NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 3–20. • DOI: 10.32561/nsz.2023.1.1

Bogdanovits András,[1] Kovács Zoltán[2]

# A vezetékes információs rendszerek védelmének speciális szabályai, eszközei a jogszabályokban, ajánlásokban

## *Specific Rules and Tools for the Protection of Wired Information Systems in Legislation and Recommendations*

*Jelen cikk célja, hogy különösen a hírközlési szolgáltatók rendszereire fókuszálva feltárja, szükséges-e a külön is foglalkozni az elektronikus információs rendszerek vezetékes elemeinek a védelmével, vagy azok már az elektronikus információs rendszerek védelmének komplex megközelítése okán kellően védettnek tekinthetők a jelenlegi jogszabályokban, ajánlásokban leírt kontrollok alkalmazásával. Ezért a cikk az információs rendszerek védelmének alapelveiből kiindulva áttekinti a vezetékes és vezeték nélküli hálózatok biztonságának főbb jellemzőit, a vezetékes hálózatokra fókuszálva röviden ismerteti az infokommunikációs hálózatok biztonságához kapcsolódó fontosabb hazai jogszabályokat és (a mérvadónak tekinthető angolszász) nemzetközi ajánlásokat, bemutatja azok kifejezetten vezetékes és vezeték nélküli hálózati elemekre vonatkozó kontrolljait, valamint a biztonság fokozása érdekében javaslatot tesz a továbblépésre.*

***Kulcsszavak:*** *elektronikus információs rendszerek, vezetékes hálózatok, kiberbiztonság, Ibtv., NIST 800-53*

*The aim of this article is to explore, with a particular focus on the systems of communications service providers, whether the protection of the wired elements of electronic information systems needs to be addressed separately, or whether they can be considered sufficiently protected by the application of controls described in current legislation and recommendations, due to the complex approach to the protection of electronic information systems. Therefore, starting from the basic principles of information systems security, the article reviews the main characteristics of wired*

[1] MSc, vezetékes tervezés és nyilvántartás menedzser, Vodafone Magyarország Zrt., e-mail: bogdanovits@gmail.com
[2] PhD, vezérigazgató, NISZ Zrt.; tanársegéd, Nemzeti Közszolgálati Egyetem Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék, e-mail: zkovacs.24@gmail.com

*and wireless network security, briefly describes the main domestic legislation and international recommendations (the most authoritative being Anglo-Saxon) related to the security of information communication networks, describes their controls specifically applicable to wired and wireless network elements, and suggests a way forward to enhance security.*

***Keywords:*** *electronic information systems, wired networks, cybersecurity, NIST 800-53*

## Bevezetés

Az információs társadalom alapját az infokommunikációs infrastruktúrák képezik. Az információs társadalom megléte, hatékony működése az említett infrastruktúrák fejlettségétől függ. Az infokommunikációs technológiák elterjedése alapjaiban alakította át a gazdasági tevékenységeket és a társadalmi kapcsolatrendszereket, ugyanis a gyors információcsere napjaink gazdaságának, társadalmának meghatározó alappillére. Az infokommunikáció sajátossága, hogy a technika, a tudomány fejlődésével mindig újabb fajtái jelennek meg, ezek pedig alapvetően befolyásolják a társadalmi-gazdasági fejlődést, mivel az infrastruktúra folyamatosan alakítja, változtatja ezeket a folyamatokat. Ezek pedig új igényeket generálva visszahatnak az előbbiek fejlődésére, így egyfajta spirált képezve gyorsítják, erősítik egymást.[3]

A felhasználót a legtöbb esetben nem foglalkoztatja, hogy milyen technológia biztosítja a munkájához szükséges hátteret, őt csupán az érdekli, hogy az adott rendszer az igényeinek megfelelő szolgáltatásokat biztosítsa, és biztonságosan működjön. Éppen ezért nem könnyű vállalkozás kizárólag a hírközlési szolgáltatók vezetékes információs rendszerei védelmének speciális szabályairól, a jogszabályi eszközeiről, ajánlásairól írni. Ugyanis a jogszabályok és ajánlások alkotói – helyesen eljárva – holisztikusan kezelik az elektronikus információs rendszerek biztonságának kérdéseit és védelmét, így jobbára a vezetékes hálózatok, különösen a szolgáltatók hálózatai védelmét külön nem emelik ki.

Ugyanakkor két jellemző vezetékes hálózati rész miatt érdemes megvizsgálni ezt a speciális kérdéskört is. Az első a felhasználókat az utolsó mérföldön kiszolgáló hálózati rész. Ebben az esetben a hírközlési szolgáltatók azon hálózati elemei, amelyek itt kizárólag vezetékes módon szolgálják ki a felhasználókat, még mindig nagy forgalmat bonyolítanak le, és általában nagyobb sebességet és megbízhatóságot kínálnak, mint a vezeték nélküli megoldások. Ráadásul a vezeték nélküli hálózati elemek segítségével az információk csak rövid távolságot tesznek meg a levegőben, ezt követően jellemzően nagy kapacitású vezetékes kapcsolatokon keresztül továbbítják azokat. Ez pedig a második olyan szegmens, amely miatt célszerű a vizsgálatot elvégezni. Ráadásul sok biztonsági kérdés mindkét esetben megjelenik.

[3] Kovács 2021.

Az utolsó mérföldön kiszolgáló hálózati részekkel kapcsolatban azonban elmondható, hogy a világon ma már sokkal több ember rendelkezik vezeték nélküli kommunikációs eszközzel, mint csupán vezetékes kapcsolatot biztosítóval. Ezt jól mutatják a magyarországi adatok is. Amíg 2022 első félévében mintegy 3 millió darab volt a lakossági helyhez kötött internet-előfizetések száma,[4] addig csak az internetforgalmat bonyolított okostelefonos SIM-kártyák száma közel 7,5 milliót tett ki.[5] Ráadásul napjainkban már a kizárólag vezeték nélküli kapcsolódási lehetőséggel rendelkező okostelefonok és táblagépek száma meghaladja a személyi számítógépekét, bár ez utóbbiak – elsősorban a hordozható kivitelűek – jellemzően szintén rendelkeznek vezeték nélküli kapcsolódási lehetőségekkel.[6] Az okostelefonok és táblagépek tömeges elterjedésével, a 3G/4G, majd az 5G mobilhálózatok bevezetésével és a wifihozzáférési pontok nagy arányú kiépítésével a vezeték nélküli adatforgalom robbanásszerűen nőtt az elmúlt években. Ám ezekben a hálózatokban is a rádiós szakasz után megjelennek a vezetékes elemek. Így a mobil adatátvitel növekedése valójában növeli a vezetékes hálózatok iránti keresletet is, ezért az infokommunikációs rendszerek biztonságát jelentősen befolyásolja a hírközlési szolgáltatók vezetékes információs rendszereinek a biztonsága. Hazánkban az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint:

> „14b. elektronikus információs rendszer:
> a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő 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; vagy
> c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;"[7]

Így az idézett rész a) pontja szerint érdemes és kell is a hírközlési szolgáltatók hálózatainak védelmi kérdéseivel foglalkozni.

