BAROSS MÁRK TAMÁS – VARGA PÉTER JÁNOS – GYÁNYI SÁNDOR

IoT-eszközök és IoT-rendszerek biztonságának kérdései a NIS2 bevezetésének szempontjából

Security issues of IoT devices and systems for the implementation of NIS2

DOI: HTTPS://DOI.ORG/10.53793/RV.2025.1.4

Absztrakt

Elemzésünkben a NIS2 irányelv bevezetésével kapcsolatos új biztonsági kérdésköröket vizsgáljuk az IoT- és IIoT-eszközök, valamint -rendszerek szempontjából. A NIS2 célja az Európai Unió kiberbiztonsági szintjének növelése, különösen a kritikus ágazatokban, mint az energiaipar, az egészségügy és a közlekedés. Az irányelv kiemelten foglalkozik a kockázatkezeléssel, az adatvédelemmel, a hálózatbiztonsággal és az incidenskezeléssel. Hangsúlyozza a folyamatos frissítések, az erős hitelesítési módszerek és a beszállítói kockázatok kezelésének fontosságát. A NIS2 célja, hogy növelje az IoT-eszközök biztonságát, minimalizálva ezzel a kibertámadások kockázatát.

KULCSSZAVAK: NIS2, IOT, IIOT, KIBERBIZTONSÁG, IPAR 5.0

Abstract

In our analysis, we look at the new security issues related to the introduction of the NIS2 Directive from the perspective of IoT and IIoT devices and systems. NIS2 aims to increase the level of cybersecurity in the European Union, especially in critical sectors such as energy, healthcare and transport. The Directive focuses on risk management, data protection, network security and incident management. It stresses the importance of continuous updates, strong authentication methods and vendor risk management. NIS2 aims to enhance the security of IoT devices, minimising the risk of cyber-attacks.

KEYWORDS: NIS2, IOT, IIOT, CYBERSECURITY, INDUSTRY 5.0

Bevezetés

A NIS2 (Network and Information Systems Directive 2) irányelv megjelenésekor már tudható volt, hogy a hálózati és információs rendszerek kiberbiztonsága kiemelt fontosságú lesz a jövőben. A NIS1 irányelv már 2016-ban megjelent, és ez alapozta meg a NIS2 irányelvet, amelyet 2022-ben adtak ki. Az új irányelv az Európai Unió minden tagállamára vonatkozik, és az egyes országoknak kötelezően implementálniuk kell annak rendelkezéseit 18 kritikus ágazatban az egységes jogi keret megvalósítása érdekében.

A legfontosabb különbség az első irányelvhez képest az, hogy a NIS2 szélesebb körben alkalmazandó, egyértelműbb szabályokat határoz meg, és szigorúbb felügyeleti követelményeket vezet be, ezáltal erősítve a kiberbiztonsággal kapcsolatos uniós törekvéseket. Az irányelv fő célja, hogy az egyes tagállamok javítsák kiberbiztonsági képességeiket, és hatékonyabban reagáljanak az esetleges kibertámadásokra.

Ezen túlmenően az irányelv előírja a kockázatkezelési intézkedések és a jelentéstételi kötelezettségek bevezetését, amelyek minél több releváns ágazatra kiterjednek. Emellett az uniós tagállamoknak együttműködési szabályokat kell kialakítaniuk az információmegosztás, a felügyelet és a kiberbiztonsági intézkedések végrehajtása érdekében.

Cikkünkben részletesen bemutatjuk a NIS2 és az IoT kapcsolatát, valamint az irányelv hatását az IoT-eszközök és -rendszerek biztonságára.

Kockázatkezelés és megfelelőség az IoT-eszközökkel és -rendszerekkel szemben

A NIS2 egy európai uniós kiberbiztonsági irányelv, amelynek fő célja, hogy a tagállamok egységes és magas

szintű kiberbiztonságot érjenek el, különös tekintettel a hálózati és információs rendszerek biztonságára. (URL1)

Az új szabályozás számos szektort érint, többek között:

- energiaipar
- gyártási szektorok
- közlekedés
- kereskedelem
- banki szektor
- egészségügy
- digitális infrastruktúra
- kritikus ipari ágazatok (például vegyipar).

