HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 165–182.
DOI: 10.32567/hm.2024.3.10

Kis Márton[1] – Bódi Antal[2] – Számadó Róza[3]

A NIS2 hazai bevezetésének folyamata és kockázatai

The Process and Risks of Introducing NIS2 in Hungary

Absztrakt

Jelen tanulmány célja annak vizsgálata, hogy a NIS irányelv hatálya alá tartozó hazai vállalkozások és szervezetek megfeleléséhez a feltételek rendelkezésre állnak-e, illetve mi szükséges ahhoz, hogy az érintett szervezetek képesek legyenek megfelelni a NIS2 elvárásainak.

Kulcsszavak: kiberbiztonság, kockázat reziliencia, képességek, megfelelés, tudatosság, NIS2

Abstract

The purpose of this study is to investigate whether the conditions are available for the compliance of domestic enterprises and organizations covered by the NIS directive, and what is necessary for the relevant organizations to be able to meet the expectations of NIS2.

Keywords: cyber security, risk resilience, capabilities, compliance, awareness, NIS

[1] Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ; Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: mcihun@gmail.com
[2] Óbudai Egyetem Biztonságtudományi Doktori Iskola; Közlekedéstudományi Intézet, e-mail: bodi.antal@kti.hu
[3] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Közigazgatás-tudományi Doktori Iskola; Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: szamado.rozaphd.uni-obuda.hu

Bevezetés

Nemzetközi trendek, hazai pillanatkép

A kibertérben zajló események, támadások száma, összetettsége az ezredfordulót követően jelentősen megnövekedett, és jelentős károkat okozott nemcsak a magánszektor, hanem a kormányzatok számára is. Ezen események egyértelművé tették, hogy szükség van átfogó kiberbiztonsági szabályozás létrehozására az EU-ban. Az unió 2016-ban elfogadta első uniós szintű kiberbiztonsági jogszabályát, a hálózat- és információbiztonsági (NIS) irányelvet, ami alapvető lépést jelentett az uniós szintű hálózati és információs rendszerek közös információbiztonsága felé. A végrehajtás során uniós és nemzeti szinten is több kihívással szembesültek az érintettek, továbbá a kiberfenyegetések gyors fejlődése, az új technológiák gyors terjedése miatt az irányelv – jellegéből következően – nehezen tudta lekövetni a folyamatos változásokat.

A felmerülő kihívások, a folyamatosan változó digitális környezet kikényszerítette az uniós keretrendszer felülvizsgálatát. Ennek eredményeként született meg a NIS2. A frissített irányelv az uniós kiberbiztonság területén átfogó stratégiát képvisel, deklarált célja, hogy megerősítse a végrehajtási mechanizmusokat, a terület alapvető jogi pillére. Egyúttal jelentős mértékben kiterjesztette – elődje, a NIS – alanyi és tárgyi hatályát, annak érdekében, hogy a kritikus infrastruktúrák és szolgáltatások ellenálló képességét megerősítse.

A NIS2 elfogadásával törvényi megfelelésben érintett szervezetek köre megsokszorozódott, a megfelelési követelmények is több jelentős pontban változtak, így mind a már gyakorlott, mind az újonnan kötelezettek részéről kérdések sokasága merül fel.

A Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) 2024 nyarán megrendezett konferenciáján ismertették egy 2022-es, a hazai cégek digitalizációjáról szóló kutatás néhány részeredményét. E felmérés szerint minden 5. cég kereskedik online is, a bevételük 25–28%-a származik elektronikus kereskedelemből, és a cégek 70%-ának van weboldala. E kutatás keretében felmérték, hogy hogyan állnak az információbiztonsági kompetenciákkal ezek a szervezetek. A felmérés eredményéből az derült ki, hogy a válaszadók 70%-a nem alkalmaz informatikai, biztonsági szakembert. A fennmaradó cégek 30%-a esetében minden, a területen felmerülő kérdést egy ember kezel, egy embert alkalmaznak.

A különböző szervezetek felkészültségének, kompetenciáinak a mértéke kiemelkedő kockázatot hordoz. Ezt támasztja alá a EU kiberbiztonsági ügynöksége, az ENISA 2030-as előrejelzése. A top 10 kiemelkedő kockázat esetében a hosszú távú, növekvő fenyegetési kilátások közé sorolta a mesterséges intelligenciával kapcsolatos kockázatokat és a felhasználók felkészültségéhez, kompetenciáihoz kapcsolódó kockázatokat. Erre erősít rá a World Economic Fórum 2024. januári kiadású, globális kockázatokat vizsgáló jelentése. A jelentés által megjelölt első öt kockázat között kettő is technológiai jellegű, így a mesterséges intelligenciához és a kibertámadások növekedéséhez kapcsolódó rizikófaktorok. Figyelmet érdemel még a globális kockázatok közül az összekapcsolt rendszerekhez fűződő rizikó is. A hazai kkv információbiztonsági helyzetéről megjelent tanulmány több jelentős problémára, hiányosságra hívja fel a figyelmet, amit a NIS2 hatálya alá tartozó szervezeteknek szintén kiemelten kell vizsgálniuk.

A fentiekből jól látszik, hogy a folyamatosan növekvő kitettségre csak komplex, holisztikus megközelítésű beavatkozás adhat kielégítő választ. Az SZTFH kidolgozott egy 4 faktoros megoldási javaslatot. A négy faktor: a cselekvő állam, a hatékony szabályozás, a felkészült szervezetek és a tudatosítás. Az első két faktor a kereteket határozza meg a cégek részére, míg a felkészülés és a tudatosság növelése érdekében jelentős erőfeszítések megtételére van szükség. Mindezek alapján a kutatási kérdések között az alábbiak merülnek fel: Mire van szüksége a hazai vállalkozásoknak és szervezeteknek, hogy a NIS2 elvárásainak meg tudjanak felelni? Melyek a kockázatos területek, amelyekre kiemelt figyelmet kell fordítani? Meghatározhatók-e ebben a feszített ütemtervben fokozatok, prioritások? A *complient* működés elérése érdekében milyen beavatkozásokra van szükség?