## *A CIA-elv*

Az elektronikus információs rendszer biztonsága a rendszer olyan állapota, amelynek védelme a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Az elektronikus információs rendszerek biztonságfogalmát tovább elemezhetjük az alábbi követelmények szerint, ami angol kifejezések kezdőbetűinek összeolvasásából CIA-elv néven fogalmazható meg:

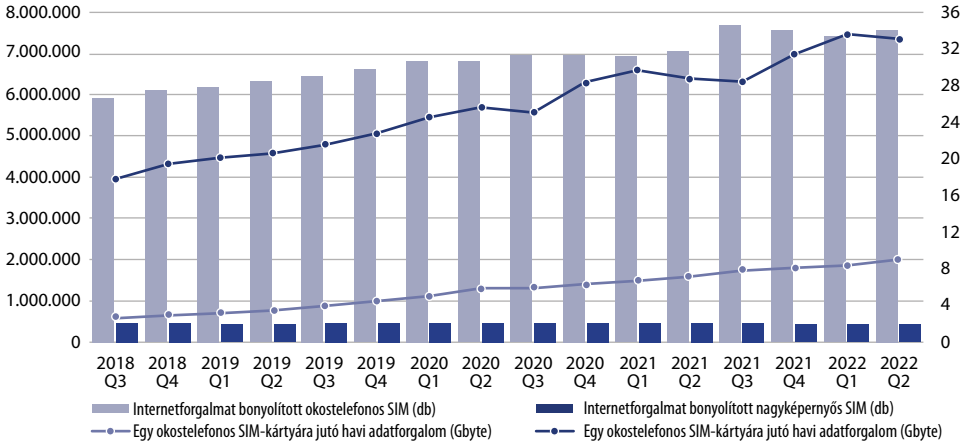
4 NMHH 2022a.
5 NMHH 2022b.
6 Lásd: www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics
7 2013. évi L. törvény.

- *Bizalmasság (Confidentiality)* követelménye azt jelenti, hogy egy adott információt csak az arra jogosultak és csak a jogosultságaik szerint ismerhetik meg, használhatják fel, vagy rendelkezhetnek annak felhasználásáról. Azaz illetéktelenek csak nagy erőbefektetéssel, költséggel, vagy kis valószínűséggel legyenek képesek az adott információhoz hozzájutni. A követelmény biztosítására például hozzáférésvédelmi rendszereket, kriptográfiai eljárásokat használnak, amelyek segítik illetéktelenek hozzáférésének megakadályozását az adott információhoz.
- *Sértetlenség (Integrity)* követelménye azt jelenti, hogy az adat tartalma és tulajdonságai megegyeznek az elvárttal, egy adott információt vagy rendszert csak az arra jogosult változtathat meg. Ebbe beletartozik, hogy az adott adat hiteles (az elvárt forrásból származik) és letagadhatatlan (bizonyítható annak származása). A véletlenül megváltozott információt is figyelembe véve, ez a követelmény nagy hangsúlyt fektet a módosítás észlelésére. A követelmény biztosítására az előző bizalmasság követelmény biztosítására szolgáló eszközökön kívül többek között használatos a digitális aláírás és különböző hitelesítő eljárások.
- *Rendelkezésre állás (Availability)* követelménye azt jelenti, hogy az adott adatot vagy rendszert az arra jogosultak a szükséges időben és időtartamban használni tudják, azaz megmutatja, hogy egy adott rendszernek milyen megbízhatósággal kell ellátni a feladatát. A követelmény olyan objektív statisztikai jellemzőkkel jellemezhető, mint az üzemidő, rendelkezésre állási tényező és a sebezhetőségi ablak.[8]

## Vezeték nélküli és vezetékes hálózati elemek biztonsága

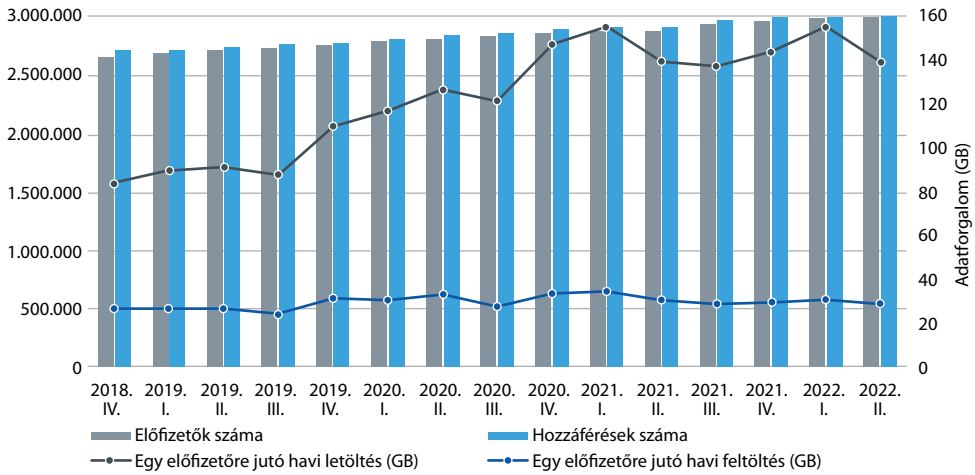
Amikor elektronikus információs rendszerek, infokommunikációs hálózatok (jelen cikk ezeket egymás szinonimájaként használja) biztonságáról beszélünk, legyenek azok vezetékesek vagy vezeték nélküliek, akkor a fent ismertetett CIA-elv alapján vizsgáljuk azokat. Manapság sok szervezet a felhasználókat közvetlenül kiszolgáló vezetékes hálózati elemeit vezeték nélküli hálózatokra cseréli, mivel a vezeték nélküli hálózatok könnyebben teszik lehetővé a számítástechnikai rendszereik elérését, kevesebb kábelt és csatlakozót igényelnek. Így tesznek a hírközlési szolgáltatók is, hiszen a vezeték nélküli internetelérés egyre nagyobb részarányt tesz ki a portfóliójukban. A mobilinternet növekedését mutatja az alábbi, 1. számú ábra.

[8] Muha 2015.




*1. ábra: Internetforgalmat bonyolított SIM-kártyák számának és fajlagos forgalmának alakulása szolgáltatási szegmensenként*
*Forrás: NMHH 2022b*

Ugyanakkor az NMHH felmérése szerint a helyhez kötött internetelérések száma és a rajtuk folytatott adatforgalom is növekszik, bár a mobilnál jelentősen lassabb ütemben. Ezt mutatja a 2. számú ábra.