Ezekben a szektorokban egyre nagyobb számban jelennek meg IoT (Internet of Things) és IIoT (Industrial Internet of Things) eszközök, amelyek fokozott biztonsági figyelmet igényelnek a meglévő rendszerekben. Ennek következtében a NIS2 irányelvben meghatározták az ilyen eszközök felügyeletét és védelmét.

Ilyen eszközök lehetnek például:

- okosmérőórák
- automatizált gyártósorok
- önvezető autók
- készletgazdálkodási rendszerek eszközei
- hordozható eszközök
- gyógyszeradagolók
- hálózati érzékelők
- légszennyezettséget monitorozó szenzorok.

A NIS2 irányelv célja, hogy megerősítse e rendszerek és eszközök biztonságát, csökkentve a kibertámadások és egyéb fenyegetések kockázatát.

Az IoT- és IIoT-rendszerek kockázatkezelése és megfelelősége különösen nagy figyelmet igényel, mivel ezek az eszközök gyakran kapcsolódnak más hálózatokhoz, folyamatos kommunikációt folytatnak más eszközökkel és rendszerekkel, valamint érzékeny adatokat is kezelnek. A NIS2 irányelv célja, hogy növelje az Európai Unió digitális infrastruktúrájának biztonságát, valamint minimalizálja a kibertámadások kockázatát az Internet of Things eszközök sebezhetőségeinek kihasználásával szemben. (Jara–Martinez–Sanchez 2024; URL2)

A kockázatkezelés magában foglalja a sérülékenységek felmérését és a megfelelő biztonsági intézkedések meghatározását. Ehhez szorosan kapcsolódik az adatbiztonság, a hálózati forgalom védelme, a hozzáférés-szabályozás, valamint a rendszeres szoftver- és firmware-frissítés. Emellett egy kiemelten fontos kockázatkezelési terület is megjelenik, amely az ellátási láncra terjed ki. Ebben az esetben tisztában kell lennünk a harmadik felek által szállított eszközök és rendszerek integrációjában rejlő kockázatokkal, ami különösen fontos az IoT-eszközök és -rendszerek esetében. (URL3)

Az alábbi három kockázati tényezőt érdemes figyelembe venni az IoT- és IIoT-eszközök, valamint -rendszerek kapcsán:

- *Sebezhetőségek és fenyegetettségek*
  Az IoT-eszközök és -rendszerek gyakran elavult szoftvereket használnak, ráadásul sok esetben nem érhető el az automatikus frissítési opció. Ennek következtében a már nem támogatott eszközök és rendszerek könnyű célponttá válhatnak a kibertámadók számára. Emellett kiemelt kockázatot jelent a firmware-frissítések elmulasztása, amely lehetőséget biztosít a támadók számára a régebbi sérülékenységek kihasználására. A NIS2 irányelv előírja, hogy ezen kockázatok minimalizálása érdekében folyamatos frissítéseket és biztonsági javításokat kell alkalmazni.
- *Adatvédelem és titkosítás*
  Az IoT-rendszerek rövid időn belül hatalmas mennyiségű adatot gyűjthetnek rólunk és környezetünkről, amelyek bizalmas információkat is tartalmazhatnak. Sajnos sok IoT-eszközt és -rendszert úgy terveztek és gyártottak le, hogy csak minimális kiberbiztonsági funkciókkal rendelkezzenek, elsősorban az alacsony költségek miatt. Kiemelt problémát jelentenek például a gyenge, alapértelmezett jelszavak, amelyekkel nap mint nap találkozhatunk. Emellett kockázatot jelentenek a nyitott portok és a sebezhető protokollok. A megfelelő adatvédelmet és titkosítást az irányelv előírásainak megfelelően biztosítani kell.
  Ez magában foglalja:
    - a titkosítás kötelező alkalmazását
    - a hozzáférések ellenőrzését
    - az adatok minimalizálását
    - az auditálás és a naplózás megfelelő végrehajtását és annak dokumentálását.

Ezek az intézkedések elengedhetetlenek az IoT-rendszerek biztonságának növelése és a kibertámadások kockázatának csökkentése érdekében.