Az előzetes felmérések, a különböző vizsgálatok és jelentések alapján feltételezhető, hogy a NIS2 21. cikkében megfogalmazott elvárások teljesítéséhez az érintett szervezeteknek mind kapacitásban, mind kompetenciában, mind pedig a tudatosság területén jelentős hiányosságaik vannak.

A tanulmány célja

Jelen tanulmány célja, hogy megvizsgálja a NIS2 bevezetésére kötelezett hazai érintettek felkészültségét, és választ keressen arra a kérdésre, hogy milyen feltételek teljesülése mentén lehetséges a NIS2-megfelelés, a szervezetek napi gyakorlatába ültetése és fenntartható működtetése.

Alkalmazott módszerek

A szabályozási környezet áttekintése, a jogi dokumentumok elemzése után a kockázatelemzés módszertanával vizsgáljuk a kutatási kérdést. A választás indoka, hogy jelenleg a sikeres alkalmazkodás a cél, ezért szükséges elemezni a felmerülő tényezőket, hogy a megelőzéshez szükséges beavatkozások megalapozottak legyenek.

A célkitűzésben megfogalmazott kérdés megválaszolásához a következő 4 lépéses módszertanon keresztül tervezünk eljutni:

1) Kockázatok leltára

Számba kell venni azokat a lehetséges kockázatokat, amelyek a NIS2 bevezetése során a szervezeteknél külső vagy belső kockázatként felmerülhetnek.

2) Kockázati térkép

Az azonosított kockázatokat a bekövetkezésük hatása és valószínűsége alapján be kell sorolni.

3) Kockázati mátrix

A besorolt kockázatok súlyossága alapján beavatkozási protokoll hozzárendelése.

4) Skillmátrix

A NIS2 bevezetési folyamatában azonosított szervezeteknél a NIS2 bevezetéséhez szükséges skillek azonosítása és besorolása.

A módszertan logikai sorrendjét az 1-es ábra szemlélteti.

1. ábra: Módszerek logikai sorrendje
Forrás: a szerző szerkesztése

A módszertan mind a négy lépésének inputjait egyrészt a limitáltan rendelkezésre álló nemzetközi szakirodalom elemzésével igyekeztünk végrehajtani, másrészt nagy számú háttérbeszélgetést és strukturált interjút folytattunk kiemelt iparági és hatósági szereplők vezetőivel és kiberbiztonságért felelős szakembereivel.

Szabályozási környezet

EU-szintű szabályozás

A belga CERT vezetője találóan foglalta össze az eredeti 2016-os NIS és a 2023-ban elfogadott, 2024 során minden EU-tagállamban fokozatosan életbe lépő NIS2-szabályozás közötti különbséget:

„💪NIS2 = NIS 1 on Steroids👇”[4]

A 2010-es évek elején az uniós törvényhozók rengeteg olyan faktorral nem számolhattak – a digitalizáció rakétasebességű térnyerése, a világméretű pandémia katalizátorhatása, a kiberfenyegetettség ugrásszerű növekedése, a háborús konfliktusok kiberoldali hatása –, ami miatt a viszonylag friss EU-szintű szabályozás felülvizsgálata és a részletesebb, szigorúbb szabályozás bevezetése elkerülhetetlenné vált.

Az EU azt várja a módosított előírásoktól, hogy a jelentősen szélesebb körben bevont szervezetek és vállalkozások összehangolt megfelelése mentén nemcsak az egyedi szervezetek, hanem az egész EU védettsége és rezilienciája lényegesen megemelkedik a korábbi szinthez képest, és a megnövekedett felhasználói tömegek alapvető kibertudatossága is hozzájárul a nagyobb EU-digitális biztonsághoz.[5]

Az eredeti NIS-irányelv – az első uniós kiberbiztonsági jogszabály – volt az első olyan szabályozó eszköz, amelynek célja az EU IT-rendszereinek kiberbiztonsági kockázatokkal szembeni ellenálló képességének javítása. A bizottság felismerte, hogy jelentős eredményei ellenére a NIS-irányelv bizonyos korlátokat mutatott. A társadalom digitális átalakulása, amelyet a Covid–19-válság felerősített, kiterjesztette a fenyegetettséget. Új kihívások jelentek meg, amelyek adaptált és innovatív válaszokat igényeltek.

Mindezek orvoslására a Bizottság a korábbi NIS-irányelv (amire ma már leggyakrabban a szakirodalomban NIS1-ként hivatkoznak) kiterjesztését javasolta: több ágazat és entitás bevonása a hatályba; harmonizálni az ezen entitások azonosítására

[4] Jean-Luc Peeters, head of CERT.be at Centre for Cybersecurity Belgium.
[5] Európai Bizottság 2023a.

vonatkozó szabályokat (a méretkorlát automatikus és egységes kritériumként történő alkalmazásával); a biztonsági követelmények kiterjesztése; a vezetők és igazgatóságok fokozottabb bevonása és felelősségvállalása; a szankciók, valamint az illetékes hatóságok felügyeleti jogkörének harmonizálása és megerősítése; az incidensek bejelentési kötelezettségeinek tisztázása (például ütemterv, feltüntetendő információ); valamint az ellátási lánc biztonságának megerősítése mind az egyes entitásokon belül, mind pedig európai szinten.

A Bizottság azt is javasolta, hogy erősítsék meg az európai együttműködést a NIS Együttműködési Csoport és a CSIRT-hálózat megbízatásának megerősítésével, valamint a nagyszabású, határokon átnyúló kiberbiztonsági válságok kezelésére szolgáló új platform hivatalos elismerésével. Javasolt továbbá egy európai keret létrehozása a sérülékenység koordinált közzétételére.[6]

A NIS-irányelv hatásának elemzése és hiányosságainak azonosítása érdekében a Bizottság kiterjedt konzultációt folytatott az érdekelt felekkel. A következő főbb problémákat azonosították:

- az EU-ban működő vállalkozások kiberellenállásának elégtelen szintje;
- a tagállamok és az ágazatok közötti nem megfelelő együttműködés;
- a fő fenyegetések és kihívások nem kielégítő közös értelmezése a tagállamok között;
- a közös válasz és válságreakció hiánya, a büntető szankciók elégtelen volta.

