Medvácz Ádám

Kiberbiztonság a szoftverfejlesztésben: amerikai szabályozási modellek és kihívások

Military and Intelligence CyberSecurity Research Paper
2025/1.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

BEVEZETÉS

A kiberbiztonság jelentősége az utóbbi években egyre inkább előtérbe került, különösen a digitális szolgáltatások és a szoftverfejlesztés területén. Az Amerikai Egyesült Államok kiemelt figyelmet fordított arra, hogy reagáljon a kibertérből érkező egyre összetettebb és gyakoribb fenyegetésekre. A digitális világ rendkívül gyors fejlődése miatt a szoftverek biztonsága kulcsfontosságúvá vált mind a magánszektorban, mind az állami szférában. A globális gazdaság és társadalom egyre inkább függ a szoftverektől, a hálózatoktól, így elengedhetetlenné váltak a hatékony kiberbiztonsági intézkedések.
Az Egyesült Államok időben felismerte a terület fontosságát. Reagálva a kihívásokra számos szabályozást vezetett be annak érdekében, hogy növelje a szoftverek kiberrezilienciáját és erősítse az informatikai rendszerek biztonságát. Az amerikai szabályozási környezet különös figyelmet fordít arra, hogy a szoftverfejlesztési életciklus minden szakaszában érvényesüljenek a kiberbiztonsági követelmények. A tervezéstől kezdve a fejlesztésen át egészen az üzemeltetésig és a támogatásig.
A dolgozat áttekinti az Amerikai Egyesült Államok kiberbiztonsági szabályozásának főbb elemeit, amelyek közvetlen hatással vannak a szoftverfejlesztésre. Kiemelt figyelmet kapnak a szabályozásnak a szoftvergyártókra, forgalmazókra és fogyasztókra gyakorolt hatásai, továbbá a magán és állami szféra kockázatkezelési gyakorlatainak sajátosságai.
A dolgozat célja átfogó képet nyújtani a szabályozási megközelítésről. Az elemzés középpontjában áll, hogyan törekszik az Egyesült Államok a kiberbiztonság megerősítésére a digitális termékek és szolgáltatások terén. Külön hangsúlyt fektetek a kiberreziliencia jelentőségére, a gyártói felelősség növelésére és a fogyasztói tudatosság erősítésére, valamint az iparági szabványok fejlődésére.

I. A SZABÁLYOZÁS RENDSZERÉNEK ELEMZÉSE AZ AMERIKAI EGYESÜLT ÁLLAMOK VONATKOZÁSÁBAN

Napjainkban a kibertér egyre jelentősebb szerepet tölt be az országok védelmi stratégiájának kidolgozásában. Jelen dolgozat vizsgálódási fő szempontjában az Amerikai Egyesült Államok hatályos kiberbiztonsági szabályozási rendszere és stratégiái állnak a szoftverek vonatkozásában. A kiindulópontot a Cybersecurity Framework adja, amely az egyik legfontosabb kiberbiztonsági irányelv a kormányzati szervek és egyéb piaci szereplők számára a kiberbiztonsági kockázatok kezeléséhez. A National Institute of Standards and Technology[1] célja a Cybersecurity Framework megalkotásával összefüggésben egy önkéntes és rugalmas rendszer kialakítása volt, amely segíti az állami szervezeteket és kritikus infrastruktúrákat a kiberbiztonsági kihívások kezelésében. A kihívások kezelése érdekében fontos megvizsgálni a

[1] NIST

szoftverek tekintetében a szabályozási rendszert, ugyanis kihatással van a szoftvercégek ellátási láncainak biztonságára. A szabályok kihatással vannak továbbá az ipari szabványokra a kibertámadások elkerülése érdekében. A szabályozásnak kiemelt szerepe van a kritikus infrastruktúrák és az amerikai gazdaság védelmében. A szoftverek vonatkozásában különösen kiemelendő az említett keretrendszer, ugyanis kiemelten hangsúlyozza a szoftverek és azok komponenseinek fejlesztése során alkalmazandó bevált módszereket, mint például a biztonsági alapú tervezést.[2]