- *Hálózati biztonság*
  Az IoT-eszközök gyakran különböző rendszerekbe integrálódnak, ezáltal a hálózat biztonsága kritikus tényezővé válhat. Ez különösen igaz az eltérő gyártók által alkalmazott különböző szabványokra és megoldásokra, amelyek megnehezítik a megfelelő biztonsági intézkedések kialakítását. Továbbá ezek az eszközök sok esetben nem megfelelően titkosított kommunikációs protokollokat használnak, amelyek könnyen lehallgathatók. A hálózat biztonságának növelése érdekében megfelelő megoldás lehet a hálózat szegmentálása, amelyet tűzfalakkal és illetéktelen

behatolásokat észlelő riasztórendszerekkel célszerű kiegészíteni.

A NIS2-ben az alábbi megfelelési elveket találhatjuk az IoT-eszközök és -rendszerek esetében:

- *Biztonsági intézkedések és megelőzés*

  A szervezeteknek olyan megfelelő biztonsági követelményrendszert kell megvalósítaniuk, amely garantálja az IoT-eszközök és -rendszerek biztonságát.

  Ennek részei:

  - erős hitelesítési módszerek alkalmazása
  - biztonságos kommunikációs csatornák kialakítása
  - a sebezhetőségek folyamatos ellenőrzése megfelelő módszerekkel.

Ezen kívül szorosan kapcsolódik hozzá a tudatosságnövelő képzés is, amelynek célja, hogy a munkavállalók felismerjék a lehetséges kockázatokat és biztonságosan használják eszközeiket. (Fehér-Polgár–Michelberger 2018; Michelberger 2024)

Incidensjelentés és reagálás

Az IoT-rendszerekhez kapcsolódó biztonsági incidensek kezelését a NIS2 irányelv szabályozza, amely előírja a jelentési kötelezettséget az illetékes hatóságok felé. Az érintett szektorokban olyan intézkedési rendszert kell kialakítani, amely hatékonyan és gyorsan reagál a kiberbiztonsági eseményekre. Az IoT-rendszerekben például az eszközök szegmentálása hatékony megoldás lehet az esetlegesen felmerülő károk minimalizálása érdekében.

Szervezeti megfelelőség

A szervezeteknek olyan intézkedéseket és eseményeket kell megvalósítaniuk, amelyek során az IoT-eszközök kockázati értékelésére, a megfelelő védelmi intézkedésekre, valamint a szabályozási megfelelőség fontosságára hívják fel a figyelmet. A NIS2 irányelv előírja, hogy megfelelőségi auditorokat kell alkalmazni, akik biztosítják az egyes rendszerek jogszabályi előírásoknak való megfelelőségét.

Folyamatos fejlesztés

Az IoT-eszközök és -rendszerek fejlesztése szempontjából a biztonságosság elengedhetetlen, ezért a NIS2 irányelv kiemeli a folyamatos fejlesztés és a jövőbeni fenyegetésekhez való alkalmazkodás fontosságát. Emellett az irányelv hangsúlyozza a nemzetközi szabványok és legjobb gyakorlatok (best practices) alkalmazását az eszközök és rendszerek tervezése során. Ennek érdekében a vállalatoknak frissítési terveket kell kidolgozniuk, figyelembe véve a különböző kockázati tényezőket.

A NIS2 irányelv által előírt kockázatkezelés és megfelelőségi követelmények betartása kulcsfontosságú az IoT- és IIoT-eszközök, valamint -rendszerek biztonságának és integritásának fenntartásához. A biztonság megerősítése közvetetten a kockázatkezelési és megfelelőségi követelményrendszer szigorításán keresztül valósul meg.

Az érintett szervezeteknek nemcsak az eszközök és rendszerek sérülékenységeit kell felismerniük és kezelniük, hanem biztosítaniuk kell az egész IoT-ökoszisztéma védelmét is. Ez magában foglalja:

- hálózati kapcsolatok biztonságát
- a beszállítók megfelelőségét a szabályozási követelményeknek.

Ezek az intézkedések elengedhetetlenek az IoT-alapú infrastruktúrák megbízhatóságának és ellenálló képességének növeléséhez.