A megállapítások eredményeként, valamint a felgyorsult digitalizáció és a külső és belső növekvő fenyegetésekre való reagálás érdekében a Bizottság 2020 decemberében egy felülvizsgált, komplexebb szabályrendszert javasolt, amelynek célja a kiberreziliencia szintjének erősítése az unióban. A jogalkotók 2022. május 13-án politikai megállapodásra jutottak, és 2022. november végén hivatalosan is elfogadták az új irányelvet.[7]

A NIS és a NIS2 közötti változást a 2. ábra részletesen szemlélteti.

A NIS2 irányelv jogi intézkedéseket ír elő a kiberbiztonság általános szintjének növelésére az EU-ban, annak érdekében, hogy hozzájáruljon a belső piac általános működéséhez. A NIS1 irányelv három fő pillérre épült:

1. A hálózati és információs rendszerek biztonságára vonatkozó NIS1 stratégiára építve a tagállamok magas szintű felkészültségének elérése érdekében a NIS2 irányelv előírta a tagállamok számára, hogy fogadjanak el nemzeti kiberbiztonsági stratégiát. A tagállamoknak ki kellett jelölniük a kockázatok és incidensek kezeléséért felelős nemzeti számítógépes biztonsági eseményekre reagáló csoportokat (CSIRT), egy illetékes nemzeti kiberbiztonsági hatóságot és egyetlen kapcsolattartó pontot (SPOC). Az SPOC-nak kapcsolattartó funkciót kell ellátnia, hogy biztosítsa a határokon átnyúló együttműködést a tagállami hatóságok és a többi tagállam illetékes hatóságai között, és adott esetben a Bizottsággal és az ENISA-val, valamint biztosítsa az ágazatokon átnyúló együttműködést a többi illetékes hatósággal.

2. A NIS2 irányelv folytatja a NIS1-keretet is, amely létrehozza a NIS-együttműködési csoportot a tagállamok közötti stratégiai együttműködés és információcsere

[6] Byttebier 2022.
[7] Európai Bizottság 2023b.

támogatására és elősegítésére, valamint a CSIRT-hálózatot, amely elősegíti a nemzeti CSIRT-ek közötti gyors és hatékony operatív együttműködést.

3. A NIS1 irányelv biztosította, hogy a kiberbiztonsági intézkedéseket hét olyan ágazatban hozzák meg, amelyek létfontosságúak gazdaságunk és társadalmunk számára, és amelyek nagymértékben támaszkodnak az IKT-ra, mint a közigazgatás, az energia, a közlekedés, a bankszektor, a pénzügyi piaci infrastruktúra, az ivóvíz, az egészségügy és a digitális infrastruktúra.

2. ábra: NIS2 Adatlap – #DigitalEU
Forrás: a szerző fordítása és szerkesztése az Európai Bizottság 2023a, 2023b alapján

A tagállamok által ezekben az ágazatokban alapvető szolgáltatások üzemeltetőiként azonosított állami és magánjogi szervezeteknek kiberbiztonsági kockázatértékelést kell végezniük, és megfelelő és arányos biztonsági intézkedéseket kell bevezetniük. A súlyos következménnyel járó eseményekről értesíteniük kell az illetékes hatóságokat.

A NIS2 irányelv jelentősen kibővíti az ágazatok körét (például államigazgatás, gyártási tevékenységek, szennyvíz- és hulladékkezelés), és méretküszöböt vezet be annak meghatározására, hogy mely jogalanyok tartoznak az irányelv hatálya alá, és melyek kötelesek jelenteni a jelentős kiberbiztonsági incidenseket az illetékes nemzeti hatóságoknak.[8]

[8] Európai Bizottság 2023b.

A kiberbiztonsági szabályozást az EU-ban régóta részlegesen hajtják végre, ami széttagolt szabályozási környezetet eredményez. A közelmúltbeli fejlemények arra késztették az EU-t, hogy felülvizsgálja megközelítését, mert az eredeti szabályozás nem eredményezte uniószerte a tervezett magas szintű kiber-ellenállóképességet. E tekintetben a NIS 2.0 irányelvre vonatkozó közelmúltban elfogadott szabályozás és a kiberrezisztenciáról szóló törvényjavaslat rávilágít arra, hogy az EU miként igyekszik összehangolni a jogszabályokat, és csökkenteni a különböző, gyakran ágazati szabályozási megközelítéseket a kiberbiztonság terén, ugyanakkor kiterjesztik a szabályozást a magas szintű kiberbiztonság elérése érdekében az egész EU-ban. A kiberrezisztenciáról szóló törvény további kiegészítést nyújt a NIS 2.0 irányelvhez a meglévő szabályozási hiányosságok megszüntetése érdekében, amire ebben a dokumentumban nem térünk ki.[9]

A NIS2 magyar vonatkozásai

Rendszerszintű szereplők

A hazai NIS2 hatósági környezetét alapvetően a *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről* határozza meg, illetve a tanúsításról szóló kiegészítő SZTFH rendelet, *10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról.*

Ennek értelmében a hazai NIS2 szabályozás központi kijelölt hatósági szereplője a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH), és fő feladata a NIS2 hatálya alá tartozó szervezetek kiberbiztonsági tanúsításának nyilvántartása és ellenőrzése, és hogy a hazai kiberbiztonsági megfelelésről rendszeresen tájékoztassa a Bizottságot.

A cikk írásának időpontjában a törvény végrehajtási rendeletét még nem hirdették ki, de a társadalmi egyeztetésre bocsátott változata ismert: „A Miniszterelnöki Kabinetirodát vezető miniszter MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről (TERVEZET)". Ezen végrehajtási rendelet végleges, kihirdetett verzióját az összes érintett szervezet várja, hogy az elvárt törvényi megfelelés pontos hatósági részletei megismerhetők legyenek, és a felkészülés, illetve annak auditálása és megfelelési értékelése elfogadható legyen.

A szabályozás alá vont szervezetek köre két lépésben meghatározott. A következő fejezetben felsorolt mérföldkövek és határidők mentén a törvény hatálya alá tartozást a szervezeteknek önazonosítás után kell meghatározniuk a törvényben szereplő kritériumrendszer figyelembevételével. Az elsődleges kötelezettség az érintett szervezeteknek az SZTFH-nál történő elektronikus regisztrációja 2024. 06. 30-ig.