A szabályozási keretrendszer vonatkozásában tapasztalható volt a preventív jellegű védekezés kialakítása Donald Trump első elnökségének ciklusa alatt is.[3] Lényegesebb azonban megvizsgálni Joe Biden elnöki ciklusának stratégiai változásait. Az említett stratégiai irányvonalat a 2023-as Nemzeti Kiberbiztonsági Stratégia foglalja össze, amely felváltotta a korábbiakban alkalmazott Donald Trump által eszközölt 2018-as kiberbiztonsággal kapcsolatos „előretörő védekezésre" irányuló stratégiát. A 2023-as Nemzeti Kiberbiztonsági Stratégia a Védelmi Minisztérium 2018-as stratégiai kiegészítésének tekinthető összességében, amely a minisztérium közreműködését szabályozta a rosszindulatú szoftverek azonosításával és a kockázatos tevékenységek megszakításával.[4]

A Joe Biden elnöksége alatt kidolgozott kiberbiztonsági stratégia egy olyan digitális jövőt kíván megalapozni, amelynek lényeges eleme a rugalmas együttműködésre épülő, az emberi jogokat és alapvető szabadságjogokat hatékonyan védő rendszer.[5]

II. Az amerikai kiberbiztonsági stratégia pilléreken nyugvó rendszere

A rendkívül gyorsan fejlődő technológia napjainkban a kiberbiztonság célzott és összehangolt működését követeli meg. A hatályos stratégia elemzése során elsődlegesen megállapítható az átgondolt feladatmegosztásnak való megfelelés szükségessége. A stratégia alapvető kérdéskörei több pilléren nyugszanak, amelyek biztosítják az átgondolt és szakszerű feladatvégzést, valamint a szabályszerű környezet megteremtését.

Alapvető irányként hangsúlyozza a stratégia azt, hogy a digitalizált ökoszisztéma irányításának azokra a szervezetekre kell átkerülnie, amelyek megfelelnek a feltételeknek a biztonság és az ellenálló képesség biztosításához a közszférában és a magánszférában egyaránt.[6] A megfelelő beruházások összpontosítása érdekében továbbra is törekszik az Egyesült Államok vezető szerepének biztosítására a rugalmas és virágzó digitális jövő terén.[7]

---

[2] Cyber Defense Agency: It's time to build cybersecurity into the design and manufacture of technology products
[3] Krizsán Bence.: Az Amerikai Egyesült Államok új Nemzeti Kibervédelmi Stratégiája
[4] Divyanshu Jindal, Mohammed Soliman: The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?
[5] Roberta Freeman: White House releases National Cybersecurity Strategy
[6] Gerhard Peters, John T. Woolley.: FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy Online
[7] Jindal, Soliman: i. m.

A vizsgálandó rendszer 5 fő pillérből áll. Fontos szempontként kezelendő a pillérek vonatkozásában a kibertérben betöltött szerep jelentőségének és az ezzel kapcsolatos felelősség rendezésének szükségessége. A stratégia rendszerének vizuális ábrázolását a következő ábra tartalmazza.[8]

Ábra: Saját készítésű ábra az Amerikai Egyesült Államok kiberbiztonsági stratégiájának alapján.

1. Pillér	2. Pillér	3. Pillér	4. Pillér	5. Pillér
A létfontosságú infrastruktúrák védelme.	**A fenyegető szereplők akadályozása és működésük megszüntetése.**	**A piaci erők alakítása a biztonság és a reziliencia előmozdítása érdekében.**	**Befektetés egy reziliens jövőbe.**	**Nemzetközi partnerségek kialakítása a közös célok elérése érdekében.**

Fontos kiemelni azt a szabályozási folyamatot, amely már a 2023. évi stratégia elkészítését megelőzően is aktív szabályozási törekvéseket foglalt magában a kiberbiztonság vonatkozásában. A létfontosságú infrastruktúrák[9] szoftveres működtetése központi kérdést jelent számos ország vonatkozásában. A stratégia célja ennek értelmében a sebezhetőségek csökkentése. A piaci erőknek a stratégiában említett átalakítása a hatékonyság és innováció érdekében történik, ellenben ez a tevékenység növeli a kiberbiztonsági kockázatot is. Elsőként érdemes megemlíteni a kormányzat tevékenységét a kibertér és a digitális ökoszisztémánk biztonsága érdekében.

Az IoT Cybersecurity Improvement Act of 2020[10] teremti meg a kiindulópontot annak vonatkozásában, hogy iránymutatások és szabványok alapján vizsgálják felül az ügynökségek információbiztonsági elveit és szabályzatait. Ez összefüggésben áll a korábbi 2014-ben kiadott A Federal Information Security Modernization Act[11] rendelkezéseivel, amely előirányozta a szövetségi ügynökségeknek és azok beszállítóinak egy alapos kiberbiztonsági rendszer kidolgozását. Ennek értelmében a törvény előírja, hogy a NIST szabványokat és iránymutatásokat dolgozzon ki az IoT eszközök biztonságára vonatkozóan. Példaként említhető a NIST által meghatározott minimális biztonsági követelmények vonatkozásában a jelszóvédelmi előírások és a firmware frissítések jelentősége. A szövetségi ügynökségek vonatkozásában kötelezővé váltak olyan biztonsági protokollok, hogy az alkalmazott IoT-eszközök megfeleljenek a NIST szabványainak. Gyakorlati vonatkozásában ezzel csökkent a

[8] NCSI Plan Version 2
[9] Ide tartoznak az energiahálózatok, a vízellátás és a pénzügyi szektor.
[10] Az internet tárgyainak kiberbiztonságát javító törvény
[11] Szövetségi információbiztonsági korszerűsítési törvény

sebezhetőségi felületek száma a kormányzati hálózatokban. A Cybersecurity Improvement Act javította továbbá a szoftvergyártók kiberbiztonsági gyakorlatát. A szövetségi ügynökségekhez történő beszállítás esetén kötelesek megfelelni a NIST szabványainak. Ezzel elérhető a gyártók ösztönzése abban az aspektusban, hogy termékeikbe beépítsék a megkívánt funkciókat a megrendelések reményében. A gyártói oldal tekintetében kiemelendő, hogy a szövetségi kórházak és egyéb egészségügyi létesítmények széles körben alkalmazhatnak IoT-eszközöket. A Cybersecurity Improvement Act biztosítja, hogy az intézmények eszközei biztonságosak legyenek és ne férhessenek hozzá a támadók a betegek adataihoz.

Az 14028. számú végrehajtási rendelet[12] kiemelt jelentőséggel bír a téma vonatkozásában. A 2021. május 12-én kiadott, a kiberbiztonság javításáról szóló 14028. számú elnöki rendelet felhatalmazta a Nemzeti Szabványügyi és Technológiai Intézetet a kiberbiztonság fokozásával a szoftverellátási lánc biztonságával és integritásával kapcsolatos kezdeményezésekben. A rendelet eredményeként kiemelhető az irányelvek mellett a szövetségi ügynökségekkel kapcsolatos beszállítási követelmények szigorítása, amely a NIST tevékenységéhez köthető. A szoftverellátási láncra gyakorolt hatása a rendeletnek kimutatható a sebezhetőségi felületek csökkentésében, mivel a szoftverek fejlesztésére irányuló követelmények szigorításra kerültek. A transzparencia jegyében átláthatóbbá vált a rendszer a szoftverellátási lánc szereplői között, ugyanis a beszállítók és szövetségi ügynökségek együttműködése során visszakövethetőek a biztonsági ellenőrzés folyamatai. A felülvizsgálati és frissítési eljárások támogatni fogják a szoftverellátási lánc naprakészen tartását.[13] A rendelet 4. szakasza deklarálja azt a kötelezettséget a NIST tevékenységével összefüggésben, hogy a magánszektorral és közszektorral együttműködve határozzon meg megfelelő szabványokat, kiberbiztonsági gyakorlatokat és iránymutatásokat a szoftverellátási lánc biztonságának fejlesztése érdekében. A Nemzeti Szabványügyi és Technológiai Intézet konzultációt folytatott a Kiberbiztonsági és Infrastrukturális Biztonsági Ügynökséggel, amelynek következtében 2021-ben iránymutatást tett közzé a kritikus szoftverekre vonatkozó biztonsági intézkedésekről. A fogyasztóknak szóló kiberbiztonsági címkézési rendszer alapján a NIST 2022-ben kiadta álláspontját a fogyasztói címkézéssel kapcsolatos kritériumok kapcsán.[14] A NIST felülvizsgálta a fogyasztói szoftvertermékek kiberbiztonsági címkézésére irányuló kísérleti programokat. Megállapítást nyert, hogy a címkézést erőteljes fogyasztói felvilágosító kampánynak kell kísérnie a védett szoftverek népszerűsítése kapcsán. A címkéknek a fogyasztók számára a vásárlás előtt elérhetőnek kell lenniük fizikailag és digitális formátumban egyaránt.[15]