Kiberbiztonsági minimumkövetelmények

A NIS2 irányelvben megfogalmazott kiberbiztonsági minimumkövetelmények létfontosságúak az IoT-eszközök biztonsága, valamint az általuk alkotott hálózatok védelme szempontjából. Az irányelv az Európai Unió egészére kiterjed, és célja az egységes kiberbiztonsági szabályozás kialakítása. A NIS2 fő feladata, hogy növelje a létfontosságú és kritikus szolgáltatások ellenálló képességét, különösen az érintett szektorokban működő szervezetek számára. Fontos megjegyezni, hogy az irányelv nem tartalmaz specifikus IoT-követelményeket. Azonban az általános kiberbiztonsági minimumkövetelmények közvetetten kiterjednek az IoT-eszközökre és -rendszerekre is, ezáltal hozzájárulva azok biztonságának és védelmének erősítéséhez. (Fagan et al. 2020; URL4; URL5)

Kiberbiztonsági minimumkövetelmények

Kockázatkezelés és sérülékenységkezelés

A NIS2 irányelvei alapján az egyes szervezetek kötelesek kockázatkezelési eljárásokat megvalósítani és végrehajtani, amelyek a teljes működési környezetet lefedik. Emellett azonosítaniuk és kezelniük kell a sérülékenységeket, beleértve az ellátási láncokat, valamint a harmadik felek által jelentett kockázatokat is.

Incidenskezelés

Az érintett szervezeteknek kötelességük incidenskezelési tervet kialakítani, amely hatékony és gyors választ ad a kiberbiztonsági események bekövetkezése esetén.

Az incidensek dokumentálása és bejelentése kötelező. A kezdeti bejelentést az illetékes hatóságok

felé 24 órán belül meg kell tenni, valamint a részletes tájékoztatást 72 órán belül kell benyújtani.

Hálózatbiztonsági követelmények

A hálózatok védelme érdekében megfelelő biztonsági intézkedési rendszert kell megvalósítani. Ennek részei többek között:

- tűzfalak alkalmazása
- behatolásmegelőző rendszerek (IPS) telepítése
- behatolásérzékelő rendszerek (IDS) használata
- a hálózati forgalom folyamatos monitorozása és naplózása.

Ezek az intézkedések kulcsfontosságúak a kiberbiztonsági fenyegetések azonosítása és elhárítása érdekében.

Adatvédelem és titkosítás

A szervezetekben keletkező adatokat bizalmasan kell kezelni, és fejlett titkosítási algoritmusokat kell alkalmazni az adatvédelem érdekében. A fontos és érzékeny adatok tárolásának biztonságosnak kell lennie, valamint azok továbbítása során is a lehető legkörültekintőbben kell eljárni, hogy minimalizálják az illetéktelen hozzáférés kockázatát.

Hozzáférés kezelése

Az egyes rendszerekhez és az azokból kinyert információkhoz való hozzáférést szigorúan szabályozni kell. A „Principle of Least Privilege" (a legkisebb jogosultság elve) alapján minden felhasználó kizárólag a saját feladatköréhez szükséges jogosultságokat kapja meg, ezzel minimalizálva a jogosulatlan hozzáférés kockázatát. Emellett elengedhetetlen a többtényezős hitelesítés (MFA) alkalmazása, amely további védelmi réteget biztosít az illetéktelen hozzáférések ellen.

Biztonsági tervezés és karbantartás

A szervezeteknek biztosítaniuk kell, hogy rendszereik és folyamataik tervezése és megvalósítása megfeleljen a „Security by Design and Default" elvének. Ezen túlmenően, a karbantartás során elengedhetetlen a rendszeres szoftverfrissítések és hibajavítások elvégzése, hogy a rendszerek folyamatosan megfeleljenek a biztonsági követelményeknek és védettek maradjanak a sérülékenységekkel szemben.

Kiberbiztonsági képzés

Az egyes szervezetek kötelessége, hogy munkavállalóik számára folyamatos kiberbiztonsági képzést biztosítsanak, amely specifikusan kiterjed az adott munkakörnyezetre. Emellett a biztonságtudatosság növelése érdekében érdemes különböző gyakorlati feladatokat és szimulációkat megvalósítani, hogy a munkavállalók hatékonyabban felismerjék és kezeljék a lehetséges kiberbiztonsági kockázatokat.

Rendszeres audit és tesztelés

A szervezetek számára további követelmény a rendszeres auditálások elvégzése, amely biztosítja saját rendszereik megfelelőségét. Emellett kötelező a penetrációs tesztek és sérülékenységi vizsgálatok folyamatos végrehajtása, hogy az esetleges biztonsági rések időben azonosíthatók és kezelhetők legyenek. Amennyiben a szervezetek nem felelnek meg a követelményeknek, szigorú szankciók léphetnek életbe, például pénzbírság, amely elérheti az éves árbevételük 2%-át, valamint egyéb jogi következményekkel is számolniuk kell.