A végrehajtási rendelet hiányában a szabályozás alá vont szereplők többféle stratégia mentén végzik a felkészülésüket. Van, aki kivár a pontos részletszabályok megérkezéséig, mások proaktívan a jelenlegi ismeretek alapján igyekeznek előre dolgozni és a megfelelésre felkészülni.

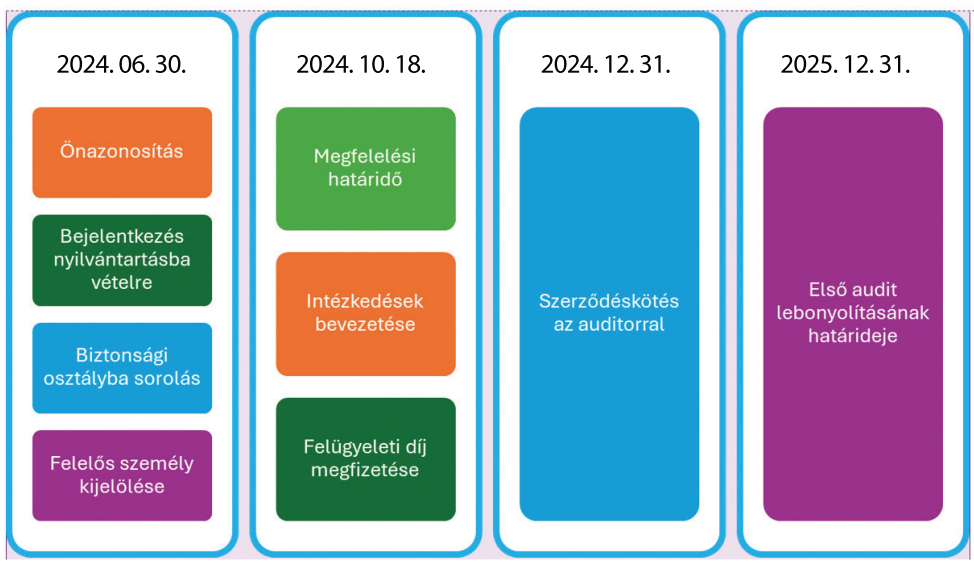
[9] Schmitz-Berndt–Cole 2023.

A felkészítő szereplőkre vonatkozóan nincs törvényi kijelölés, a szervezetek akár saját hatáskörben is felkészülhetnek a NIS2-megfelelésre. Mivel az érintett szereplők nagy részének nincs megfelelő saját belső szaktudása, illetve HR-kapacitása, piaci alapon igény keletkezett a felkészítő tanácsadó tevékenységre. A versenyszféra cégei különböző szolgáltatáscsomagokat kínálnak az érintett cégek részére (komplex felkészítés, biztonsági osztályba sorolás, szabályzatok elkészítése, gap-analízis, előaudit stb.). Kiemelt kockázatként jelentkezik, hogy a felkészítő szervezet munkatársai nagyon szenzitív belső információkhoz férhetnek hozzá, így a kiválasztásnál a megfelelő személyi garanciákat be kell építeni a folyamatba.

A kötelező audit lebonyolítására alkalmas cégek köre valószínűleg nagyon limitált lesz a szigorú megfelelőségi kritériumok mentén, azonban a cikk írásának idején még sem a végleges pontos kritériumrendszer, sem az audit lebonyolítására képes cégek teljes körű hivatalos jegyzéke nem elérhető. A felkészítő szervezeteknél jelentkező személyi garancia kockázata itt sem zárható ki, így kiemelten fontos a megfelelő személyi garanciák beépítése a folyamatba.

NIS2-megfelelés kötelező lépései szervezeti oldalon

Az érintett szervezetek NIS2-megfeleléshez szükséges tevékenységeinek köre meglehetősen komplex. A lépések és határidők a *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről* 30. §-a alapján a következők:



3. ábra: NIS2-megfelelés törvényi határidői
Forrás: a szerző szerkesztése

A szervezetek oldalán jelentkező kockázatok körét a következő pontban részletesen is feldolgozzuk, azonban általánosságban is megállapítható, hogy az alábbi lehetséges általános problémák, kockázatok merülhetnek fel a 4 kiemelt határidő teljesítése körül:

- Végrehajtási rendelet meglehetősen későn jött ki a határidők teljesítéséhez.
- 2013. évi L. törvény vs. NIS2-előírások megfeleltetése (szabályzatok, kockázatértékelés, biztonsági osztályba sorolás) időt és szakértelmet igényel, amelyek korlátozottan állnak rendelkezésre.
- Kritikusnak minősített kockázatokhoz kapcsolódó korrekciós tevékenységek erőforrás-szükségletének rendelkezésre állása (HR és pénzügyi egyaránt).
- A korrekciós tényezők miatti szükséges fejlesztések és eszközbeszerzések fedezete és közbeszerzési folyamatainak időigénye.
- Az előírt – teljes munkavállalói létszámot érintő – biztonságtudatossági oktatások megszervezése és lebonyolítása (a napi üzletmenetet nem akadályozva).
- Olyan szervezetekre is kiterjed a NIS2-kötelezettség, ahol korábban ez a feladat még nem merült fel, ezért nagyon alacsony a szervezet kibertudatossága, a menedzsment nem készült fel a feladatra, nincs tapasztalat a valós kockázatokról.

Szervezeti érintettek a bevezetés során

A megfelelésre kötelezett intézmények szervezeti struktúrájának megfelelően – függetlenül attól, hogy a szervezet mely ágazatban tevékenykedik – a NIS2-megfeleléshez szükséges feladatok több szervezeti egységnél és a hierarchia több szintjén jelentkeznek. Mivel a megfelelés komplex intézkedéseket igényel, ami a teljes szervezet tekintetében tartalmaz feladatokat, elsődleges fontosságú kérdés, hogy a menedzsment értse a kérdés jelentőségét, támogassa a végrehajtásból fakadó feladatokat, és biztosítsa a szükséges (HR- és pénzügyi) erőforrásokat. Jó megoldás lehet a NIS2-bevezetést projektformában, előre lefektetett feltételek mentén végrehajtani, de amennyiben ez nem lehetséges, akkor is egyértelmű felelősöket és erőforrást kell kijelölni a 3-as ábrában felsorolt törvényi határidőkhöz kapcsolódó feladatok végrehajtásához. Az 1-es táblázat a legfontosabb szereplőket és azok kulcscélfüggvényét veszi számba a NIS2-bevezetés problémakörére koncentrálva.