*2. ábra: Lakossági helyhez kötött internet-előfizetések és -hozzáférések számának, valamint a fajlagos forgalomnak az alakulása*
*Forrás: NMHH 2022a*

A teljes hálózaton alkalmazott vezetékes technológiát sokkal biztonságosabbnak tartották, mint amikor vezeték nélküli rendszerelemeket is felhasználtak.[9] Köszönhetően azonban a fejlődő technológiáknak és a biztonsági előírásoknak, a vezeték nélküli hálózati részek megfelelően biztonságosnak tekinthetők, mint a vezetékesek, már amennyiben azok tartalmazzák az előírt biztonsági kontrollokat és megfelelően vannak konfigurálva. Ennek okán a biztonsági ajánlások, előírások vizsgálatakor azt láthatjuk, hogy a vezeték nélküli hálózati elemek biztonságára lényegesen több részletszabályt dolgoztak ki, mint speciálisan a vezetékesre.

A vezeték nélküli hálózati elemek biztonságára több ok miatt is nagyobb figyelmet fordítottak korábban. Egyrészt a vezeték nélküli hálózati elemekhez való hozzáférés nem igényel fizikai hozzáférést például egy hálózati csatlakozóhoz vagy kábelhez, mint a vezetékes hálózatok esetében. Másrészt a vezeték nélküli hálózati elemek a végfelhasználók és a hálózat közötti adatátvitelhez rádióhullámokat használnak, és ezeket a rádióhullámokat nem lehet például a vállalat működési területénél (például kerítés) megállítani. Ezért lehetséges, hogy valaki az épület mellett vagy a parkolóban ülve lehallgatja a vezeték nélküli hálózati kommunikációt, sőt adott esetben aktívan be is avatkozhat a hálózati forgalomba, így például akár manipulálhatja az ott található adatok tartalmát is. Márpedig ezeket sokszor a felhasználók nem ismerték, vagy nem foglalkoztak vele kellő mértékben.

Ugyanakkor a belső fenyegetések, a kívülről érkező célzott támadások, valamint a vállalati hálózatokhoz való fizikai hozzáférés megszerzéséhez pszichológiai manipulációt (ismert angol elnevezéssel: social engineering) és mérnöki módszereket is alkalmazó hackerek világában a hálózat vezetékes részének biztonságát is szem előtt kell tartani. Különösen igaz ez a hírközlési hálózatok hosszú, sok esetben utak mellett a földben elvitt vagy akár légvezetékes hálózati elemeire is. Éppen ezért érdemes megvizsgálni, hogy az elektronikus információs rendszerek egészére, valamint azok vezeték nélküli hálózati elemeire vonatkozó biztonsági előírások mellett milyen kifejezetten a vezetékes hálózati elemek védelmét szolgáló ajánlások, előírások léteznek, és azok a hírközlési szolgáltatók hálózatai esetében elégségesek-e a mai világban.

## *A tisztán vezetékes hálózati elemekkel kialakított hálózatok előnyei*

Megfelelő telepítés és konfigurálás esetén a vezetékes hálózati elemek megbízhatóságot és stabilitást nyújtanak. A hálózati elemek és a kábelezés (például optikai vagy Ethernet-kábelek) telepítése után a végeredmény egy rendkívül megbízhatóan működő rendszer lesz. Bár a vezeték nélküli kapcsolatok folyamatosan fejlődnek, a vezetékes hálózatok elérése általában stabilabb és megbízhatóbb. A vezetékes hálózatok azért is megbízhatók, mert a jelet nem befolyásolják a rádiós terjedési viszonyok. Ha például egymáshoz közeli, ugyanazon a csatornán működő wifihálózatok[10] vannak, az egyik

[9] NIST 2020.

[10] Wifi: Az engedély nélkül használható 2,4 és az 5 GHz-es frekvenciasávban működő vezeték nélküli helyi hálózat (WLAN) kialakítására szolgáló, széles körben elterjedt szabvány (IEEE 802.11).

jel zavarhatja a másikat, ami veszélyeztetheti a stabilitást. De ha a közelben reflexiót okozó tereptárgyak vannak, ez hatással van a vezeték nélküli kapcsolatra, míg a vezetékes hálózati kapcsolatot ezek a tényezők nem befolyásolják. Ezenkívül a vezetékes hálózatokban természetesen nem lép fel az ellátatlan területek problémája, amelyek a vezeték nélküli kapcsolatokban időnként a lefedettség hiánya vagy terjedési anomáliák miatt előfordulnak. Ez azért van így, mert minden egyes eszköznek a hálózathoz való csatlakoztatásához külön kábelt használnak, és mindegyik kábel – megadott hosszig – azonos sebességgel továbbítja az adatokat.

A vezetékes hálózatok másik előnye, hogy általában gyorsabbak, mint a vezeték nélküli hálózatok. Bár az adatsebesség folyamatosan javult a vezeték nélküli technológiák (például 5G hálózatok, a wifi 6[11] routerek, wifi mesh hálózatok) megjelenésével, ám jelenleg még mindig a vezetékes hálózaton érhető el nagyobb átviteli sebesség.

A harmadik említésre méltó előny a hozzáférés biztonsága. Illetéktelen felhasználó nem, vagy csak sokkal nehezebben tud csatlakozni egy tisztán vezetékes hálózathoz, mint vezeték nélküli technológiát is használó társához. Egy tisztán vezetékes hálózat ugyanis mind fizikailag (például kerítéssel, rácsok, őrség stb. alkalmazásával), mind logikailag (a szükséges, jól konfigurált biztonsági eszközökkel és alkalmazásokkal) jobban védett lehet az illetéktelen hozzáféréstől, mint egy vezeték nélküli elemekkel kiegészített hálózat. Ez utóbbi esetében gondoljunk például arra, hogy a wifihálózatok még a korszerű levegő interfész titkosító protokollt használva (például WPA2, WPA3) is könnyen hozzáférhetők.[12]

## *A vezetékes hálózati elemek hátrányai*

Elsőként megemlíthetnénk a mobilitás hiányát, ugyanis a vezetékes hálózatok rugalmatlanok a mobilitás szempontjából. Ahhoz, hogy a felhasználó az eszközt egy másik helyen használhassa, extra kábeleket és/vagy beállításokat kell használnia. Például egy vállalatnál használt rendszer biztonságának alapvető eleme, hogy adott portról csak adott (előre konfigurált) eszköz(ök) használhassa(k) a hálózatot, de egy hírközlési szolgáltató által fix helyre kiépített vezetékes szolgáltatás áthelyezése is sok időt és szolgáltatói közreműködést igényel.

