BLACK CELL
Protecting critical infrastructures

Folytatódik a NIS 2 hazai implementációja – érkezik a követelményeket determináló rendelet

Egy újabb lépéssel közelebb – folytatódik a NIS 2 hazai implementációja, érkezik a követelményeket determináló rendelet

Alig több mint egy éve robbant be a köztudatba a NIS 2 irányelv, és már több hullámot vetett, mint korábban olyan szabályozások megjelenése, amelyek teljesen új alapokra helyeztek egyes szakterületeket (pl.: CIP irányelv 114/2008. EU irányelv, kiberbiztonsági jogszabály 2019/881. EU rendelet). Fontos hangsúlyozni, hogy NIS 2 inkább megerősíti, fokozza, növeli azokat a törekvéseket, amelyeken az EU tagállamai már évek óta fáradoznak a biztonságosabb kibertér és így a fejlett ellenállóképeségük révén üzletfolytonos szolgáltatások garantálása érdekében.

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) 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 tulajdonképpen konkrétabb, formálhatóbb, szervezetre szabhatóbb követelményeket vezet be az uniós és tagállami kiberbiztonsági szabályozási környezetbe, amelyek – többek között a 2016-os NIS végrehajtásának hiátusai okán – eddig nem voltak kellően egyértelműek, vagy nem tükrözték kellő mértékben a közösség elvárásait, célkitűzéseit.

SZERVEZETI KÖTELEZETTSÉGEK

- IBIR bevezetése (kockázatelemzés alapon)
- szállítói lánc biztonságának fokozása
- incidenskezelési képesség és jelentési kötelezettség
- a szükséges és elégséges elv betartása mellett információmegosztás
- tudatosítás és képzés

TAGÁLLAMI SZINTŰ KÖTELEZETTSÉGEK

- nemzeti kiberbiztonsági stratégia megalkotása minden tagállamban
- illetékes hatóságok kijelölése
- nemzeti eseménykezelési képesség fejlesztése (nemzeti CSIRT)
- felsőszintű válságkezelési képességek kialakítása

Hazai érintettség

Magyarországon több mint 10 éve léteznek olyan, információbiztonsággal kapcsolatos szabályok és követelmények, amelyekre alapvetően lehet építeni, amikor a fenti elvárásoknak történő megfelelésre törekszik egy szervezet. A hazánkban ismert jogi környezet természetesen változás alatt van, a jogharmonizációs folyamat jelenleg is zajlik és várhatóan legalább 2024. első félévének végéig eltart majd, mire minden kapcsolódó jogalkotási tevékenység lezárul. Az érintett szabályozói keret a következő:

- a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), amelyről szakmai körökben már kézenfekvő, hogy nem csak állami és önkormányzati szerveket érintő információbiztonsági kötelezettségeket taglal;
- a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben

meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (41-es BM rendelet), amelynek megújulása tulajdonképpen karnyújtásra van; valamint

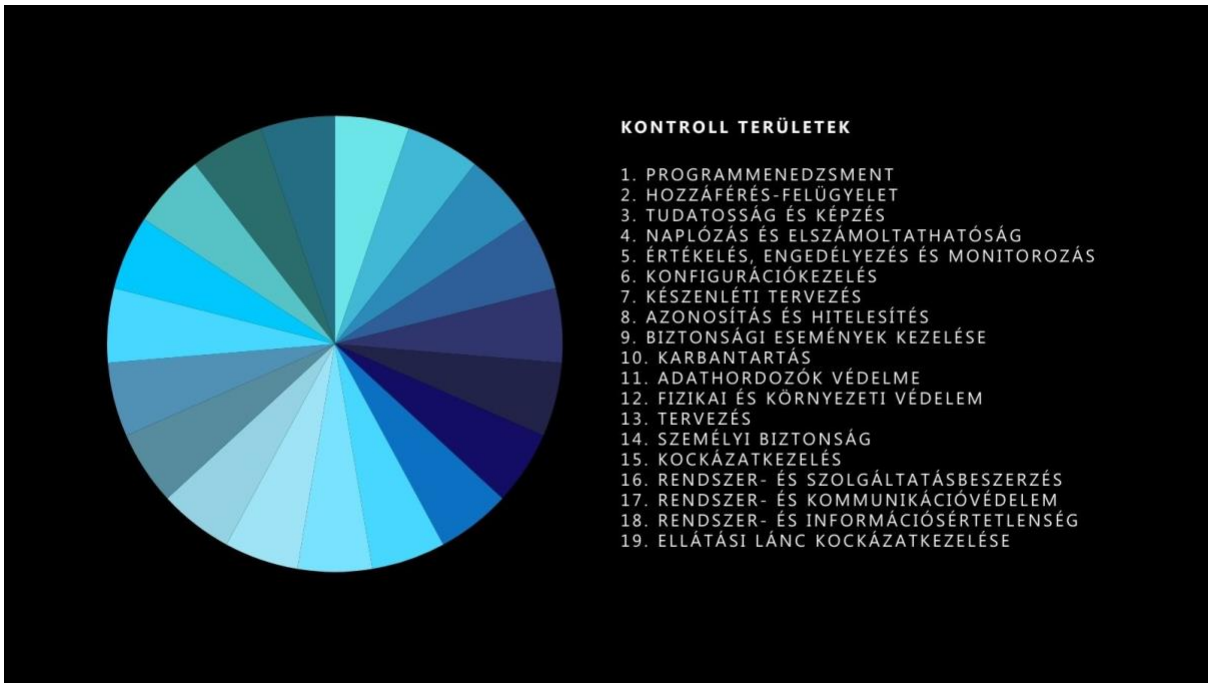
- a jogharmonizációs tevékenység **első eredményterméke, a 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertan.tv)**, amelynek – hatályos verzióját tekintve – fő rendeltetése, hogy a kötelezettségek vonatkozásában **kiterjessze a NIS 2 irányelv által meghatározott személyi hatály szerint az érintettek körét** az állami és önkormányzati szerveken, illetve kritikus infrastruktúrákon túl egyéb piaci szereplőkre is.