1. táblázat: Az érintettek érdekei, megoldási irányok

Érintettek	**Érdekek, motiváció, kooperáció**
IT-szervezeti egység, IT-biztonsági felelős	A rendszerek gazdájaként a végrehajtás ide koncentrálódik, a fő motiváció a hibamentes végrehajtás. Sokszor kooperációs, kommunikációs problémák vannak a többi szervezeti egységgel. Gyakori az általános, illetve a specifikus információbiztonsági tudással rendelkező HR-kapacitás hiánya. Gyakori hiba, hogy az IT-biztonsági felelős az IT-üzemeltetés alá kerül szervezeti beosztásra, így gyakran nem jut el a menedzsmenthez az információ a kötelezettségből adódó feladatok méretéről és a nem megfelelés esetén felmerülő valós kockázatról.
Üzemeltetés	A fő motiváció a zökkenőmentes működés biztosítása. Szükséges annak a tudatosítása, hogy a NIS2-megfelelés része ennek. Konfliktus van a napi üzemeltetési gyakorlat és a kapcsolódó üzleti elvárás, illetve a NIS2-előírások betartása, betartatása, betarthatósága és ellenőrizhetősége között. A konfliktus feloldása szükséges, aminek a fentieken túl a kooperáció lehet az eszköze.
Adminisztráció	Az adminisztráció célja a NIS2-megfelelés lehető legkisebb költség (HR-többletigény, lehetséges többlet-infrastrukturális beruházások, felkészítés, audit tanácsadói költsége, munkavállalók oktatásának költsége, oktatás miatti munkaidő-kiesés költsége) melletti megvalósítása. Jellemző a legkisebb árajánlat kiválasztása a külső tanácsadóknál, amely komoly szakmai kockázattal jár együtt, mivel nincs a felkészítő tanácsadókra egységes szakmai elvárás, végzettség vagy szakmai tapasztalat.
Menedzsment	Sok esetben gyakorlatilag feloldhatatlan konfliktust eredményez a költséggazdálkodás miatti nyomás és a törvényi megfelelési kényszer közötti ellentmondás feloldása. A NIS2-bevezetést kiváltó valós megnövekedett kiberkitettség kockázatának felismerése és az *ownership* felvállalása. A szigorúbb szabályok miatti szervezeti ellenállás csak a menedzsment teljes elkötelezettsége mellett kezelhető, amihez szükséges a kockázatokból adódó hátrány, veszély, veszteség megismerése, felismerése.
Munkavállalók	Digitális higiénia és tudatosság alacsony, a napi gyakorlat megváltoztatása szükséges, az új, szigorúbb szabályok óhatatlanul kényelmetlenebbé és bonyolultabbá teszik a napi megszokott munkát, ami feszültséget okoz. A kikényszerítés sem egyszerű, a hosszú távú szemléletváltás és – a képzéssel, szervezetfejlesztéssel támogatott – vállalati kultúrába épülés a megoldás.

Forrás: a szerző szerkesztése

Eredmények

Probléma-/kockázati térkép

A 2-es táblázat alapján jól követhető, hogy még az egy szervezetben, alapvetően közös célok érdekében dolgozó érintetteknek is gyakran erősen eltérnek az érdekeik és motivációjuk; természetesen igaz lesz ez az állítás a kiberbiztonsági megfeleléshez szükséges feladatok végrehajtására is.

A következőkben számba vesszük az ebből az eltérő nézőpontból és érdekeltségből fakadó kockázatok listáját. A lista a dinamikusan változó környezet hatására nyilvánvalóan dinamikusan változik, de igyekeztünk a fő kockázatokat teljeskörűen számba venni.

2. táblázat: Kockázatok listája

#	Kockázat
A	Alacsony szintű kibertudatosság
B	Felhasználók szabálykövetése alacsony
C	Egységes NIS2-bevezetési módszertan hiánya
D	Nem megfelelő IT-szabályozottság
E	Hiányzó IT-kockázatmenedzsment
F	Az üzemeltetés kockázatos
G	Nincs vagy nem megfelelő a DRP
H	Nincs vagy nem megfelelő a BCP
I	A NIS2-megfelelés bevezetésére és fenntartására nincs tapasztalat és egységes módszertan
J	Késik a Kibertan. tv. végrehajtási rendelete
K	A szervezet IT-rendszerének extrém kitettségei
L	A menedzsment elköteleződésének hiánya
M	Felkészületlen vagy csalárd „felkészítők” – NIS2-bűnözők megjelenhetnek

Forrás: a szerző szerkesztése

A felsorolt kockázatok áttekintésével felismerhető, hogy bár van néhány, a szervezet hatáskörén kívül eső kockázat (C, J, M), mégis a kockázatok többsége vagy a szervezet menedzsmentjéhez kötődik (D, E, G, H, K, L), vagy az egyedi felhasználók magatartásából következik (B, F).

Az 1-es számú mellékletben a felsorolt kockázatok értelmezését követően a bekövetkezés valószínűségét és annak szervezetre gyakorolt hatását értékeltük.

A 3-as táblázatban kockázati mátrixba rendezve látható ezeknek a lehetséges eseményeknek a vizuális megjelenítése. A táblázat színkódjai megmutatják a szervezet incidenshez kapcsolódó attitűdjét és az ebből következő beavatkozás szintjét és időtávját.

Az ábrázolás egyértelműen megmutatja, hogy a lehetséges kockázatok túlnyomó többsége azonnali beavatkozást igényel a szervezetek részéről.