A vezetékes hálózat telepítése hosszabb időt vehet igénybe és drágább, mivel több komponensre van szükség a folyamat befejezéséhez. Az infrastruktúra méretigényétől függően a telepítés hosszadalmas és összetett lehet, mivel ki kell építeni a kábelezést, és minden egyes eszközt fizikailag is csatlakoztatni kell a hálózathoz.

Egy tisztán vezetékes hálózat esetén nemcsak a kiépítés, hanem a karbantartás is költségesebb. Ráadásul a kábeleket véletlenül vagy akár szándékosan is el lehet vágni, ki lehet húzni stb.

[11] A wifiszabvány legújabb generációja a wifi 6, más néven 802.11ax, amely akár 4,8 gigabit/sec adatátviteli sebességet is lehetővé tesz.

[12] Khandelwal 2019.

### *Megállapítás a vezetékes hálózati elemekről*

Összességében megállapítható, hogy az előnyök és hátrányok mérlegelése mellett, elsősorban a költséghatékonyság és a javuló biztonság miatt a hírközlési szolgáltatók kínálatában is egyre terjednek a vezeték nélküli megoldások. Ugyanakkor a vezeték nélküli hálózati részekkel rendelkező hálózatok esetében is minden esetben vannak vezetékes részek, ráadásul ezek a hírközlési szolgáltatók hálózatában jellemzően nagy sebességű, nagy földrajzi kiterjedésű optikai hálózatokat is jelentenek. Így az infokommunikációs hálózatok esetében elmondható, hogy legtöbb esetben hibrid megoldással, azaz a két technológia kombinációjával találkozhatunk. A fent leírtak okán mindenképp érdemes elemezni a vezetékes hálózati elemekre vonatkozó biztonsági előírásokat, ajánlásokat, majd megvizsgálni, hogy ezek teljes mértékben elegendők-e a mai viszonyok mellett, vagy speciális, kifejezetten a vezetékes technológiát jobban védő kontrollokra is szükség van. Ennek teljes feldolgozása messze meghaladja jelen cikk kereteit, így a továbbiakban a főbb szabályzatok, ajánlások ismertetése következik.

## Vezetékes hálózati elemek biztonsági kontrolljainak önálló megjelenése a fontosabb jogszabályokban, ajánlásokban

Az elektronikus információs rendszerek biztonságával foglalkozó és konkrét kontrollokat előíró fontosabb jogszabályok és ajánlások áttekintése alapján elmondható, hogy ezek jórészt komplex megközelítéssel dolgoznak. Ez azt jelenti, hogy a biztonsági kontrollok úgy jelennek meg, hogy azok függetlenek attól, hogy a hálózatot vezetékes vagy vezeték nélküli módon valósították-e meg. Ez egyrészt teljesen érthető és helyes megközelítés. Másrészt viszont vannak, lehetnek olyan speciális elemek, különösen a hírközlési szolgáltatók hálózatában, amelyek csak vezetékes, vagy csak vezeték nélküli rendszerelemeknél jelentkeznek. Épp emiatt ezekben a jogszabályokban, ajánlásokban megjelennek olyan kontrollpontok is, amelyek kifejezetten vezeték nélküli vagy vezetékes hálózati elemekre vonatkoznak. Érdemes ezeket áttekinteni és megvizsgálni, vajon a kifejezetten vezetékes rendszerelemekre vonatkozó kontrollpontok elégségesek-e, megfelelnek-e a mai viszonyoknak.

## 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)[13] és a 41/2015. (VII. 15.) BM rendelet[14]

Az Ibtv. célja a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon védelme érdekében az elektronikus információs rendszereikben kezelt adatokra vonatkozóan

[13] 2013. évi L. törvény.
[14] 41/2015. (VII. 15.) BM rendelet.

a bizalmasság, a sértetlenség és a rendelkezésre állás követelményeinek érvényesítése. Ahhoz, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek zárt, teljes körű, folytonos és kockázatokkal arányos védelmét garantálni lehessen, a 41/2015. (VII. 15.) BM rendelet az osztályba sorolásnak megfelelő logikai, fizikai és adminisztratív védelmi intézkedések bevezetését írja elő. A kockázatarányosságot az elektronikus információs rendszerek biztonsági osztályba soroltatásával, valamint az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének meghatároztatásával érték el.

Az Ibtv.-ben az elektronikus információs rendszer fogalma igazodott 2019 elejétől a NIS irányelv hálózati és információs rendszer fogalmához, de úgy, hogy tartalmazza az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózatokat is.

A 41/2015. (VII. 15.) BM rendeletben kimondottan vezetékes hálózati elemekre nincsenek kontrollpontok, ugyanakkor vezeték nélkülire igen. A 3. számú mellékletben található kontrollpontot az alábbi, 1. táblázat tartalmazza.

*1. táblázat: Részlet a 41/2015. BM 3. mellékletéből*

| 1. | Sorszám | Intézkedés típusa | Alapelvek | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. | | | Bizalmasság | | | | Sértetlenség | | | | Rendelkezésre állás | | | |
| 3. | | | Biztonsági osztályok | | | | | | | | | | | |
| 4. | | | 2 | 3 | 4 | 5 | 2 | 3 | 4 | 5 | 2 | 3 | 4 | 5 |
| 112. | 3.3.10. | Hozzáférés ellenőrzése | | | | | | | | | | | | |
| 144. | 3.3.10.14. | Vezeték nélküli hozzáférés | 0 | X | X | X | 0 | X | X | X | 0 | X | X | X |

*Forrás: 41/2015. (VII. 15.) BM rendelet*

Az adminisztratív, fizikai és logikai biztonsági követelmények szöveges magyarázatát tartalmazó 4. mellékletben az alábbi, 2. táblázatban található példák olvashatók.