A korábbi szabályozások (elsősorban Ibtv.) megújulása és a Kibertan.tv. egyes rendelkezéseinek fokozatos hatályba lépése értelemszerűen magával hozza majd a hatóságok feladatairól szóló, illetve az eseménykezeléssel kapcsolatos kormányrendeletek változását is, ezek azonban már olyan részletszabályok, amelyek kisebb mértékben lesznek hatással a megfelelésre történő felkészülésre.

Mindezt az implementáció kvázi utolsó fázisa követi, vagyis az érdemi jogalkalmazás. **2024. októberétől** ugyanis az **érintett szervezeteknek teljesíteniük kell** a rájuk vonatkozó kötelezettségeket az **elvárt szinten és minőségben**, úgy, hogy az kielégítse azt a közösségi célkitűzést, amely egységesen magasszintű kiberbiztonságot kíván kialakítani a tagállamok számára **kiemelten kritikus/kockázatos** (pl. energia, szállítmányozás, banki és pénzügyi szolgáltatások, egészségügy és bizonyos közműszolgáltatások), illetve az **egyéb kritikus/kockázatos ágazatok**ban (pl. postai és futárszolgálatok, hulladékgazdálkodás, gyártás, digitális szolgáltatók) működő szervezetek vonatkozásában. Az implementáció végezetül azzal zárul majd (valamikor 2027 környékén), hogy az EU részéről is megállapítást nyer a jogharmonizáció megfelelősége és az alkalmazás útján elérni kívánt eredményesség.

A megfelelés kulcsfontosságú a ténylegesen magasszintű kiberbiztonság eléréséhez, és nem csak közösségi érdekeket szolgál, hanem minden érintett – tagállamok és szervezetek – alapvető, üzleti-piaci-szolgáltatói érdeke is kell legyen.

Mindennek egyik eszköze lesz a 2024. január 31-én társadalmi egyeztetésre közzétett, a fent említett 41-es **BM rendelet megújulását célzó rendelettervezet a Miniszterelnöki Kabinetiroda gondozásában**. Szakmai tartalmát tekintve a tervezet a **NIST SP 800-53 rev. 5.** szabványban szereplő kontrollkövetelményekre alapoz. Ugyanakkor a hatályos 41-es BM rendelethez képest összesen 19 kontrollterületet különít el, amelyekhez 913 követelmény csoportot sorol fel. A követelménycsoportok vonatkozásában megállapítható, hogy azokban NIST szabványokra jellemző keretrendszer mellett az **ISO/IEC 27001:2022** megújult megközelítései is fellelhetők.



A követelmények **fókuszpont**jában természetesen továbbra is az **elektronikus információs rendszer**t találjuk, amely a védendő információkat és adatokat tárolja, feldolgozza és továbbítja. Metodikát tekintve szintén nincs változás abban, hogy az elektronikus információs rendszereket a **bizalmasság**, a **sértetlenség** és a **rendelkezésre állás** szempontjából értelmezhető fenyegetések vizsgálatával, illetve a működési sajátosságokat figyelembe vevő **kockázatértékelési módszertan** alkalmazásával **biztonsági osztályok**ba kell sorolnia a szervezeteknek. Ehhez azonban a korábban ismert 5-ös skála helyett 2024 októberétől a háromosztatú, **ALAP-JELENTŐS-MAGAS** osztályokat kell alkalmazni. A rendelettervezet 1. melléklet 2. fejezete részletezi az osztályok közötti különbségeket, amelyek ismerősek lehetnek a korábbi rendezési elv jellemzői révén (káresemény bekövetkezése, adatok érintettsége, társadalmi-politikai hatásvizsgálat, kárérték-költségvetés reláció).