3. táblázat: Kockázati mátrix

Valószínűség (1–5)	Következmény (1–5)				
	Jelentéktelen	Mérsékelt	Közepes	Súlyos	Kritikus
Elhanyagolható					
Alacsony					
Közepes			C	J	H, L, M
Valószínű				D	B, F, G, K
Nagyon valószínű			I		A, E

Kockázati szintek	Tolerancia	Akció
Elhanyagolható	**elfogadható**	**Nincs, elegendő kontroll**
Alacsony	**elfogadható**	**Nincs, elegendő kontroll**
Normál	**elfogadható**	**További szorosabb kontroll**
Magas	**nem elfogadható**	**Kockázatkezelési beavatkozás monitorozott határidővel**
Kritikus	**nem elfogadható**	**Azonnali kockázati beavatkozás**

Forrás: a szerző szerkesztése

Skillmátrix

Kiemelt figyelmet érdemel, hogy a sikeres NIS2-bevezetéshez, és a megfelelés folyamatos fenntartásához minimum két fő tényező együttes bekövetkezésére van szükség:

- Az előző pontban részletezett kockázatok kezeléséhez szükséges erőforrások (HR-kapacitás és pénzügyi fedezet) gyakorlatilag azonnali és párhuzamos rendelkezésre állása.
- A törvényi előírások és kötelezettségek pontos ismerete és a végrehajtáshoz szükséges skillek szervezeti jelenléte a NIS2-ökoszisztéma minden érintett szervezetét figyelembe véve.

A NIS2-megfelelés érdekében szükséges fejlesztések, beavatkozások megítélésének érdekében alkottunk meg egy többdimenziós mátrixot a rendszer szereplőivel, a szükséges készségekkel, képességekkel, szakismeretekkel, a meglévő tudásszintekkel és a hozzájuk tartozó tevékenységgel a megfelelés fenntartásához.

A rendszer szereplői: szabályozó, törvényhozó; ágazati irányító minisztérium; ellenőrző szervezet; ágazati középirányító szervezet; felkészítő szervezet; auditor; oktató szervezet; szabályozás alá vont szervezet.

Az azonosított, a NIS2-bevezetés lebonyolításához szükséges készségek, szakismeretek az alábbiak:

- NIS2-előírások ismerete;
- vonatkozó hazai szabályzók ismerete;
- szükséges szabályzatok struktúrája és elemei;
- IT-infrastruktúra rendszerelemeinek ismerete;
- IT-alkalmazási szint ismerete;
- ágazati specifikumok ismerete;
- jelenlegi rendszer állapotismerete;
- jelenlegi rendszerkorlátok ismerete (forrás, HR stb.);
- rendszerszereplők oktatásának képessége;
- rendszerszereplők ellenőrzésének képessége;
- szervezeti szintű IT-biztonsági tudatosság;
- támogató szervezeti kultúra;
- felelős egyéni szintű viselkedés, szabálykövetés.

Az is fontos információ, hogy az adott készség mely szereplőnél milyen tudásismereti mélységben, illetve milyen gyakorlati felhasználási képességgel párosulva kell hogy megjelenjen. A skillmátrixban ezt a dimenziót színekkel azonosítottuk a beavatkozási irányok megjelölésével.

A 4. táblázatot áttekintve könnyen felismerhető, hogy az elvárások, törvényi kötelezettségek oktatására minimum 3 szinten van szükség:

- A kötelezett szervezetek munkavállalóinak érzékenyítő oktatásokat kell tartani, amelyhez a megfelelő tananyagot is létre kell hozni.
- A majdani oktatásokat végző szervezetek, csakúgy, mint a felkészítő tanácsadók és auditorcégek részére is központi, egységes képzéseket kell tartani.
- A végrehajtásban és a kötelezettek felügyeletében, irányításában érintett szervezetek részére is oktatást kell szervezni az irányelv részletes megismerése és feladataik gyakorlati részleteit érintően.

Ez a 3 szintű feladat teljeskörűen felkészült oktató szervezetet, gárdát és a 3 szintnek megfelelően kifejlesztett oktatási anyagokat és számonkérési keretrendszert feltételez.

A skillmátrix áttekintésével vizuálisan is gyorsan átlátható, hogy az egyik azonnali feladat annak biztosítása, hogy a szabályozásban és a végrehajtásban érintett (felkészítő, oktató és auditor-) intézmények és cégek minél hamarabb rendelkezzenek a különböző ágazati specifikumokkal (például egészségügy esetén a 7/24 működés és a folyamatos ellátási kötelezettségből fakadó eltérő napi gyakorlat) és az ehhez kapcsolódó IT-infrastruktúra és HR-támogató személyzet egyedi vonásaival.

A mátrix vizsgálata – a későbbiek során – segítséget nyújthat egy komplex, rugalmas és szinergikusan működő többszintű képzési rendszer kialakításához.

4. táblázat: Skillmátrix

	Szükséges skillek és rendelkezésre állásuk												
Érintettek/ rendszer-szereplők	NIS2-előírások ismerete	Vonatkozó hazai szabályzók ismerete	Szükséges szabályzatok struktúrája és elemei	IT-infrastruktúra rendszerelemeinek ismerete	IT-alkalmazási szint ismerete	Ágazati specifikumok ismerete	Jelenlegi rendszerállapot ismerete	Jelenlegi rendszerkorlátok ismerete (forrás, HR stb.)	Rendszerszereplők oktatásának képessége	Rendszerszereplők ellenőrzésének képessége	Szervezeti szintű IT-biztonsági tudatosság	Támogató szervezeti kultúra	Felelős egyéni szintű viselkedés, szabálykövetés
Szabályozó, törvényhozó													
Ágazati irányító minisztérium													
Ellenőrző szervezet													
Ágazati közép-irányító szervezet													
Felkészítő szervezet													
Auditor													
Oktató szervezet													
Szabályozás alá vont szervezet													

Tudásszint	**Szükséges tevékenység, kompetencia állapota**
Hiányos ismeretek	oktatás szükséges
Felhasználói/végrehajtó szintű ismeret	képes a szabályozási utasítást végrehajtani
Rendszerszintű ismeret	képes a végrehajtás szakszerűségét ellenőrizni
Mester-/oktatói szintű ismeret	képes a rendszer többi szereplőjét oktatni, instruálni

Forrás: a szerző szerkesztése

Értékelés, további vizsgálandó területek

A kockázatok és a szükséges és hiányzó skillek vizsgálatát követően számos lehetséges és szükséges feltétel megfogalmazható, amelyek ahhoz kellenek, hogy a NIS2-megfelelés ne csak egyszeri, kampányszerű tevékenység legyen, hanem fenntartható, a szervezetek napi gyakorlatába és szervezeti kultúrájába szervesen beépülő, napirutin-szerű tevékenységek sorozatává váljon.