*2. táblázat: Részlet a 41/2015. BM 4. mellékletéből*

| Sorszám | Kategória | Példák az ellenőrzésekre |
|---|---|---|
| 1.2.4. | Technológiai eltérések | Példaként említi a vezeték nélküli kommunikációt, hogy az erre vonatkozó előírások csak akkor alkalmazandók, ha használják is. |
| 3.3.10.14. | Vezeték nélküli hozzáférés | Az alkalmazandó speciális biztonsági feladatokat írja le:<br>• szabályozás, technikai útmutató, valamint engedélyezési eljárás;<br>• hitelesítés és titkosítás;<br>• felhasználó konfigurálás tiltása;<br>• antennák;<br>tekintetében. |

*Forrás: 41/2015. (VII. 15.) BM rendelet*

A Nemzeti Kibervédelmi Intézet által kiadott *Felhasználói kézikönyv a 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez* című dokumentum[15] az alábbiakat tartalmazza a 3.3.10.14. számú kontrollpont vonatkozásában:

*3. táblázat: Részlet a Felhasználói kézikönyv A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez dokumentumból*

| Védelmi intézkedés sorszáma | Védelmi intézkedés megnevezése | Magyarázat, cél | Biztonsági osztály | | | Példa, előremutató gyakorlat, iparági legjobb gyakorlat, értelmezés |
|---|---|---|---|---|---|---|
| | | | B | S | R | |
| 3.3.10.14. | Vezeték nélküli hozzáférés | A Szervezet definiálja a vezeték nélküli hálózatra vonatkozó korlátozásokat, konfigurációs lehetőségeket és az engedélyezési eljárást. | 3 | 3 | 3 | A Szervezet az azonosításra és hitelesítésre vonatkozó eljárásrendben vagy az IBSZ-ben felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán (mint például UHF/VHF, 802.11x, and Bluetooth, wifi);<br>továbbá meghatározza az engedélyezési eljárást. |
| 3.3.10.14.2. | Hitelesítés és titkosítás | Az EIR-rendszerben hitelesítéssel és a forgalom titkosításával védik a vezeték nélküli hozzáférést. | 5 | 5 | 5 | Tanúsítvány alapú hitelesítés és forgalomtitkosítás használata a 802.11i szabvány szerint. |
| 3.3.10.14.3. | Felhasználói konfigurálás tiltása | Csak arra felhatalmazott – jogosultsággal rendelkező – felhasználó és csak vezetékes LAN-kapcsolatról végezhet bárminemű konfigurációs tevékenységet a vezeték nélküli hálózatot illetően. | 5 | 5 | 5 | Adminisztrációs célra szeparált, dedikált VLAN használata, amely VLAN-nak csak vezetékes végpontjai vannak, és csak ebből a VLAN-ból lehetséges a vezeték nélküli hálózat konfigurálása. |
| 3.3.10.14.4. | Antennák | A Szervezet olyan antennákat és árnyékolási megoldásokat alkalmaz, amelyek csökkentik a jelek észlelésének esélyét külső fél számára. | 5 | 5 | 5 | A legfelső biztonsági szinten szükség van speciális védelmi intézkedésekre, például az elektronikai felderítés elleni védelemre.<br>A jelek külső fél általi észlelésének az esélye csökkenthető:<br>- Az eszközök sugárzásának korlátozásával (természetesen csak ameddig nem veszélyezteti az elsődleges használati célját). A korlátozás lehet időbeli, térbeli vagy teljesítménybéli.<br>- Árnyékolási technikákkal. Jellemzően különböző fémezett szövetekkel oldható meg az árnyékolás.<br>A fentieken túl a legfelkészültebb iparágak (jellemzően a hadiipar) irányított antennákat, mobil antennákat vagy akár megtévesztő antennákat is használhatnak. |

*Forrás: Nemzeti Kibervédelmi Intézet 2021*

[15] Nemzeti Kibervédelmi Intézet 2021.

A 41/2015. (VII. 15.) BM rendeletben az egyetlen pont, ahol vezetékes hálózatot említik, az a következő:

> „3.10.14.3. Felhasználó konfigurálás tiltása
> Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását."[16]

Ám ebben a pontban is csupán említés szintjén jelenik meg és a védett hálózat részének tekinti a teljes vezetékes hálózatot.

Speciálisan a hírközlési szolgáltatók hálózatára és kifejezetten azok vezetékes hálózati elemeire külön utalás a 41/2015. (VII. 15.) BM rendeletben nem található.

A fentiekből megállapítható, hogy hazánkban jelenleg csupán a vezeték nélküli hálózatokra vannak speciális követelmények, kontrollpontok, a vezetékesre pedig nem, a hírközlési szolgáltatók esetében pedig specifikus követelményeket nem találunk.

## NIST 800-53

A NIST az Egyesült Államok legrégibb fizikai kutató laboratóriuma, amely ma a Kereskedelmi Minisztérium alatt, szövetségi ügynökségként dolgozik. A honlapjukon is közzétett küldetésük az, hogy támogassák az Egyesült Államok beruházásait és ipari versenyképességét olyan tudományok, szabványok és technológiák fejlesztésével, amelyek segítségével javul az ország gazdaságbiztonsága és az itt élő emberek életminősége. Elért eredményeiket számos területen kamatoztatják, így az egészségügyi nyilvántartásoktól kezdve az atomórákon és nanoanyagokon át a számítógépes chipekig számtalan termék és szolgáltatás használja a NIST által kidolgozott technológiákat, szabványokat. A szervezet meghatározó szerepet játszik az infokommunikációs rendszerekkel és azok biztonságával kapcsolatos szabványok és ajánlások kidolgozásában is.[17]

Ez utóbbi kapcsán a NIST számos dokumentumot készített, amelyek a kritikus biztonsági elemek azonosításában is segítenek. Az infokommunikációs rendszerekkel kapcsolatban megjelentetett dokumentumai közül a téma szempontjából kiemelendő kategóriák:

- NIST Special Publication 500 Series, amelyben a különböző szabványokhoz és referenciaarchitektúrákhoz kapcsolódó anyagokat teszik közzé;[18]
- NIST Special Publication 800 Series, amelyben a biztonsági kérdésekkel foglalkozó anyagok találhatók. A sorozat iránymutatásokat, ajánlásokat, műszaki előírásokat és éves jelentéseket tartalmaz a NIST kiberbiztonsági tevékenységeiről. Az SP 800 kiadványokat az Egyesült Államok szövetségi kormánya információi és információs rendszerei biztonságának és adatvédelmi igényeinek kielégítésére és támogatására fejlesztették ki;[19]

[16] 41/2015. (VII. 15.) BM rendelet.
[17] National Institute of Standards and Technology: www.nist.gov
[18] Lásd: www.nist.gov/system/files/documents/2018/08/07/SP500LIST_2005-present_GOOD-ONE-8.pdf
[19] Lásd: www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

- NIST Special Publication 1800 Series, amelyben praktikus, használható kiberbiztonsági megoldásokat mutatnak be.[20]

Ezek közül a cikk célkitűzése szempontjából a legfontosabb a NIST 800-53,[21] amely az információs rendszerek szervezetek által használandó biztonsági és adatvédelmi kontrollok egyfajta katalógusa.