Jelentős válaszlépésként szolgált jelen rendelet a magánszektort és közszektort fenyegető kiberfenyegetésekkel szemben. Rögzítette a szövetségi kormányok fellépését a kiberbiztonsági fenyegetésekkel felmerülő események azonosítására, felderítésére és orvoslására. Alapvetően

[12] Executive Order 14028, Improving the Nation's Cybersecurity
[13] A Report to the President on Progress in Implementing Section 4 of Executive Order 14028 on Improving the Nation’s Cybersecurity 6.o. 12-13.o.
[14] Improving the Nation's Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order
[15]National Institute of Standards and Technolog :Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products 18-19. o.

itt rögzítésre került annak az együttműködésnek a szükségessége, hogy nem csupán kormányzati intézkedésekre van szükség a kiberbiztonsági rendszer kialakítása során. A digitális infrastruktúrába vetett bizalom kihangsúlyozásra került. Fontos megvizsgálni azt, hogy mennyire megbízható és átlátható egy infrastruktúra, valamint mi történik az infrastruktúrával abban az esetben, ha a bizalom meghiúsul egy adott termék okán. Ennek okán a szövetségi kormánynak megfelelő hatáskört kell biztosítania és jelentős erőforrásokat szükséges feláldoznia a számítógépes szoftverekkel kapcsolatos biztonságos keretrendszer kialakításához. Fontos ugyanis a kibertérben történő incidensek észlelése, értékelése, megelőzése. Alapvető szempont a nemzetgazdasági biztonság vonatkozásában is az információs rendszerek megfelelősége az alaposan kimunkált kiberbiztonsági szabványokhoz és követelményekhez.[16] A NIST ajánlása alapján a végrehajtási rendelet kezdeti szakaszán olyan önálló szoftverekre összpontosított, amelyek jelentős kár okozására voltak alkalmasak és biztonságkritikus funkciókkal rendelkeztek. Ezt követően a felülvizsgálati spektrum szélesedett a felhőalapú hibrid szoftverekre, a hozzáférést szabályozó szoftverekre, valamint az üzemeltetési szoftverkomponensekre.[17] Utalva a harmadik pillér második célkitűzésében található feladatok egy része folytatni kívánja az 14028. rendelet munkáját az IoT biztonsági címkézési program kidolgozásával a nemzet kiberbiztonságának javítása érdekében. Elősegítve a fogyasztókat azzal, hogy könnyebben összehasonlíthassák az előírt követelményeknek megfelelő esetleges szoftverek és egyéb informatikai eszközök biztonságát. Azonosítva így azokat, amelyek megfelelnek bizonyos biztonsági kritériumoknak.[18] Az IoT biztonsági címkézési program bevezette a címkézési irányelveket, amelyek az adott szoftver frissítési gyakoriságát és gyártói támogatás időtartamát tartalmazzák leglényegesebb elemként. További eredményként kiemelendő a fogyasztók tudatos döntéshozatalának elősegítése a címkézések vonatkozásában. A gyártók felelősségének vonatkozásában is szükséges megemlíteni a változást, ugyanis a címkézés követelményeinek elterjedésével nőtt a gyártói felelősség. Az amerikai kiberbiztonsági környezetre összességében megvizsgálva pozitív változásokat hozott a címkézési program. Növelte a kiberbiztonsági tudatosságot a fogyasztókban, másrészt növeli a piaci versenyt a szoftvercégek között.