Amíg az EU és a hazai törvényhozói szándék egyértelmű – a megnövekedett kiberkockázatok megelőzésére és kezelésére hozott magasabb szintű intézkedések

bevezetése –, addig a kötelezett szervezetek szintjén ez a szándék elsődlegesen megnövekedett költségeket, komplexebb folyamatokat és a jelenlegi HR-kapacitás további terhelése mellett még extra HR szükségletet is teremt. Összességében a NIS2-megfelelés mindenképpen jelentős anyagi és HR-terhet ró a szervezetekre, amelyek fedezetét a piaci cégek kénytelenek kigazdálkodni, azonban az állami fenntartású szervezetek esetében a szükséges kiadások fedezetéről az államnak kell gondoskodni.

A részletszabályok hivatalos ismeretének hiányában jelen pillanatban a kötelezettek nagyrészt önállóan és különböző intenzitással foglalkoznak a feladattal. A részszabályokon túl szükség lenne az ágazati középirányítók részéről olyan egységes módszertanok kidolgozására és közzétételére, amelyek mentén a hasonló tevékenységet folytató szervezetek egységes keretek között tudhatnak felkészülni a megfelelésre, és ezáltal a fenntartható megfelelés is könnyebben elérhető lehet.

Mindezek figyelembevételével a specifikus ajánlások megtételéhez még sok változó ismerete és feldolgozása lenne szükséges, azonban már most látható néhány általánosan levonható következtetés:

- szervezeti kultúraváltás kell majdnem minden érintett szintjén és jelentős edukáció szükséges:
  - a hazai digitális éberség és tudatosság egyéni és szervezeti szinten is komoly fejlesztésre szorul. Minden szereplőnek el kell fogadnia, hogy a digitalizáció nem visszafordítható folyamat, és a digitális, online világban más típusú és nagyobb odafigyelést igénylő veszélyek leselkednek a napi használat során. Ennek a tudásnak a megszerzése csakis szervezett oktatás mentén valósítható meg, és utána nap mint nap szükséges az új folyamatok kikényszerítése, amíg az a megszokott rutin részévé nem válik;
- a tudatosság és egyéni felelősségvállalás kérdése kritikus:
  - az előző pont kiterjesztéseként szükséges a szemléletváltás a szervezeti és egyéni felelősség kérdésében is. Tudatosulnia kell annak a ténynek, hogy a legkisebb felhasználói figyelmetlenség is (például adathalász-e-mailre kattintás) nagyon komoly károkat okozhat a szervezet számára. Az oktatás ezen a szinten is kritikus, az egyénnek tisztában kell lennie cselekedetei hatásával és felelősségével a nem várt incidensek hatására vonatkozóan;
- vezetői/fenntartói/szabályozói támogatás mellett lehetséges csak a fenntartható NIS2-bevezetés:
  - az egyénektől elvárt éberség és felelősségvállalás folyamatos fenntartása nem képzelhető el a szervezet közvetlen vezetői és menedzsmenttámogatása nélkül, de szükséges a folyamatos visszacsatolás és kommunikáció a szabályozói szinten is (a tájékoztatásnak, oktatások tematikájának reagálnia kell a várhatóan fejlődő felhasználói tudásszintre, és annak megfelelő további magasabb szintű információk rendelkezésre bocsátása válik majd szükségessé;
- standard módszertanok kellenek, jógyakorlatok bemutatása, érzékenyítő események (például HunEx, hackathonok stb.):
  - az oktatásokon túl szükség lesz olyan egyéb platformok bevonására, ahol a szervezetek a hétköznapokban tudnak adott felmerülő probléma esetén tájékozódni, információt szerezni. A jógyakorlatokat, módszertanokat közzétevő online felületek mellett érdemes lehet olyan személyes

eseményeket is szervezni, ahol a napi problémákat, tapasztalatokat tudják a szervezetek képviselői megosztani és megbeszélni. A valós problémákra reflektáló szimulációs és problémamegoldó események szintén jobb hatásfokú eredményeket hoznak a közös alkotás és az eltérő skillek együttes felhasználása miatt;

- a digitalizációt finomhangolni kell:
  - az elvárt szabálykövetés napi fenntartásában a felhasználói élmény kritikus. A digitális megoldás nem lehet bonyolultabb, időigényesebb, mint a régi analóg, mert akkor a felhasználó kiskapukat fog keresni, a szabályszegés kockázata meg fog nőni;
- automatizmusokat kell keresni, ami mentesíti, de legalább támogatja a felhasználókat, IT-üzemeltetőket a kockázatok elkerülésében:
  - az előző pont folyományaként szükséges lehet olyan lokális vagy központi egységes NIS2-megfeleléshez kapcsolódó támogató intézkedéseket hozni, ami egyszerűbbé teszi a szervezetek és az egyéni felhasználók számára a napi munkavégzés során a digitális szabályok észszerű betartását.

Összefoglalásként kijelenthető, hogy a NIS2 megszületése és több dimenziójában is kiterjesztett hatálya a megnövekedett kiberkockázatok miatt szükséges és elkerülhetetlen volt.

A jelen helyzet hazai vizsgálata több limitáló tényező miatt is csak részleges következtetések levonását tette lehetővé.

A megvalósítás tapasztalatainak ismerete nélkül a jelenleg látható kockázatok és a bevezetéshez szükséges készségek elemzését követően csak általános, de mégis alapvetően releváns következtetések levonása volt lehetséges.

A hipotéziseket igazoltuk, és tézisként kijelenthető, hogy a NIS2 hatálya alá tartozó szervezeteknek mind kapacitás-, mind kompetenciafejlesztésre szükségük van.

Kimondható, hogy a NIS2 fenntartható megfelelés napi gyakorlatba való rögzülésének alapvető kritériuma a rendszer több szintjén minél hamarabb megtervezett és megvalósított oktatások rendszere. Ennek hiányában sem a kötelezett szervezetek és azok felhasználói, sem a felkészítésüket és ellenőrzésüket a jövőben ellátni hivatott szereplők nem lesznek képesek a feladatukat megfelelően elvégezni.