A NIST 800-53 meghatározza a Federal Information Processing Standard (FIPS) által megkövetelt biztonsági ellenőrzések minimális alapszintjét is az összes egyesült államokbeli szövetségi információs rendszerre vonatkozóan (kivéve a nemzetbiztonsággal kapcsolatos rendszereket), de ajánlásként szolgál más szervezet, így más országok szervezetei számára is. A NIST 800-53 első változatát 2005-ben adták ki, jelenleg már az ötödik verziója, az úgynevezett rev5 van hatályban. [A korábban említett 41/2015. (VII. 15.) BM rendelet is a NIST 800-53-on, bár annak egy korábbi verzióján alapszik.] A NIST 800-53 amellett, hogy tartalmazza információs rendszerek különböző fenyegetések – a természeti katasztrófáktól az ellenséges támadásokig – elleni védeleméhez alkalmazható biztonsági és adatvédelmi kontrollokat, még a megfelelő védelem kialakításához szükséges kontrollok kiválasztásához, értelmezéséhez szükséges útmutatást is biztosítja a felhasználók számára. Az egyes szervezeteknek ugyanis a saját rendszereik és az azokban tárolt adatok ismerete és a felhasználás célja alapján kell kiválasztaniuk az alkalmazandó kontrollokat. Ehhez természetesen szükség van az általuk elvégzett gondos kockázatértékelésre és a lehetséges incidenseknek az információs rendszereikre gyakorolt hatásainak elemzésére.

A NIST 800-53 rev.5 több mint 100 kontrollpontot tartalmaz, amelyeket további kategóriákba soroltak a készítők. Ezeket az alábbi, 4. táblázat mutatja be:

*4. táblázat: NIST 800-53 kontrollkategóriái*

| ID | Kategória | Példák az ellenőrzésekre |
|---|---|---|
| AC | Hozzáférés-ellenőrzés | Fiókkezelés és -figyelés; legkisebb jogosultság elv betartása; a feladatok elkülönítése |
| AT | Tudatosság és képzés | A biztonsági fenyegetésekkel kapcsolatos felhasználói képzés; műszaki képzés a magasabb szintű jogosultsággal rendelkező felhasználók számára |
| AU | Ellenőrzés és elszámoltathatóság | Az ellenőrzési feljegyzések tartalma; elemzés és jelentéstétel; a feljegyzések megőrzése |
| CA | Értékelés, engedélyezés és felügyelet | Kapcsolódás nyilvános hálózatokhoz és külső rendszerekhez; behatolásvizsgálat |
| CM | Konfigurációkezelés | Engedélyezett szoftverpolitikák, konfigurációváltoztatás-ellenőrzés |
| CP | Vészhelyzeti tervezés | Alternatív feldolgozási és tárolási helyszínek; üzletmenet-folytonossági stratégiák; tesztelés |
| IA | Azonosítás és hitelesítés | A felhasználókra, eszközökre és szolgáltatásokra vonatkozó hitelesítési irányelvek; hitelesítő adatok kezelése |
| IP | Egyéni részvétel | Hozzájárulás és adatvédelmi engedélyezés |

[20] Lásd: www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information
[21] NIST 2020.

| ID | Kategória | Példák az ellenőrzésekre |
|---|---|---|
| IR | Incidenskezelés | Incidensreakció-képzés, felügyelet és jelentéstétel |
| MA | Karbantartás | Személyzet és eszközök karbantartása |
| MP | Médiavédelem | Hozzáférés, tárolás, szállítás és médiahasználat |
| PA | Adatvédelmi engedély | Személyes adatok gyűjtése, felhasználása és megosztása |
| PE | Fizikai védelem | Fizikai hozzáférés; vészhelyzeti áramellátás; tűzvédelem; hőmérséklet-szabályozás |
| PL | Tervezés | Közösségi média és hálózati korlátozások; mélységében védett biztonsági architektúra |
| PM | Programmenedzsment | Kockázatkezelési stratégia; belső fenyegetések elleni program; vállalati architektúra |
| PS | Személyi biztonság | A személyzet átvilágítása, megszüntetése és áthelyezése; külső személyzet; szankciók |
| PI | Személyes adatokkal kapcsolatos eljárások és átláthatóság | Személyes adatok kezelési eljárásának dokumentálása; kezelhető személyes adatok körének meghatározása; hozzájárulások kezelése |
| RA | Kockázatértékelés | Sérülékenységvizsgálat; adatvédelmi hatásvizsgálat |
| SA | Rendszerek és szolgáltatások beszerzése | Rendszerfejlesztési életciklus; beszerzési folyamat; ellátási lánc kockázatkezelése |
| SC | Rendszer- és kommunikációvédelem | Alkalmazások particionálása; határvédelem; kriptográfiai kulcsok kezelése |
| SI | Rendszer- és információintegritás | Hibaelhárítás; rendszerfelügyelet és riasztás |
| SR | Ellátási lánc kockázatmenedzsment | NIST-modellekre épülő szállítókkal vagy szervezetekkel való megfelelés |

*Forrás: NIST 2020*

A fenti kategóriákba tartozó kontrollpontok elemzésekor megállapítható, hogy a NIST 800-53 nem tartalmaz kifejezetten a vezetékes hálózatokra vonatkozó önálló kontrollpontokat, de a vezetékes hálózatot megemlíti az alábbi, 5. táblázatban szereplő pontokban:

*5. táblázat: Vezetékes hálózat említése a NIST 800-53-ban*

| Kontrollpont | Ellenőrzés neve | Leírás | Vezetékes hálózat említése |
|---|---|---|---|
| SC-5 | Denial-of-service védelem | Egy szolgáltatásmegtagadásos esemény számos belső és külső ok miatt bekövetkezhet, például egy ellenséges támadás vagy nem megfelelő tervezés miatt kialakuló kapacitás- és/vagy sávszélességhiány miatt. Ilyen típusú támadások a hálózati protokollok széles skáláján (pl. IPv4, IPv6) fordulhatnak elő. A szolgáltatásmegtagadási események keletkezésének és hatásainak korlátozására vagy kiküszöbölésére számos technológia, eszköz áll rendelkezésre. | A szervezet korlátozza az egyének azon képességét, hogy szolgáltatásmegtagadásos támadásokat indítsanak más rendszerek ellen. Ennek egyik része, hogy a szervezet korlátozhatja az egyének azon lehetőségét, hogy kapcsolódjanak és tetszőleges információkat továbbítsanak az átviteli közegen (pl. vezetékes hálózatokon). |

| Kontrollpont | Ellenőrzés neve | Leírás | Vezetékes hálózat említése |
|---|---|---|---|
| SC-43 | Felhasználási korlátozások | Használati korlátozások és megvalósítási irányelvek megállapítása a szervezet által meghatározott rendszerelemekre, valamint az ilyen komponensek használatának engedélyezése, felügyelete és ellenőrzése a rendszeren belül. | A felhasználási korlátozások többek között minden vezeték nélküli és vezetékes perifériakomponenst érintenek. A használati korlátozások és megvalósítási irányelvek a rendszerelemek által a rendszerben okozott károk potenciális kockázatán alapulnak, és segítenek biztosítani, hogy csak az engedélyezett rendszerhasználat történjen. |
| SI-4 | Rendszer-monitoring | A vezeték nélküli hálózatok alapvetően kevésbé biztonságosak, mint a vezetékes hálózatok, pl. lehallgatás ellen, ezért a vezeték nélküli hálózatból vezetékes hálózatba belépő forgalmat ellenőrizni kell. | A szervezet használjon behatolásérzékelő rendszert (intrusion detection system, IDS) a vezeték nélküli kommunikációs forgalom figyelésére, amikor a forgalom vezeték nélküli hálózatról vezetékes hálózatra halad át. |

*Forrás: NIST 2020*

Összességében a NIST 800-53 kapcsán is elmondható, hogy kifejezetten a vezetékes hálózatokra és főképp a hírközlési szolgáltatókra vonatkozó speciális kontrollokat itt sem találunk.