A követelmények meghatározása szintén követi az eddigi metodológiát, az adott elektronikus információs rendszer biztonsági osztálya irányadó a **teljesítendő kontrollok**at illetően, továbbra is azzal a céllal, hogy a fenyegetések által okozható **károk mértékével arányos módon** biztosított legyen a rendszerek és azok fizikai környezetének védelme. A tervezet ismert verziójában – az eddigi szabályozási körülménynél jóval pontosabb és alkalmazhatóbb tartalommal – helyet kapott az **eltérés lehetősége** is, az 1. melléklet 3-4. fejezetei ugyanis lehetővé teszik, hogy indoklással és az egyenértékűség alátámasztása mellett a szervezetek alternatív megoldásokat alkalmazzanak, vagy kifejezetten a működtetési specifikációra tekintettel egyedi eltéréseket valósítsanak meg.

Üdvözlendő újítás a rendelettervezetben, hogy a korábbi szabályozás hiátusát pótló **kockázatkezelési keretrendszer** kialakítását és működtetését követeli meg az érintettektől, amely nem csak adminisztrációs kötelmeket jelent, hanem a **stratégiai gondolkodás** képességét, a kiberbiztonsághoz kötődő, hosszútávú **célok** megvalósítását és annak **felügyelet**ét, illetve **ellátási lánc szintű – komplex – megközelítés**t egyaránt elvár a szervezetektől.

A NIS 2 egyik erőteljes vívmánya, hogy sokkal markánsabban nevesíti a felelősségi köröket, és **dedikáltan ruházza fel az első számú vezetőket a felelősség intézményével**. Ennek leképezését találjuk meg a tervezet olyan megfogalmazásaiban, mint a *„szervezet vezetője más személyre át nem ruházható feladatkörében eljárva…”*, illetve a 2. mellékletben található védelmi intézkedések katalógusában fellelhető **jóváhagyás**i jogkörökben, a felsővezetőkre is kiterjesztett biztonságtudatossági **képzés**ekben, vagy a biztonsági események kezelésének hatékonyabbá tételéhez kapcsolódó **erőforrásbeli és vezetői támogatás**t elváró kontrolljaiban.

A tervezet – a szakmai körökben már jól ismert 41-es BM rendelet struktúrájára emlékeztető formában, mégis új arculattal – tartalmazza a már említett védelmi intézkedéseket, amelyeket ezúttal nem kategorizál be a jogalkotó adminisztratív-fizikai-logikai halmazokba. A 19 kontrollterülethez felsorolt követelménycsoportok, illetve az azokhoz tartozó követelmény szövegezés egyértelműen azt a megközelítést kívánja erősíteni, amit önmagában a NIS 2 irányelv is:

- **a komplex látásmód** kialakítását,
- az adminisztratív, a fizikai, illetve a logikai **intézkedések egymásra épülését és egymástól való függőségét,**
- azt a **speciális szimbiózist**, amelyből látnia kell minden szervezetnek, hogy **az interdependens körülmények** valóban **magasszintű és reziliens képességek meglétét teszik szükségessé,** amelyek **átfogó szemléletet igényelnek a döntéshozás, a végrehajtás és az ellenőrzés folyamataiban** egyaránt.

A Black Cell kiemelt figyelemmel kíséri a NIS 2 irányelvvel kapcsolatos fejleményeket mind EU-s, mind hazai viszonylatban. Különösen fontosnak tartjuk, hogy a változások által érintett ügyfeleinket támogassuk a megfelelésben. Célunk továbbá olyan új partnerségeket kialakítani, amelyekben szakértőink a NIS 2 miatti szabályozói elvárásoknak való megfelelésen túl, a reziliens működés kialakítása érdekében a kontrollterületek szinergiáinak kiaknázásával támogathatják ügyfeleinket.

A Black Cell, mint a Microsoft Security Solutions Partnere elsőkézből rendelkezik azokkal a fejlesztési törekvésekkel, Security és Compliance megoldásokkal kapcsolatos információkkal, amelyekkel a Microsoft – nem csak a termékeit már használó – ügyfeleit kívánja kifejezetten a NIS 2 megfelelésben támogatni.

A következő hónapok a felkészülés, a tervezés és a megvalósítás égisze alatt fognak telni azoknak a cégeknek, akik eddig még nem tartoztak az érintettek közé, illetve azoknak a szereplőknek is, akik csak részben tudták teljesíteni a már ismert kötelezettségeiket. Az eddig ismert szabályozások viszonylatában a következő mérföldköveket és határidőket célszerű figyelembe venni: