CTI jelentés

Kiberbiztonsági fenyegetések és kihívások 2030-ig

Az ENISA Identifying Emerging Cyber Security Threats and Challenges for 2030 című kiadványa nyomán

1996

Fortes fortuna adiuvat

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

enisa

Tartalomjegyzék

Bevezetés

Jelen CTI jelentés az ENISA (Európai Unió Kiberbiztonsági Ügynöksége) *Identifying Emerging Cyber Security Threats and Challenges for 2030* című, 2023 márciusában publikált kiadványa, valamint a kiegészítésének szánt, felülvizsgálatot tartalmazó jelentések nyomán készült.

A kiadványokban az ENISA 6. számú stratégiai célkitűzése jelenik meg, mely szerint az ENISA célja, hogy előrejelzést nyújtson az új és jövőbeli kiberbiztonsági kihívásokról, ezáltal pedig növelje a tagállamok és az egyéb érdekelt felek kiberbiztonsági tudatosságát.

Az ügynökség a cél elérése érdekében a saját, 2021-ben kidolgozott, jövőkutatásokon alapuló keretrendszerét alkalmazta. A keretrendszert egy interdiszciplináris szakértői csoporttal együttműködve hozták létre, amelyben többek között futuristák, szociológusok, üzleti vezetők és kiberbiztonsági szakértők vettek részt. A keretrendszer átfogó küldetése, hogy betekintést nyújtson a jövőbe, és gazdagítsa a különböző szakmájú és hátterű szakértők közötti párbeszédet.

Tekintettel arra, hogy az Európai Unió **védelmének kulcsa a jövőre való felkészülés**, a konkrét célkitűzés az, hogy azonosítsa és összegyűjtse a 2030-ra várhatóan megjelenő kiberbiztonsági fenyegetéseket, amelyek hatással lehetnek az Unió infrastruktúrájára és szolgáltatásaira, valamint az európai társadalom és a polgárok digitális biztonságának megőrzésére irányuló képességére. Az ENISA – és ezzel együtt az NKI – szándéka az, hogy az érintett feleket új ismeretekkel vértezzük fel, amelyekkel megkezdhetik a jövőbeli fenyegetések elleni küzdelmet.

A projekt fő célközönsége a kiberbiztonság területén érdekelt felek, köztük a nemzeti kiberbiztonsági hatóságok, nemzeti és uniós döntéshozók, szakértők és nem utolsó sorban a gyakorlati szakemberek.

Újonnan megjelenő kiberbiztonsági fenyegetések 2030-ig

A jelentésben azonosított és rangsorolt veszélyek között számos olyan téma jelenik meg, amelyek már ma is aktuálisak. A tanulmány arra a következtetésre jutott, hogy ezek a fenyegetések még 2030-ban is sürgető problémát fognak jelenteni, ugyanakkor jellegük megváltozik, mivel mind inkább függő helyzetbe kerülünk ezen technológiáktól, valamint egyre inkább elterjedtebbek lesznek a mindennapok során is.

Módszertan

Az ENISA a PESTLE (*Political, Economic, Social, Technological, Legal and Environmental* - politikai, gazdasági, társadalmi, technológiai, jogi és környezeti) területek releváns szakértőivel 2022 márciusa és augusztusa között tartott műhelybeszélgetések és interjúk sorozatán keresztül 21 olyan veszélyt **azonosított** és **rangsorolt**, amelyek előfordulása 2030-ra növekedni fog.

Az alkalmazott módszertan négy szakaszból áll:

1 Együttműködő feltárás

A trendkutatás és az információgyűjtés olyan szakasza, amely integrálja a szakértői tudást, a visszajelzéseket és a validálást.

2 Előrejelző csoportok workshopja

A PESTLE egyik dimenziójában tapasztalattal rendelkező szakértők csoportjait gyűjtik össze, hogy tovább vitassák, feltárják, értékeljék és rangsorolják az azonosított trendeket.

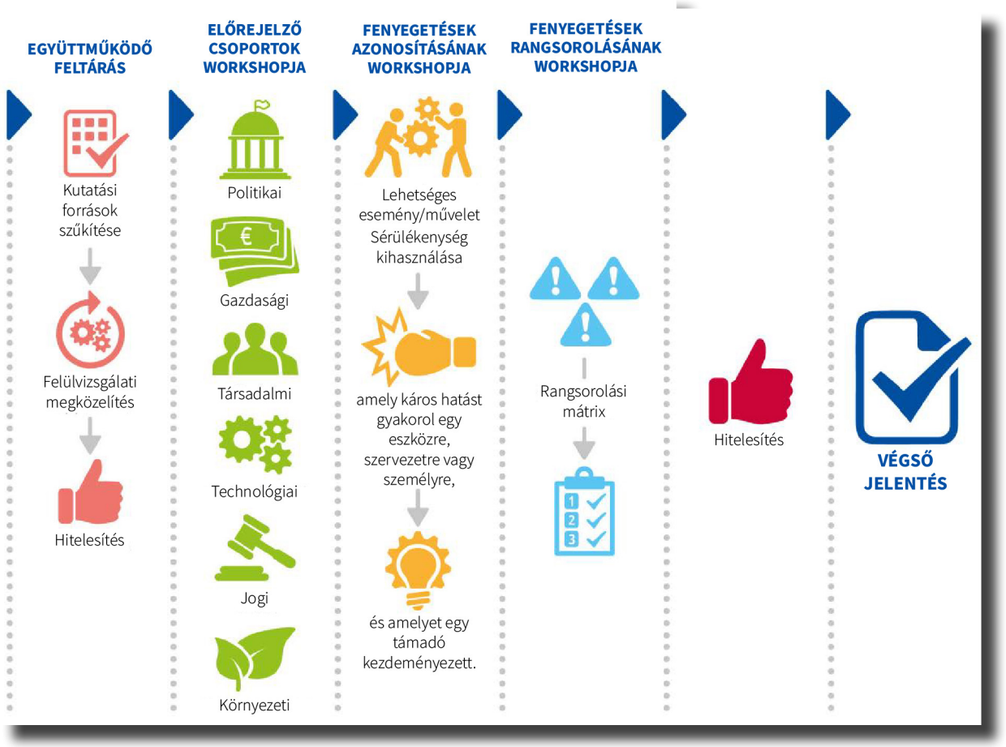
3 A fenyegetések azonosításának workshopja

A következő 10 évben felmerülő kihívások azonosítására a „Threat casting" módszertant használják. Ez gyakorlatban azt jelenti, hogy a kiberbiztonsági szakértők kis csoportjai olyan forgatókönyveket kapnak, amelyekben megjelennek a rangsorolt kiberfenyegetettségi trendek. A forgatókönyvek pusztán a fenyegetésekkel kapcsolatos tartalom közvetítésére szolgáló médiumként szolgálnak.

A csoport a forgatókönyvet **személyiségek kialakításával** és egy **rövid, fantáziadús sci-fi esszé megírásával** tárja fel. A szakértők ezután ellenséges perspektívát vesznek fel, hogy a leírt jövőben feltárják a potenciális fenyegető szereplőket és a sebezhetőségeket. Ez a perspektívaváltás lehetővé teszi a csoport számára, hogy megállapítsa az ellenfél motivációit és meghatározza a lehetséges fenyegetéseket.

4 A fenyegetések rangsorolásának workshopja

Ebben a szakaszban egy rangsorolási mátrixot használnak, amelyben a fenyegetések a **valószínűség**, a **hatás**, az **újdonság** és az ENISA által **korábban közzétett fenyegetések** alapján kaptak pontszámot.



1. ábra
A módszertan folyamatának áttekintése
Forrás: ENISA Identifying Emerging Cyber Security Threats and Challenges for 2030
Az ábrát fordította a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete.

A fenyegetések leírása

Összesen **21 fenyegetés** került azonosításra, melyek közül az első **10 legnagyobb hatású** fenyegetés kerül részletesen ismertetésre. A módszerek leírására során az ENISA fenyegetés taxonómiájára hivatkoznak, mely alapján az alábbi magas szintű kategóriák kerültek megállapításra: (szándékos) fizikai támadás, (nem szándékos) információ vagy IT-infrastruktúra károsodás/veszteség, (természeti) katasztrófa, meghibásodás, kiesés, lehallgatás, rosszindulatú tevékenység és jogi jellegű fenyegetések.

1. Az ellátási láncok szoftverfüggőségeinek kompromittálása

A vízió szerint 2030-ra egyre több új termékben lesz több komponens és szolgáltatás integrálva. Mivel a piac gyors termékkiadási ciklust követel, így a komponensalapú programozás várhatóan erőteljesen növekedni fog, mely a kódok újrafelhasználásához, valamint a nyílt forráskódú kódkönyvtárak használatához fog vezetni. Ez újszerű és előre nem látható sebezhetőségekhez vezethet, ami több lehetőséget teremt a rosszindulatú szereplők számára, hogy beszállítói és vevői oldalról veszélyeztessék az ellátási láncot, mivel a támadók manipulálhatják ezeket a szoftverfüggőségeket és a fejlesztői eszközöket „back door"-ok hozzáadásával a kódkomponensekhez.

A támadók számára a legegyszerűbb módszer a **nyílt forráskódú könyvtárak manipulálása**. Az ilyen módon kompromittálódott szoftverek elterjedése – esetlegesen akár állami szereplők által – rendkívül széleskörű támadásra ad lehetőséget.

2. Fejlett dezinformációs / befolyásolási műveletek

2030-ban a nem állami szereplők – bűnözői csoportok, bérhackerek stb. – valószínűleg rendelkeznek majd a technológiai képességekkel (pl.: deepfakes), mellyel képesek lehetnek közösségeket is sikeresen manipulálni.

Míg a deepfake technológia alkalmazása a bűnözői csoportok és egyének pénzügyi meggazdagodását szolgálja elsődlegesen, addig a hamis személyazonosságok segítségével folytatott dezinformációs kampányok elsődleges motivációja (geo)politikai jellegű, így elsősorban állami szereplők és más politikai motivációjú szereplők fogják végrehajtani. A deepfake technológiák alkalmazásához már szinte korlátlanul elérhetőek a megfelelő adatforrások – videók, képek, hangfelvételek – és a biometrikus arcképek **különösen sebezhetők** a morfológiai támadásokkal szemben, így a fenyegető szereplők rendkívüli pontossággal **képesek megszemélyesíteni a célpontokat**.

Mivel már olyan fejlett arcok is létrehozhatók, amelyek az emberi szem számára már megkülönböztethetetlenek a valódi arcoktól, így olyan valósághű avatárok hozhatók létre a közösségi médiában (részletesen kidolgozott és adatokkal feltöltött profilokkal együtt), amelyek túlmutatnak a jelenlegi közösségi média botokon. A jövő botjai viszont **hatékonyan fogják befolyásolni** a választásokat és a közbizalmat, hitelességüket pedig csak növelni fogja, hogy videókat is tömegesen képesek lesznek megosztani magukról. Fontos stratégiai célkitűzés, hogy az **uniós szakpolitika felkészüljön** a dezinformáció kezelésére, a hatáscsökkentésre és az ilyen típusú incidensek kezelésére.

3. A magánélet elvesztése – A digitális megfigyelés önkényuralma

A jelenlegi tendencia azt mutatja, hogy a bűnüldöző szervek egyre gyakrabban azonosítják a bűnözőket olyan technológiák segítségével, mint a helymeghatározás, nyilvános kamerák felvételei, valamint az arcképfelismerés. Ezen technológiák hatásfoka folyamatosan növekszik, így ez a jövőben arra ösztönözheti az államokat és a magánszereplőket, hogy tovább növeljék a technológia használatát. Egyre inkább terjedőben van a fokozott **digitális felügyelet az internetes platformokon** is, valamint megjelentek a **digitális személyazonosságok** is.

Ezen adathalmazok lehetővé teszik a bűnüldöző- és kormányzati szerveknek a potenciális gyanúsítottak nyomon követését, ugyanakkor ezek az adatbázisok is könnyen válhatnak bűnözői csoportok célpontjává, mivel ezen szenzitív adatok jól értékesíthetők online. További nehézségeket okoz, hogy esetenként egyes technológia szolgáltatásokat – például arcfelismerés – nem az állami szolgáltatók, hanem piaci szereplők biztosítják, akik nem felelnek meg az adatvédelmi és biztonsági követelményeknek. A digitális megfigyelés térhódítása tehát kettős veszélyt rejt magában: lehetőséget biztosít a kormányzati szereplők részére az **egyének totális megfigyelésére** és fontos célpontként jelenhetnek meg az **adatok a feketepiaci szereplők részére**.

4. A kiber-fizikai ökoszisztémában megnövekszik a sérülékeny, elavult rendszerek és az ehhez kapcsolódó emberi hibák száma

2030-ban várhatóan az IoT már szinte teljes mértékben áthatja a közlekedési, az energia- és vízhálózati, valamint az ipari infrastruktúrát a hatékonyság növelése és az intelligens döntéshozatal javítása érdekében. Ezen túlmenően jelentősen meg fog nőni az átlagos felhasználókhoz társított okoseszközök száma (2021-ben már egy átlagos ember 7 okoseszközzel rendelkezett). Emiatt rendkívül **nehézzé válhat az összes eszköz karbantartása és kezelése**, különösen biztonsági szempontból. Ráadásul az okoseszközök gyártói valószínűleg sikertelenek lesznek a végfelhasználók oktatásban az eszközök karbantartásának szükségessége vonatkozásában.

Az IoT gyors elterjedése és a növekvő készséghiány 2030-ra a kiber-fizikai ökoszisztéma megértésének rovására fog menni, ami az IT és OT biztonsági karbantartási problémákhoz fog vezetni, amelyek a félrekonfigurálásból, a késedelmes karbantartásból és a megszűnő IoT-szoftverek életciklusának nem megfelelő végtámogatásából adódnak. Mindezt nehezítheti, hogy egyes célzott támadások kifejezetten **a javításokat terjesztő szervereket vehetik célba**, hogy ezzel is **megzavarják a tervezett frissítéseket**.

Példa lehet egy ilyen támadásra az alábbi szituáció: a régebbi OT berendezések kézikönyvei online elérhetőek, így a támadó csoportok át tudják tanulmányozni őket a rendszerben lévő sebezhetőségek felkutatása végett. Amint találnak ilyet, a támadók már a felhasználói eszközöket és az üzemeben használt egyéb IoT-eszközöket veszik célba. Ezáltal a kiberbűnözők **fontosabb ipari infrastruktúrákat vehetnek célba**.

5. Okoseszközök adataival megtámogatott célzott támadások (zsarolóvírusok)

2030-ra az összegyűjtött viselkedési adatok mennyisége exponenciálisan nőni fog, valamint a különféle okoseszközök használata a mindennapi életünkben szintén jelentősen fog nőni. Veszélye abban rejlik, hogy az élet minden területéről gyűjtenek ezek az eszközök adatokat, melynek eredményeképpen egyedi és rendkívül pontos viselkedési profil állítható fel a felhasználóról. Az összegyűjtött adatok közé tartozhatnak (többek között) a viselhető eszközökből és orvosi berendezésekből származó **egészségügyi adatok**, vagy az **intelligens otthonokban található IoT-eszközök**, amelyek információkat gyűjtenek az otthoni viselkedésről, a mozgásadatokról vagy az online platformokon jellemző viselkedésről. Az eszközök mennyisége, valamint a végfelhasználói tudatosság hiánya miatt itt is fennáll annak veszélye, hogy ezekről az eszközökről származó adatokat felhasználják célzottan, például a felhasználó viselkedési profiljához illeszkedő, testreszabott social engineering támadásokhoz.

Az egyre kifinomultabb social engineering támadások kihívások elé állítják majd a végfelhasználókat, a bűnüldöző szerveket és a kormányokat egyaránt, mivel **újabb megelőzési módszereket kell találni** az ilyen jellegű támadásokra, valamint a hitelesítések javítására.

6. Űr-alapú infrastruktúrák (teljes körű) ellenőrzés alatt tartásának hiánya

A 2010-es évektől kezdődően egy új korszak kezdődött az űrutazásban is, amikor egyre több magáncég jelent meg a piacon – sokszor csatlakozva az állami szereplőkhöz -, hogy felfedezzék a világegyetemünket. 2030-ra az űrágazat valószínűleg még tovább fejlődik, mivel a magánvállalatoknak egyre több beruházásuk lesz, ráadásul egyre inkább kötnek partnerséget a kormányokkal. Mindezt pedig csak fokozza a világűrben zajló geopolitikai és kereskedelmi verseny. Az ágazat gyors növekedés számos kulcsfontosságú szolgáltatást tesz majd lehetővé, és ugyan számos előrelépés történt biztonsági területen is, mégis a szakemberek aggályukat fejezték ki, hogy ez elegendő-e. Álláspontjuk szerint ugyanis biztonsági szempontból **nem megfelelő a világűrbe telepített infrastruktúra ellenőrzése**.

Egy kellően erős védelem kiépítése viszont elképzelhető, hogy túlságosan lassú folyamat lenne (pl. egy K+F projekt keretében), így **nem lehet felkészülni** a nulladik napi sérülékenységekre. Fennáll a veszélye annak, hogy a piac arra ösztönzi majd a magánvállalatokat, hogy felgyorsítsák a munkafolyamatokat, innováljanak és csökkentsék a költségeket a kiberbiztonság rovására. A magáncégek megpróbálhatják ezt arra használni, hogy szabotálják riválisaikat; a kormányok megpróbálhatják kihasználni a sebezhetőségeket, hogy **geopolitikai versenyelőnyt teremtsenek** a világűrben; a bűnözői csoportok pedig arra fogják használni a sebezhetőségeket, hogy **anyagi haszonszerzés** céljából zsarolják a vállalatokat, vagy akár **fizikai károkat okozzanak**. Mivel a világűrben a magán- és a közszféra infrastruktúrája keresztezi egymást, a támadók a magánszereplők, a kormányzati szervek vagy az infrastruktúrával kapcsolatba kerülő egyének elleni támadással szerezhetnek kezdeti hozzáférést a világűrbe telepített infrastruktúrához.

Mivel a kormányok és a társadalmak nagymértékben **függnek a műholdaktól** (pl. GPS), az államilag támogatott támadók és a felbérelhető hackerek az ellátási láncot érintő támadások révén próbálnak majd kezdeti hozzáférést szerezni a hardverhez, és olyan technikákat alkalmaznak, amelyekkel fenntarthatják jelenlétüket az űrinfrastruktúrán belül - beleértve a bázisállomásokat is.

A bázisállomások olyan adó-vevőkészülékek, amelyek a műholdakat egy központi földi csomóponthoz kötik, amely azokat egy hálózathoz kapcsolja. Ezek az állomások kulcsfontosságú elemet jelentenek, amelyeket a támadók **szolgáltatásmegtagadási támadásokkal** vesznek célba, hogy megzavarják a kritikus katonai és polgári rendszereket. A támadók a rendelkezésre álló technikákat a védelmi és észlelési **mechanizmusok kijátszására használják**, de mindaddig lappangva maradnak, amíg stratégiailag nem hajtják végre a támadást, például egy konfliktus során, a hibrid hadviselés eszközeként.

7. Fejlett hibridfenyegetések terjedése

2030-ra a kibertámadások még kifinomultabbá válhatnak, és fizikai vagy offline támadásokkal párosulhatnak majd. A támadási módszerek folyamatosan fejlődnek, és gyakran párhuzamosan, illetve egymást követően kombinálják őket céljaik elérése érdekében. Ezeket a hibrid műveleteket összetettségük és az egyes támadásokat külön-külön kezelő tendencia miatt **nehezebb felderíteni és védekezni ellenük**. Az új működési móddal az észlelőeszközöknek nagyobb korrelációs képességekre van szükségük, beleértve a látszólag egymástól független események összekapcsolását is. Ezért egyre nagyobb kihívást jelentenek a kormányok, a vállalatok és a polgárok számára egyaránt. A múltban a hibrid támadásokat elsősorban állami szereplők hajtották végre a hagyományos és a kiberhadviselés kombinációjaként.

A jövőben a hibrid fenyegetések még tovább fejlődnek és egyre több új technológiát alkalmaznak és kombinálják azokat. A támadók például egyre inkább a mesterséges intelligenciát és a mélytanulást is felhasználják majd, hogy képességeiket kombinálva **új, előre nem látott támadási módszerek létrehozására használják**. A támadók a kezdeti hozzáférés megszerzéséhez a technikák egyidejű kombinációját fogják használni, beleértve a nagy mennyiségű adatgyűjtést a spear phishing kampányok testre szabásához, a gépi tanulást az adatok értelmezéséhez, új eszközök kifejlesztését a védelmi mechanizmusok kijátszásához, valamint a fizikai és a virtuális eszközök kombinációját a támadások végrehajtásához.

Az okoseszközök, a felhőhasználat, a több online identitás és közösségi platform, valamint a kormányok által kiadott digitális azonosítók számának növekedésével a támadóknak **számos új terület** áll majd rendelkezésükre, amelyeket felhasználhatnak és kombinálhatnak kreatív támadási vektorok létrehozásához.

8. Készséghiány

A készséghiány jelenleg is hozzájárul a legtöbb biztonsági réshez, mely súlyosan érinti a vállalkozásokat, a kormányzatokat és a polgárokat. 2030-ra a készséghiány problémája nem oldódik meg. Bár a betöltetlen kiberbiztonsági munkahelyek számának növekedése mérséklődött, a készséghiány továbbra is **jelentős kockázatot jelent** majd a társadalom és a kormányok számára. Az egyik lényeges tényező, amely 2030-ban hatással lesz a fenyegetésre, a **szervezetek hajlandósága** (és erőforrásai) a személyzet bővítésére és a tehetségek fejlesztésére. A kiberbiztonsági funkciók megvalósítása is szenvedni fog a készségek és az általános érettség hiánya miatt, még akkor is, ha a hajlandóság megvan.

A kockázatot tovább növeli az új technológiák és a régi technológiák közötti kölcsönhatás, amelyre a munkaerő nem kapott megfelelő képzést - a régi technológiákra vonatkozó ismeretek nem alakulnak át elég gyorsan ahhoz, hogy a 2030-as kockázatot kezelni lehessen. Az örökölt készséghiányon felül az olyan új technológiák, mint az intelligens eszközök, a mesterséges intelligencia, az űralapú infrastruktúra vagy a kvantumszámítástechnika is új kiberbiztonsági kihívásokat jelentenek majd. A bűnözői csoportok olyan szervezeteket, intézményeket és vállalatokat fognak megcélozni, amelyekben sok a betöltetlen kiberbiztonsági álláshely, hogy megtalálják a sebezhetőségeket, és ezeket anyagi haszonszerzés céljából kihasználják.

A kiberbűnözők elemezni fogják a szervezeti készségeket és hiányosságokat, hogy betekintést nyerjenek a védelem gyengeségeibe, a potenciális sebezhetőségekbe és a rendszereik és hálózataik kihasználásának lehetőségeibe. A nyilvános álláshirdetések gyakran részletes információkat adnak arról, hogy egy vállalatnál vagy egy kormányzati ügynökségnél milyen készségekből van hiány, így a támadók betekintést nyerhetnek a lehetséges behatolási vektorokba.

Ezen túlmenően a támadók megpróbálnak nyílt- és zártforrású információkat szerezni, hogy szervezeti és hálózati információkat gyűjtsenek, és így kiszúrják az ismert sebezhetőségekkel rendelkező régebbi rendszereket. Például egy helyi erőmű az álláshirdetésében megoszthatja azt a terméktípust, amelyhez támogatásra van szükségük - ez bőséges időt biztosít a fenyegető szereplők számára a **termékspecifikus sebezhetőségek vizsgálatára**.

9. Határon átnyúló infokommunikációs szolgáltatók, mint támadási célpontok

2030-ban a technológiai összekapcsoltság megerősödik. A fizikai és a számítógépes határ még jobban elmosódik, mivel az olyan infrastrukturális ágazatok, mint a közlekedés, az egészségügy, az elektromos hálózatok és az ipar egyre inkább az infokommunikációs szolgáltatókra támaszkodnak az internethez való csatlakozás és az eszközök közötti kommunikáció kezelése terén. Bár a társadalom működésének fenntartásában való felelősségük már jelenleg is jelentős, ez 2030-ra még inkább megnő.

Az infokommunikációs szolgáltatók és infrastruktúrájuk - beleértve a műholdas technológiát is - **a társadalom gerincét alkotják**, ezért a meghibásodása jelentős hatással lehet rá. Az intelligens városok példázzák, hogy 10 év múlva még kritikusabbá válnak a működési hálózatok. Ezért ezek a szolgáltatók valószínűleg a kormányok, terroristák és bűnözői csoportok célpontjai lesznek. A sebezhetőségek kihasználásával vagy hibrid támadásokkal hozzáférést szerezhetnek hálózataikhoz, végpontjaikhoz, adatközpontjaikhoz vagy az infrastruktúra egyéb fizikai elemeihez, és ezzel **városokat és egész régiókat tehetnek tönkre**. Külföldi kormányok megpróbálhatják ezt felhasználni nemzetek destabilizálására, a terroristák pedig arra, hogy félelmet szítsanak, valamint politikai célokat érjenek el.

Az infokommunikációs infrastruktúrát valószínűleg fegyverként fogják használni egy jövőbeli konfliktus során. A szolgáltatóknak védekezniük kell majd az államilag támogatott, tartós és magasan fejlett támadások ellen, amelyeket vélhetően a kormányzati hírszerző ügynökségek is elkövethetnek.

10. Visszaélés a mesterséges intelligenciával

A mesterséges intelligencia már a kezdetektől fogva manipulálható, többek között a célzott tanítással az ellenfél támadásai révén. A mesterséges intelligencia tudattalan elfogultsága már jelenleg is aggodalomra ad okot, azonban 2030-ra az AI-algoritmusok és képzési adatok szándékos manipulálása már sokkal komolyabb veszélyt jelenthet, mivel az algoritmusokat úgy képezhetik, hogy hibás döntéseket hozzanak a magas kockázatú ágazatok tekintetében. A fenyegető szereplők megpróbálják majd kihasználni a mesterséges intelligencia alkalmazások erejét a **döntéshozatali eredmények alakítására** és a potenciális áldozatokról való információgyűjtésre.

Például manipulálhatják a képzési adathalmazokat, hogy **diszfunkcionális és káros AI-alkalmazásokat** hozzanak létre. A mesterséges intelligencia felhasználható az egyénekre vonatkozó tömeges adathalmazok átvizsgálására, hogy a róluk szóló adatpontokat korrelálják, mely képesség megléte a zaklató szoftverek számának növekedéséhez vezethet. A támadók továbbá bűncselekmények elkövetése céljából is felhasználhatják a mesterséges intelligenciát - például a felhasználói viselkedés elemzésére, hogy magasan fejlett spear phishing vagy hibrid kampányokat hozzanak létre.

Ezen felül a mesterséges intelligencia számos rosszindulatú tevékenység fokozására használható, például: dezinformáció és hamis tartalom létrehozására, elfogultságok kihasználására, biometrikus és egyéb érzékeny adatok gyűjtésére vagy esetleg adatmérgezésre.

További fenyegetések

A következő veszélyek szerepeltek a végleges prioritási listán, de az ENISA rangsorolási rendszer alapján nem kerültek be az első 10 közé, ugyanakkor relevanciájuk miatt mégis kiemelendők.

A digitális valutával támogatott kiberbűnözés növekedése

A kriptovaluták és széles körű piaci elterjedésük már most is lehetővé tette a szervezett bűnözés számára, hogy kiterjessze hatókörét. Mivel a digitális valuták befektetési eszközként és fizetőeszközként nagyon elterjedtek lesznek az európai piacokon, a szervezett bűnözés is képes lehet bővíteni a célpontjait. Ez azt jelenti, hogy a professzionális szolgáltatásokat (kibertámadásokat) kínáló kiberbűnözői csoportok a hatékonyság és eredményesség növekedése miatt jobban finanszírozhatók lesznek.

Az e-egészségügyi (és genetikai) adatok hasznosítása

A genetikai és egészségügyi adatok mennyisége 2030-ra óriási mértékben megnő. A nagyon érzékeny és/vagy genetikai információkat tartalmazó e-egészségügyi eszközök és adatbázisok sebezhetőségeit bűnözők kihasználhatják vagy felhasználhatják arra, hogy célba vegyék az egyéneket, vagy a kormányok a népesség ellenőrzésére, például a betegségeket és a genetikai sokféleséget felhasználva az egyénekkel szembeni megkülönböztetésre.

A deepfake ellenőrző szoftverek ellátási láncának manipulálása

2030-ra a deepfake technológiát még szélesebb körben fogják használni. A zaklatás, a bizonyítékok meghamisítása és a társadalmi zavargások előidézésének egyik formája lehet. Bár valószínűleg gyorsan beáramlanak majd az olyan ellenőrző szoftverek, amelyek videókat és hangokat elemeznek az emberek személyazonosságának ellenőrzésére, de a generált képek, videók és hangok minősége olyan szintre emelkedik, hogy a felhasználó képtelen lesz eldönteni, hogy valós vagy hamis információt látott. Ezek az ellenőrző szoftverek valószínűleg célpontjai lesznek mindazoknak, akik a deepfake-t illegális vagy etikátlan célokra kívánják felhasználni.

Kvantumszámítást alkalmazó támadások

2030-ban a kvantumszámítási erőforrások szélesebb körben elérhetővé válnak, ami lehetővé teszi a fenyegető szereplők számára, hogy a kvantumszámítást a nyilvános kulcsú kriptográfia meglévő alkalmazásainak megtámadására használják. Ez különösen releváns a jelenlegi digitális azonosítók esetében, amelyek aszimmetrikus kriptográfiát használnak a hitelesítéshez.

AI által megszakított/megerősített kibertámadások (avagy AI az AI ellen)

A mesterséges intelligencia-alapú eszközök eredményeként bekövetkező eszkaláció. A támadók mesterséges intelligencia-alapú technológiákat fognak használni a támadások indításához. Az ilyen támadások elleni védekezéshez, sőt az ellenintézkedések elindításához is szükség van a mesterséges intelligencia alapú védelmi eszközökre. A mesterséges intelligencia viselkedése ezekben az esetekben nehezen tesztelhető, mérhető és ellenőrizhető manuálisan vagy automatizáltan, de más mesterséges intelligencia felhasználása nélkül.

A javítatlan és elavult rendszerek kihasználása a túlterhelt ágazatközi technológiai ökoszisztémában

A "minden, mint szolgáltatás" olyan eszközök és szolgáltatások sokaságát eredményezi, amelyek mind a fogyasztók, mind a szolgáltatók részéről gyakori frissítéseket és karbantartást igényelnek. Mindez a készséghiánnyal együtt a sebezhetőségek nehezen kezelhető felületét jelenti, amelyet a fenyegető szereplők kihasználhatnak.

Rosszindulatú szoftverek beillesztése az élelmiszer-előállítási ellátási láncba

Az élelmiszertermelés fokozódó automatizálása és digitalizálása miatt az élelmiszer-ellátási láncokat számos, közepesen magas erőforrásokkal rendelkező fenyegető szereplő megzavarhatja.

A csomagolóüzemek elleni szolgáltatásmegtagadási támadások például megakadályozhatják az élelmiszeripari műveletek folytatását; a feldolgozott élelmiszereket előállító eszközök manipulálhatók, hogy megváltoztassák magának az élelmiszernek összetevőinek arányát. Az ilyen jellegű támadások élelmiszerhiányhoz, gazdasági zavarokhoz, legrosszabb esetben mérgezésekhez vezethetnek.

A blokklánc technológiák összeegyeztethetetlensége

2030-ig számos regionális alapú blokklánc-technológiát hoznak létre különböző kormánycsoportok, hogy kialakítsanak egy nemzetközi "aranyszabványt". Ennek hátterében az elmúlt években fokozódó blokklánc iránti társadalmi bizalomhiány áll. Minden technológiai csoport célja, hogy versenyelőnyre tegyen szert. Ez a blokkláncok technológiai inkompatibilitásának időszakát eredményezi, ami meghibásodásokhoz, üzemzavarokhoz, adatvesztéshez és a különböző blokkláncok interfészeinél lévő sebezhetőségek kihasználásához vezet. Ez kihívások elé állítja az ökoszisztémát és az adatvédelemi szakembereket, tovább fokozza a bizalmatlanságot, és negatívan befolyásolja a kereskedelmet és a GDP növekedését.

Zavarok a nyilvános blokkláncokban

A blokkláncot a társadalom szinte minden területén alkalmazni fogják 2030-ban. Sajnos a biztonsági szakértelem a blokklánc területén nem haladt előre jelentősen, ami számos sebezhetőséget teremtett, amelyeket a jövőben ki lehet használni. Ezáltal például a helyileg elérhetetlen blokklánc-technológiák meghiúsíthatják a szavazásokat, a különféle jogi ügyleteket vagy a különféle biztonsági rendszerekhez történő hozzáférést.

A természeti/környezeti zavarok fizikai hatása a kritikus digitális infrastruktúrára

A környezeti katasztrófák megnövekedett súlyossága és gyakorisága több regionális leállást okozhat. A kritikus infrastruktúra rendelkezésre állását fenntartó redundáns tartalék telephelyek is érintettek lesznek.

A vészhelyzeti reagáláshoz szükséges rendszerek manipulálása

A vészhelyzeti szolgálatokhoz kapcsolt érzékelők manipulálása túlterhelhetik a mentők, tűzoltók és a rendőrség rendszereit. Ezek a fals hívások a rendszer túlterhelésével előidézhetik a rendszer teljes elérhetetlenségét is.

Az újraértékelés

A fentiek alapjául szolgáló kiadvány 2023. márciusában került publikálásra, azonban a kiberbiztonsági szektorban állandó a változás, így folyamatosan jelennek meg új fenyegetések és történnek új (összetettebb) incidensek. Emiatt szükséges az elemzés rendszeres időközönként történő megismétlése, hogy figyelembe lehessen venni a fenyegetések változását és az általános társadalmi változásokat. Sok esetben az egyes fenyegetések előfordulási valószínűsége és relevanciája **hirtelen változhat** különféle innovációk, társadalmi változások és más előre nem látható események miatt. Ezért ajánlott egy olyan folyamat meghatározása és végrehajtása, amely a felmerülő veszélyek listájának vezetésére és a fenti jelentésben bemutatott veszélyek figyelemmel kísérésére szolgál.

Maga az ENISA is elvégezte ezt az ismételt elemzést a Foresight Cybersecurity Threats for 2030 című kiadványának második kiadásában. Fontos kiemelni, hogy a fent közölt potenciális fenyegetések rangsorolásra kerültek az összesített pontszámok alapján (hatás, valószínűség, újdonság, korábbi publikálás). A 2023. szeptemberi és a 2024. március frissítésben nem változtak meg a lehetséges fenyegetések, ugyanakkor a sorrendben **jelentős változások** történtek.

Például a 15. helyen lévő „*A javítatlan és elavult rendszerek kihasználása a túlterhelt ágazatközi technológiai ökoszisztémában*" nevű fenyegetés a lista 4. helyére került, valamint a 20. helyen lévő „*A természeti/környezeti zavarok fizikai hatása a kritikus digitális infrastruktúrára*"nevű fenyegetés a lista 10. helyére került. További érdekesség, hogy a 8. helyről a növekvő készséghiány, mint fenyegetés, a 2. helyre került.

A változásokat a mellékelt táblázat foglalja össze:

	2023. szeptember	2024. március
1	SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES	SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES
2	ADVANCED DISINFORMATION CAMPAIGNS	SKILL SHORTAGES
3	RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY	HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBERPHYSICAL ECOSYSTEMS
4	HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBERPHYSICAL ECOSYSTEMS	EXPLOITATION OF UNPATCHED AND OUT-OF-DATE SYSTEMS WITHIN THE OVERWHELMED CROSS-SECTOR TECH ECOSYSTEM
5	TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA	RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY
6	LACK OF ANALYSIS AND CONTROL OF SPACEBASED INFRASTRUCTURE AND OBJECTS	CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE
7	RISE OF ADVANCED HYBRID THREATS	ADVANCED DISINFORMATION CAMPAIGNS
8	SKILL SHORTAGES	RISE OF ADVANCED HYBRID THREATS
9	CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE	ARTIFICIAL INTELLIGENCE ABUSE
10	ARTIFICIAL INTELLIGENCE ABUSE	PHYSICAL IMPACT OF NATURAL/ ENVIRONMENTAL DISRUPTIONS ON CRITICAL DIGITAL INFRASTRUCTURE
11	INCREASED DIGITAL CURRENCY-ENABLED CYBERCRIME	LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS
12	EXPLOITATION OF E-HEALTH (AND GENETIC) DATA	TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA
13	TAMPERING WITH DEEPFAKE VERIFICATION SOFTWARE SUPPLY CHAIN	INCREASED DIGITAL CURRENCY-ENABLED CYBERCRIME
14	ATTACKS USING QUANTUM COMPUTING	MANIPULATION OF SYSTEMS NECESSARY FOR EMERGENCY RESPONSE
15	EXPLOITATION OF UNPATCHED AND OUT-OF DATE SYSTEMS WITHIN THE OVERWHELMED CROSS-SECTOR TECH ECOSYSTEM	TAMPERING WITH DEEPFAKE VERIFICATION SOFTWARE SUPPLY CHAIN
16	AI DISRUPTING / ENHANCING CYBER ATTACKS	AI DISRUPTING / ENHANCING CYBER ATTACKS
17	MALWARE INSERTION TO DISRUPT FOOD PRODUCTION SUPPLY CHAIN	MALWARE INSERTION TO DISRUPT FOOD PRODUCTION SUPPLY CHAIN
18	TECHNOLOGICAL INCOMPATIBILITY OF BLOCKCHAIN TECHNOLOGIES	EXPLOITATION OF E-HEALTH (AND GENETIC) DATA
19	DISRUPTIONS IN PUBLIC BLOCKCHAINS	ATTACKS USING QUANTUM COMPUTING
20	PHYSICAL IMPACT OF NATURAL / ENVIRONMENTAL DISRUPTIONS ON CRITICAL DIGITAL INFRASTRUCTURE	DISRUPTIONS IN PUBLIC BLOCKCHAINS
21	MANIPULATION OF SYSTEMS NECESSARY FOR EMERGENCY RESPONSE	TECHNOLOGICAL INCOMPATIBILITY OF BLOCKCHAIN TECHNOLOGIES

2. ábra
A rangsor változása

A 2024 márciusi publikáció alapjául szolgáló felülvizsgálat során alkalmazott módszertan a valós idejű Delphi felmérés technikájának és egy tematikus workshopnak a kombinációja volt. A 24 szakértő részvételével online végzett, valós idejű Delphi-felmérés eredményeként felülvizsgálták a tíz legnagyobb kiberbiztonsági fenyegetést. A szakértők a különböző fenyegetések **hatásával és valószínűségével** kapcsolatos értékelésekkel járultak hozzá, átfogó képet nyújtva a kiberbiztonsági helyzetről. A felülvizsgált tízes listát a résztvevő szakértők által adott hatás- és valószínűségi pontszámok szorzata alapján állították össze.

Felkészülés a jövőre

A jelentésben bemutatott kiberbiztonsági fenyegetések 2030-ig **jelentős kihívásokat jelentenek** majd mind az Európai Unió, mind pedig tagállamai számára. Az előrejelzés alapján a fenyegetések egy része jelenleg is ismert, azonban azok súlyossága, jellege és komplexitása az elkövetkező években jelentősen változhat. E változásokra való felkészülés kulcsfontosságú a biztonság fenntartásában és a potenciális károk minimalizálásában. A folyamatos újraértékelés és a szakértők közötti együttműködés lehetővé teszi az érintett felek számára, hogy proaktív intézkedéseket tegyenek, így biztosítva az infrastruktúrák, szolgáltatások és állampolgárok digitális biztonságát. Az Európai Uniónak és tagállamainak folyamatosan fejleszteniük kell képességeiket, hogy hatékonyan reagáljanak a dinamikusan változó fenyegetési környezetre.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025