## ISO 27001

Az ISO/IEC 27001:2013[22] az a nemzetközi szabvány, amely keretrendszert biztosít az információbiztonsági irányítási rendszerek számára, hogy a szervezetek folyamatosan biztosítani tudják az információk és információs rendszerek bizalmasságát, sértetlenségét és rendelkezésre állását. Az ISO 27001 az egyetlen olyan információbiztonsági szabvány, amely alapján a szervezetek független auditált tanúsítást szerezhetnek. Ez szakértői biztosítékot nyújt a szervezetek számára, hogy az információbiztonságot a nemzetközi legjobb gyakorlatoknak megfelelően kezelik. A tanúsítás nem feltétlenül kell hogy az egész szervezetre vonatkozzon, akár egyes üzleti egységekre is lehet ilyen tanúsítást szerezni.

Az ISO/IEC 27002:2013 az ISO/IEC 27001:2013 szabványnak megfelelő ISMS[23] részekénti biztonsági ellenőrzések végrehajtására vonatkozó referencia. Az ISO 27001 előírja az ISMS specifikációját, beleértve a kockázatkezelési folyamatra vonatkozó követelményeket, amelyet a szervezet kockázatainak megfelelő biztonsági intézkedések kiválasztásához kell használnia.

A szabvány „A" mellékletében kaptak helyet azok a szabályzók, amelyek lefedik azon kontrollpontokat, amelyek fontos szerepet játszanak a szervezetek információbiztonságának megvalósításában. A szervezet az „Alkalmazhatósági nyilatkozatban" rögzíti, hogy mely kontrollpontoknak felel meg.

[22] Lásd: www.iso.org/isoiec-27001-information-security.html
[23] ISMS (information security management system) információbiztonsági irányítási rendszer (IBIR).

Az ISO 27002 keretrendszer az ISO 27001 „A” mellékletében felsorolt ellenőrzések alkalmazására vonatkozó bevált gyakorlatokra nyújt útmutatást. Támogatja az ISO 27001 szabványt, és azzal együtt kell olvasni, alkalmazni.

Az ISO kockázatkezelési keretrendszere is hasonló a NIST-éhez. A kockázatkezelést három lépésre bontják:

- a szervezet információit érintő kockázatok azonosítása;
- a kockázatnak megfelelő kontrollok kialakítása;
- a teljesítményük nyomon követése.

Az ISO 27001:2013 szabvány „A” melléklete 114 kontrollt sorol fel 14 ellenőrzési csoportra osztva, amelyek tartalmilag bővebben ki vannak fejtve az ISO 27002 szabvány 5–18. pontjai alatt.[24]

A 14 csoportot az alábbi, 6. táblázat ismerteti.

*6. táblázat: ISO 27 001:2013 ellenőrzési csoportjai*

| Ellenőrzési csoport | Leírás |
|---|---|
| A.5 Információbiztonsági irányelvek | Az információbiztonságot a szervezet legfelsőbb szintjéről kell irányítani, és az irányelveket világosan közölni kell az összes alkalmazottal. |
| A.6. Az információbiztonság szervezete | Az irányítási keretrendszernek támogatnia kell a szervezet információbiztonsági műveleteit, mind a szervezeten belül, mind azon kívül. |
| A.7. Személyi biztonság | Az alkalmazottaknak és az alvállalkozóknak tisztában kell lenniük a szervezet információinak védelmében betöltött szerepükkel a foglalkoztatás előtt és alatt. |
| A.8 Vagyonmenedzsment | A szervezeteknek azonosítaniuk kell fizikai és információs eszközeiket, és meg kell határozniuk az egyes eszközökhöz szükséges megfelelő védelmi szintet. |
| A.9 Hozzáférés-szabályozás | Az információkhoz és az információfeldolgozó eszközökhöz való hozzáférés korlátozása. Biztosítani kell a rendszerekhez és szolgáltatásokhoz való hozzáférést a jogosult felhasználók számára, és meg kell előzni a jogosulatlan hozzáférést. A felhasználókat elszámoltathatóvá tenni a saját felhasználói azonosságkezelési információik védelméért. Meg kell akadályozni a felhatalmazás nélküli hozzáférést rendszerekhez és alkalmazásokhoz. |
| A.10 Titkosítás | A kriptográfiára és a kriptográfiai kulcsok használatára vonatkozó szabályzatokat kell kidolgozni, és végre kell hajtani az információk titkosságának, integritásának és/vagy rendelkezésre állásának védelme érdekében. |
| A.11 Fizikai biztonság | Ellenőrzéseket kell bevezetni az információfeldolgozó létesítményekhez való illetéktelen fizikai hozzáférés, károsodás és zavarás megakadályozása érdekében. |
| A.12 Üzembiztonság | Az információkat és az információfeldolgozó létesítményeket védeni kell a rosszindulatú szoftverektől, az adatvesztéstől és a technikai sebezhetőségek kihasználásától. |
| A.13 A kommunikáció biztonsága | Az információkat védeni kell a hálózatokban és az információ továbbítása során, mind a szervezeten belül, mind azon kívül. |
| A.14 A rendszer beszerzése, fejlesztése és karbantartása | Az információbiztonságot az információs rendszerek teljes életciklusa alatt kell megtervezni és meg kell valósítani, így már a tervezés, fejlesztés, beszerzés során is. A tesztadatokat is védeni kell. |

[24] Lásd: www.itgovernanceusa.com/iso27002

| Ellenőrzési csoport | Leírás |
|---|---|
| A.15 Szállítói kapcsolatok | A szervezet minden olyan információs eszközét, amelyhez a beszállítók hozzáférnek, megfelelően védeni kell. |
| A.16 Információbiztonsági incidensek kezelése | Az információbiztonsági incidenseket következetesen és hatékonyan kell kezelni. |
| A.17 Üzletmenet-folytonossági menedzsment információbiztonsági szempontjai | Az információbiztonság folytonosságát be kell ágyazni a szervezet működésfolytonosság-irányítási rendszereibe. |
| A.18 Követelményeknek való megfelelőség | Az információkat úgy kell védeni, hogy azok megfeleljenek a jogi, törvényi, rendeleti és szerződéses kötelezettségeknek, valamint a szervezet irányelveinek és eljárásainak. |

*Forrás: Irwin 2023*

A kommunikációs biztonsággal, amelynek célja az információ védelme a hálózatokban, valamint annak továbbítása során, az A.13 melléklet[25] foglalkozik. Ebben a vezetékes és a vezeték nélküli hálózatokkal kapcsolatos releváns elemek a következők (7. táblázat).

