartalmi módosítás nem történt.
23	Digital Twin(s)	Tartalmi módosítás nem történt.
	Rövidítés-jegyzék	A rövidítésjegyzék több új fogalom és rövidítés meghatározásával bővült.

Záradék

Ez a dokumentum nonprofit szakmai együttműködés keretében készült, Creative Commons Nevezd meg – Ne add el – Ne változtasd 4.0 (CC BY-NC-ND 4.0) licenc alatt került publikálásra.

A dokumentum szabadon terjeszthető, idézhető, illetve felhasználható belső felkészüléshez, oktatáshoz, ügyfelek támogatásához, azonban a dokumentum nem értékesíthető, és nem tüntethető fel saját fejlesztésű anyagként.

Módosítása, részleteinek önálló újrakiadása, valamint bármely kereskedelmi csomagba való beépítése kizárólag a koordinátor (Dr. Váczi Dániel) írásos engedélyével történhet. a szerzők és a dokumentum eredete minden felhasználás esetén jól látható módon meg kell jelenjen.