Egyúttal az is leszögezhető, hogy a NIS2 hatálya alá tartozó szervezetek egy proaktív, stratégiai szinten megfogalmazott cselekvési tervvel eleget tudnak tenni az irányelv elvárásainak, és egyúttal kialakíthatják a saját maguk biztonságos és rugalmas működési kereteit.

A kutatás következő fázisában tovább lehet és kell majd vizsgálni, hogy a NIS2 kötelező megfelelése lehetőség az érdemi változásra, vagy csak egy következő kipipálandó feladat (mint az ISO vagy a GDPR sok szervezetnél). Létrejön-e a valós szervezeti felismerés, hogy a kiberkockázatok jelentősen növekedtek az elmúlt években, és ezek új megoldásokat, válaszokat igényelnek? Léteznek-e olyan módszertanok, amik támogathatják ezt a felismerési, tudatosságnövelési folyamatot?

Felhasznált irodalom

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

Bor Olivér – Bencsik Balázs (2024): Ki és hogyan készüljön fel a NIS2-re? *SZTFH konferencia.* Online: www.youtube.com/watch?v=IAsXC_qFNNc

Byttebier, Pieter (2022): NIS-2: Where are you? *Centre for Cybersecurity Belgium,* 2022. április 30. Online: https://ccb.belgium.be/en/news/nis-2-where-are-you

ENISA (2024): *Foresight Cybersecurity Threats For 2030. Executive Summary.* Online: www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary

Európai Bizottság (2023a): *NIS2 Directive*. Online: https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive

Európai Bizottság (2023b): *NIS2 FAQS*. Online: https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás. *Hadmérnök,* 12(3), 198–209. Online: https://real.mtak.hu/64731/1/1.Farkas_Hadm%C3%A9rn%C3%B6k2017.pdf

Mike Nimród – Krén Enikő – Kecskeméti Tamás (2023): Farkasbiztos téglaház? A KKV-k információbiztonsága Magyarországon. *Vezetéstudomány,* 54(9), 44–57. Online: https://doi.org/10.14267/VEZTUD.2023.09.04

Schmitz-Berndt, Sandra – Cole, Mark (2023): Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act. *Applied Cybersecurity and Internet Governance,* 1(1), 1–17. Online: https://doi.org/10.5604/01.3001.0016.1323

Vandezande, Niels (2024): Cybersecurity in the EU: How the NIS2-directive Stacks up Against Its Predecessor. *Computer Law and Security Review*. Online: https://doi.org/10.2139/ssrn.4383118

World Economic Forum (2024): *Global Risks Report 2024*. 19th Edition: Online: www.weforum.org/publications/global-risks-report-2024/

Zágon Csaba – Gecsei Márton (2021): Kockázatelemzés a gyakorlatban: cigaretta a repülőtéren. In *Tradíció, tudomány, minőség. 30 éves a Vám- és Pénzügyőri Tanszék.* Tanulmánykötet. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, 129–142. Online: http://doi.org/10.37372/mrttvpt.2021.2.7

1.sz. melléklet – kockázati térkép

Azonosító	Kockázat	Kockázat leírása	Esemény bekövetkezésének valószínűsége (1–5)	Esemény hatása (1–5)	Kockázati érték
A	Alacsony szintű kibertudatosság	A felhasználók kiberhigiénia-szintje alacsony. A hétköznapi gyakorlatban sok NIS2-ben elfogadhatatlan elem rögzült.	5	5	25
B	Felhasználók szabálykövetése alacsony	Az ellátás érdekét előtérbe helyezve kockázatos tevékenységet folytatnak (pl. jelszómegosztás, nincs MFA kikényszerítve vagy megkerülhető).	4	5	20
C	Egységes módszertan hiánya	A szervezetek különböző szabályzatokat hoznak létre és eltérő gyakorlatok alakulnak ki az incidensek kezelésére.	3	3	9
D	Nem jó az IT-szabályozottság	Hiányos, elavult szabályzatok, hibás vagy kockázatos gyakorlatok.	4	4	16
E	Nincs IT-kockázatmenedzsment	Nem azonosított, fel nem ismert kockázatok és forgatókönyvek.	5	5	25
F	Az üzemeltetés kockázatos	Nincs elegendő tudás vagy személyzet az események megelőzésére, a kitettségek és a kockázatok felismerésére.	4	5	20
G	Nincs vagy nem megfelelő a DRP	Esemény bekövetkezése esetén nincs megfelelő követendő protokoll a normál szolgáltatási szint mielőbbi helyreállítására.	4	5	20
H	Nincs vagy nem megfelelő a BCP	Esemény bekövetkezését követően nincs megfelelő eljárás az üzletmenet fenntartására.	3	5	15
I	A NIS2-megfelelés bevezetésére és fenntartására nincs tapasztalat és egységes módszertan	Nincs központi (ágazati) követendő módszertan, keretrendszer, irányelv a NIS2-megfelelés bevezetésére és fenntartására.	5	3	15
J	Késik a Kibertan. tv. végrehajtási rendelete	Nem ismertek a megfeleléshez kapcsolódó pontos részfeladatok, a folyamatban részt vevő hivatalos szereplők (pl. felkészítők, auditorok).	3	4	12
K	A szervezet IT-rendszerének extrém kitettségei	Nincs fedezet orvosolni az elavult gépparkot, a nem támogatott vagy nem frissített szoftvereket és a nem naprakész alkalmazásokat.	4	5	20
L	A menedzsment elköteleződésének hiánya	A menedzsment nem kezeli kiemelt prioritásként a kiberbiztonságot, a NIS2 esetében a teljesítés elkerülésére helyez nagyobb hangsúlyt.	3	5	15
M	Felkészületlen vagy csalárd „felkészítők" – NIS2-bűnözők megjelenhetnek	Az időzavarban vagy az elodázott döntések következtében a nem megfelelően kiválasztott felkészítést végző szervezet hamis biztonságot ad, közben kiszolgáltathat a belső rendszerekről sok bizalmas információt, amelynek ismeretében kihasználhatók lesznek a cégek IT-rendszereinek gyengeségei vagy akár zsarolhatókká tehetők. A „GDPR-bűnözés"-hez hasonlóan.	3	5	15