*7. táblázat:Vezetékes és vezeték nélküli hálózatokkal kapcsolatos elemek*

| Kontrollpont | Leírás |
|---|---|
| **A.13.1 A hálózati biztonság menedzsmentje** | A hálózatban lévő információk és az azokat támogató információ-feldolgozó létesítmények védelmének biztosítása. |
| **A.13.1.1 Hálózati intézkedések** | A hálózatokat menedzselni kell, hogy védjük az információkat a rendszerekben és az alkalmazásokban. |
| **A.13.1.2 A hálózati szolgáltatások biztonsága** | Minden hálózati szolgáltatásra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és az irányítási követelményeket, beleértve a hálózati szolgáltatási megállapodásokat függetlenül attól, hogy ezeket a szolgáltatásokat házon belülről vagy kiszervezett formában nyújtják. |
| **A.13.1.3 Elkülönítés a hálózatokban** | A hálózati szolgáltatások, a felhasználók és az információs rendszerek csoportjait el kell különíteni a hálózatokban. |

*Forrás: Irwin 2023*

Az ISO/IEC 27001 és az ISO/IEC 27002[26] egyaránt felülvizsgálat alatt áll, előreláthatólag 2022 közepe táján jelennek meg a változások. Várhatóan azonban nem lesz ISO/IEC 27001:2022 név alatt új kiadás, hanem egy módosítást adnak ki ISO/IEC 27001:2013+A1:2022 néven.

Az egyik fő változása az lesz, hogy az „A" melléklet hivatkozik az ISO/IEC 27002:2022 szabványban szereplő kontrollokra, amely tartalmazza az adott kontroll címét és a kontrollt magát. Amíg az ISO/IEC 27002:2013 114 kontrollt tartalmaz 14 területen, az átdolgozás után az ISO/IEC 27002:2022 93 kontrollt tartalmaz majd 4 területen.

Összességében az ISO/IEC 27001 kapcsán is elmondható, hogy speciálisan a vezetékes elemekre vonatkozó kontrollok nem jelennek meg, és kifejezetten a hírközlési szolgáltatókra vonatkozó speciális kontrollokat pedig itt sem találunk.

[25] Lásd: https://infocerts.com/iso-27001-annex-a-13-communications-security/
[26] Lásd: www.iso.org/standard/75652.html

## Összefoglaló, tanulságok

A vezetékes és vezeték nélküli hálózatok nagy kiterjedése és összetettsége kihívást jelent a biztonsági szakemberek számára. Igaz ez a hírközlési hálózatokra is. A releváns, már konkrét kontrollokat is tartalmazó hazai jogszabályok és angolszász ajánlások áttekintését követően elmondható, hogy ezek komplex megközelítést alkalmaznak és jellemzően szervezetek saját információs rendszereinek védelmére fókuszálnak. Ennek megfelelően jellemzően csupán az egyébként biztonsági szempontból több figyelmet követelő vezeték nélküli szakaszokra, rendszerelemekre kerültek be speciális kontrollok, speciálisan a vezetékes hálózati elemek védelmére szolgáló kontrollokkal nem igazán lehet találkozni. Mint ahogy a hírközlési szolgáltatók infrastruktúra-elemeinek védelmét szolgáló speciális kontrollokkal sem, bár hazánkban az Ibtv. elektronikus információs rendszernek tekinti ezeket is, amelyeket ugyanazon elvek szerint, ugyanazon kontrollok segítségével szükséges védeni.

Ha megnézzük, hogy ma milyen veszélyek fenyegetik, fenyegethetik a hírközlési szolgáltatók vezetékes rendszereit, rendszerelemeit, akkor azt látjuk, hogy széles a paletta. Az optikai kábelek munkálatok (például építés vagy mezőgazdasági tevékenység) közbeni elvágásától az optikai kábelek meghajlításával való információkicsatolásig széles a skála. Éppen ezért célszerű tovább vizsgálni és felmérni, hogy milyen veszélyek fenyegetik pontosan a hírközlési szolgáltatók nagy kiterjedésű vezetékes rendszereit, rendszerelemeit, ezek mekkora problémát okozhatnak a szolgáltatóknak és a felhasználóknak, majd amennyiben szükséges, ajánlásokat, kontrollokat fogalmazni meg ezek kivédésére, enyhítésére.

## Irodalomjegyzék


Irwin, Luke (2023): ISO 27001 Annex A controls explained. IT Governance, 2023. január 6. Online: www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Khandelwal, Swati (2019): Security Flaws in WPA3 Protocol Let Attackers Hack WiFi Password. *The Hacker News,* 2019. április 10. Online: https://thehackernews.com/2019/04/wpa3-hack-wifi-password.html

Kovács Zoltán (2021): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest: Ludovika.

Muha Lajos (2015): *A kritikus információs infrastruktúrák védelme.* (h. n.): Relnet Technológia Kft. Online: http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf

NIST (2020): *NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations.* (h. n.): National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53r5

NMHH (2022a): *A Nemzeti Média és Hírközlési Hatóság helyhez kötött piaci jelentése.* 2018. IV. – 2022. II. negyedév. Nemzeti Média- és Hírközlési Hatóság. Online: https://nmhh.hu/dokumentum/234021/helyhez_kotott_piaci_jelentes_2018_negyedik_2022_masodik_negyedev.pdf

NMHH (2022b): *A Nemzeti Média és Hírközlési Hatóság mobilpiaci jelentése.* 2018. IV. – 2022. II. negyedév. Nemzeti Média- és Hírközlési Hatóság. Online: https://nmhh.hu/dokumentum/233271/mobilpiaci_jelentes_2022_elso_felev.pdf

## *Jogi források*

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

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

Nemzeti Kibervédelmi Intézet (2021): *Felhasználói kézikönyv* a 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez. 2021. december. Online: https://nki.gov.hu/wp-content/uploads/2021/12/Felhasznaloi-kezikonyv-vedelmi-intezkedesekhez-v1.0.pdf