A fent említett minimumkövetelmények célja, hogy a szervezetek ellenállóbbá váljanak a kiberfenyegetésekkel szemben. Az irányelv hangsúlyt helyez a proaktív intézkedésekre, amelyek célja a támadások kockázatának és hatásának csökkentése. (Fagan et al. 2020; URL6)

Ellátási lánc és beszállítói kockázatok

A NIS2 irányelve szerint az ellátási lánc és a beszállítói kockázatok kezelése kulcsfontosságú, mivel az IoT-eszközök és -rendszerek különböző gyártóktól és beszállítóktól származhatnak. A hálózatokba kapcsolt eszközök biztonsága nagymértékben függ az ellátási lánc biztonságától, valamint a beszállítók által alkalmazott biztonsági gyakorlatoktól, ezért a szervezeteknek kiemelt figyelmet kell fordítaniuk a harmadik felektől származó eszközök és szolgáltatások kockázatelemzésére, és biztosítaniuk kell azok megfelelőségét a kiberbiztonsági követelményeknek. (Fagan et al. 2021)

A legfontosabb vonatkozások a NIS2 szempontjából az alábbiak:

Ellátási lánc biztonsági követelményei

Az ellátási lánc biztonsági követelményei szempontjából két kulcsfontosságú terület emelhető ki: a szervezeti felelősség és a harmadik felek ellenőrzése.

A szervezeti felelősség kiterjed a teljes ellátási lánc biztonsági megfelelésének biztosítására. Ez magában foglalja:

- a beszállítók kiválasztását
- a velük megkötött megállapodások és szerződések biztonsági követelményeit
- az együttműködés során alkalmazott biztonsági előírások betartását.

A harmadik felek ellenőrzése során három fő területet kell figyelembe venni:

- a gyártási folyamatok ellenőrzése

- a firmware- és hardverkomponensek eredetének vizsgálata
- a szoftveres biztonsági szabályok betartásának ellenőrzése.

Ezek az intézkedések kulcsfontosságúak az ellátási lánc biztonságának fenntartásához, valamint a lehetséges kiberbiztonsági fenyegetések minimalizálásához.

Beszállítói kockázatértékelés

A kockázatalapú megközelítés alkalmazása során az IoT-eszközök és a beszállítók esetében folyamatos kockázatelemzést kell végezni.

Ez magában foglalja:

- az IoT-eszközök szoftveres és hardveres összetevőinek sérülékenységvizsgálatát
- az egyes beszállítók biztonsági gyakorlatainak értékelését.

Emellett folyamatos monitorozást kell alkalmazni, hogy a beszállítóknál felmerülő kockázatokat időben azonosítani lehessen, különösen az új típusú fenyegetések és sérülékenységek esetén.

Szerződéses követelmények

Az érintett szervezeteknek szigorú követelményeket kell meghatározniuk szerződéseikben a beszállítókkal szemben.

A legfontosabb követelmények közé tartoznak:

- adatvédelmi szabályok betartása: biztosítani kell, hogy az eszközök által gyűjtött adatok megfelelő módon legyenek kezelve
- frissítési és javítási kötelezettségek teljesítése: ideértve a hibajavítások biztosítását és a megfelelő firmware-frissítések rendszeres elvégzését
- incidensjelentési követelmények teljesítése: a beszállítóknak haladéktalanul jelenteniük kell a biztonsági eseményeket, hogy minimalizálják a lehetséges károkat.

Ezek az előírások biztosítják az ellátási lánc biztonságát és az IoT-eszközök folyamatos védelmét a kibertámadásokkal szemben.

Gyártói biztonság

Az IoT-eszközök integrálása során biztosítani kell mind a hardveres, mind a szoftveres komponensek eredetének ellenőrzését, valamint azok biztonságos beépítését. Különösen fontos a harmadik felek által biztosított firmware és szoftver, mivel ezek rejtett sérülékenységeket hordozhatnak, amelyeket a támadók kihasználhatnak. Emellett a hardverelemek gyártási életciklusában található gyenge vagy nem megfelelően ellenőrzött egységek is jelentős biztonsági kockázatot jelenthetnek.

Frissítések és javítások kezelése

Az IoT-eszközök gyártóinak és a rendszerek üzemeltetőinek biztosítaniuk kell a biztonsági és hibajavítási frissítések gyors elérhetőségét és telepíthetőségét, valamint ezek biztonságos, távoli végrehajtását. Ezen túlmenően az ellátási lánc minden szintjén garantálni kell a frissítések biztonságosságát és hitelességét, hogy minimalizálják az esetleges manipulációs vagy támadási lehetőségeket. A frissítések és javítások végrehajtásának dokumentálása elengedhetetlen.

Incidensekre való felkészültség

A beszállítóknak kötelezően részt kell venniük az incidenskezelési tervek végrehajtásában. Az együttműködésük a szervezetekkel és hatóságokkal elengedhetetlen az IoT-rendszerekkel kapcsolatos biztonsági incidensek esetén. Különösen fontos a kapcsolódó adatok, naplófájlok és eseménynaplók biztosítása, mivel ezek nélkülözhetetlenek az incidensek okainak beazonosításához és hatékony kezeléséhez.

Szabványok és tanúsítványok

Az IoT-eszközök gyártóinak és beszállítóinak tisztában kell lenniük az iparági szabványokkal és tanúsítványokkal, mint például:

- ISO/IEC 27001 – Információbiztonsági irányítási rendszerek
- ETSI EN 303 645 – IoT-eszközök biztonsági szabványa
- CSA IoT Security Controls Framework – Felhőbiztonsági Szövetség (CSA) által meghatározott IoT-biztonsági ellenőrzési keretrendszer.

A gyártók és beszállítók számára a meglévő tanúsítványok növelik hitelességüket és erősítik a bizalmat az ellátási láncban részt vevő felek között. Azok a beszállítók, akik nem felelnek meg a NIS2 irányelv elvárásainak, kizárhatók a szervezeti ellátási láncból. Súlyos szabálytalanság esetén jogi lépések vagy pénzbírság is kiszabható.

A NIS2 irányelv előírásai szerint azoknak a szervezeteknek, amelyek IoT-eszközöket alkalmaznak, monitorozniuk kell az ellátási láncot és ki kell értékelniük a beszállítói kockázatokat.

Ez magában foglalja:

- a kockázatok rendszeres felügyeletét
- a harmadik felek biztonsági gyakorlatainak ellenőrzését
- a szerződéses és jogi szabályozások pontos betartását.

Ezek az intézkedések biztosítják, hogy az érintett rendszerek ne legyenek kitéve veszélynek az ellátási lánc

gyenge pontjai miatt, így csökkentve a kibertámadások kockázatát. (URL7; Fagan et al. 2021)

Összefoglalás

Elemzésünkben bemutattuk a NIS2 irányelv bevezetésével kapcsolatos új biztonsági kihívásokat, különös tekintettel az IoT- és IIoT-eszközök és -rendszerek védelmére. A NIS2 célja az EU kiberbiztonsági szintjének növelése, különösen a kritikus szektorokban, mint például az energiaipar, az egészségügy, a banki szektor, a digitális infrastruktúrák, a közlekedés és a kritikus ipari ágazatok, például a vegyipar és az energiaszektor.

Az adott szektorokban az IoT- és IIoT-eszközök alkalmazása jelentősen befolyásolja a kockázatkezelési megfelelőséget, ezért kiemelten fontos azok biztonsági kockázatainak vizsgálata és kezelése. A kockázatkezelés magában foglalja a sérülékenységek felmérését, a megfelelő biztonsági intézkedések kidolgozását, az adatbiztonságot, a hálózati forgalom védelmét, a hozzáférés szabályozását, valamint a rendszeres szoftver- és firmware-frissítések biztosítását. Ezen túlmenően egy kiemelten fontos terület az ellátási lánc kockázatkezelése. A szervezeteknek tisztában kell lenniük a harmadik felek által szállított eszközök és rendszerek kockázataival, mivel ezek különösen jelentősek az IoT-eszközök esetében. A NIS2 által előírt kockázatkezelés és megfelelőség betartása elengedhetetlen az IoT- és IIoT-eszközök és -rendszerek biztonságának és integritásának fenntartásához, amelyet közvetetten a kockázatkezelési és megfelelőségi követelményrendszer szigorításán keresztül lehet biztosítani.

A szervezeteknek nemcsak az eszközök és rendszerek sérülékenységeit kell azonosítaniuk és kezelniük, hanem felelősek a teljes IoT-ökoszisztéma biztonságáért is, beleértve a hálózati kapcsolatok védelmét, valamint a beszállítók megfelelőségét a kiberbiztonsági követelményeknek. A NIS2 irányelvben megfogalmazott kiberbiztonsági minimumkövetelmények létfontosságúak az IoT-eszközök biztonsága és az általuk alkotott hálózatok védelme szempontjából. Az irányelv célja, hogy növelje a létfontosságú és kritikus szolgáltatások ellenálló képességét, valamint minimalizálja a kibertámadások hatásait. Fontos megjegyezni, hogy az irányelv nem ír elő specifikus IoT-követelményeket, azonban az általános kiberbiztonsági minimumkövetelmények közvetetten kiterjednek az IoT-eszközökre és -rendszerekre is.

Az irányelv hangsúlyt helyez a proaktív intézkedésekre, amelyek célja a támadások kockázatának és hatásának csökkentése. Emellett a NIS2 szerint az ellátási lánc és a beszállítói kockázatok kezelése elengedhetetlen, mivel az IoT-eszközök és az általuk megvalósított rendszerek különböző gyártóktól és beszállítóktól érkezhetnek. A hálózatokba kapcsolt eszközök biztonsága nagymértékben függ az ellátási lánc biztonságától, valamint a beszállítók kiberbiztonsági gyakorlatától.

A NIS2 irányelv kiemeli a kockázatkezelés, az adatvédelem, a hálózati biztonság és az incidenskezelés jelentőségét. Emellett hangsúlyozza a folyamatos frissítések, az erős hitelesítési módszerek és a beszállítói kockázatok kezelésének fontosságát. Az irányelv egyik célja, hogy növelje az IoT-eszközök biztonságát, ezáltal minimalizálva a kibertámadások kockázatát.

Irodalomjegyzék

Fagan, M.–Marron, J.–Brady, K. G. Jr.–Cuthill, B. B.–Megas, K. N.–Herold, R. (2021) *IoT Non-Technical Supporting Capability Core Baseline*. National Institute of Standards and Technology. NISTIR 8259B. pp. 1-21. https://doi.org/10.6028/NIST.IR.8259B

Fagan, M.–Megas, K. N.–Scarfone, K.–Smith, M. (2020) *IoT Device Cybersecurity Capability Core Baseline.* National Institute of Standards and Technology, NISTIR 8259A. pp. 1-23. https://doi.org/10.6028/NIST.IR.8259A

Fehér-Polgár P.–Michelberger P. (2018) The Information Security Risks of the BYOD. *International Journal of Engineering and Management Sciences*, Vol. 3. No. 4. pp.176–185. https://doi.org/10.21791/IJEMS.2018.4.16.

Jara, A. J.–Martinez, I. C.–Sanchez, J. S. (2024) CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2. *IEEE Smart Cities Futures Summit (SCFC)*, pp. 56-60. DOI: 10.1109/SCFC62024.2024.10698057

Michelberger P. (2024) *Fejezetek a vállalati biztonságmenedzsmentből*. Budapest, Akadémiai Kiadó. DOI: 10.1556/97896345493 76

Internetes hivatkozások

URL1: A NIS 2 irányelv hazai implementációja a T/3314. törvénytervezet alapján. Black Cell Magyarország Ltd. 2023. https://blackcell.io/wp-content/uploads/2023/04/NIS-2-paper.pdf [Letöltve: 2024.10.15].

URL2: 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről. https://net.jogtar.hu/jogszabaly?docid=a2300023.tv [Letöltve: 2024.09.17].

URL3: A 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf [Letöltve: 2024.09.17].

URL4: Managing the Risk of IoT: Regulations, Frameworks, Security, Risk and Analytics. *Isaca Journal*, 2017. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/managing-the-risk-of-iot-regulations-frameworks-security-risk-and-analytics?gad_source=1 [Letöltve: 2024.09.17].

URL5: ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines. ISO, 2022. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27400:ed-1:v1:en [Letöltve: 2024.09.17].

URL 6: ISO/IEC DIS 27404 ISO Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT Draft. ISO, 2024. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27404:dis:ed-1:v1:en [Letöltve: 2024.09.17].

URL7: *The NIS2 Directive A high common level of cybersecurity in the EU*. European Union. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 [Letöltve: 2024.10.15].