Kiemelendő ezenfelül 2021. évi nemzetbiztonsági memorandum, amely a létfontosságú infrastruktúrák ellenőrző rendszereinek kiberbiztonságának javításáról rendelkezett. A nemzeti létfontosságú infrastruktúra védelme többek között az állam és az infrastruktúra tulajdonosainak közös felelőssége. Az infrastruktúrákat irányító rendszerek károsodása, megsemmisülése és hibás működése jelentős károkat okozhat az optimális működés kárára, ezzel fenyegetve az Egyesült Államok nemzeti és gazdasági biztonságát. A memorandum értelmében a kiberbiztonság és a nemzeti létfontosságú rendszerek ellenállásra képes működése elengedhetetlen. Megemlítésre került benne a létfontosságú infrastruktúrák kiberbiztonságú teljesítménycéljairól való rendelkezések előirányzása és az alapvető

[16] Executive Order on Improving the Nation's Cybersecurity
[17] Critical Software - Definition & Explanatory Material
[18] BORGIA, Michael; AUSTIN, Patrick: Overview of the National Cybersecurity Strategy

kiberbiztonsági célok rögzítése, amelyek minden létfontosságú ágazatban következetesen betarthatóak.[19]

A jelentőséggel bíró harmadik pillér a piaci erők átalakítása vonatkozásában bír kiemelt szerepkörrel a reziliencia és a biztonság aspektusaiban. Jelen pillér előtérbe helyezi a kiberbiztonsági szempontból gyengébbik félnek tekinthető szereplők védelmét és célként tűzi ki az IT-szektor vezető szereplőinek a felelősségi szempontú rendszer alapvető átszervezését a kockázatok csökkentése érdekében. Ezzel összefüggésben szükséges kiemelni a szoftvertermékek életciklusának és egyéb informatikai szoftveres szolgáltatások biztonságos fejlesztésének előmozdítását. Másodlagosan rendelkezik a magánélet fokozott védelméről és a személyes adatok biztonságos kezelésének előmozdításárol.[20]

III. A KIBERREZILIENCIA JELENTŐSÉGE A KIBERTÉRBEN BEKÖVETKEZŐ TÁMADÁSOK TEKINTETÉBEN

A Világgazdasági Fórum 2023-ban kiadott jelentésében a kiberbiztonsági kockázatok továbbra is állandó aggodalomra adtak okot. Jelentős kockázati tényezőnek minősítették a zsarolóvírusok elterjedését és a szoftverellátási láncokat célzó támadásokat. Továbbá a kockázati tényezők tekintetében 2024-ben további növekedés volt várható a technológiaalapú erőforrások és szolgáltatások vonatkozásában. Lényeges a rezilienca aspektusa, ugyanis kibertámadások kiemelt számban a pénzügyi rendszerekre és a kommunikációs infrastruktúra ellen irányulnak. A 2016-os Banglades Bank elleni kibertámadás példaként szolgál a kiberreziliencia hiányának illusztrálására. A támadás során a hackerek kártékony szoftverekkel fértek hozzá a bank rendszereihez, majd tranzakciókat indítottak meg. A támadók hamis üzeneteket küldtek más bankoknak a tranzakciók leplezésének érdekében. Az eset következtében jelentős pénzügyi károkat szenvedett a bank a naprakész kiberbiztonsági intézkedések hiányában.[21] A kommunikációs infrastruktúra elleni támadások testesítik meg a másik kiemelten fontos esetkört. Kiemelt esetként vizsgálható a Colonial Pipeline 2021-es kibertámadása, amely jelentős károkat és zavarokat okozott az amerikai olajellátásban. A kiberreziliencia jelen példában a kommunikációs és energetikai infrastruktúrák zavartalan működésének fenntartásában van jelentőséggel.[22] Az elmúlt évek statisztikai vizsgálata alapján megállapítható, hogy éves szinten 25% mértékű emelkedés következett be az amerikai kormány sebezhetőségi adatbázisában.[23]

A harmadik pillér részletes elemzését megelőzően azonban elengedhetetlen megvizsgálni a kiberreziliencia jelentőségét. A helyreállítással és a védelemmel kapcsolatban fontos kiemelni

[19] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
[20] Gerhard Peters, John T. Woolley.:i. m.
[21] Crooks Behind $81M Bangladesh Bank Heist Linked To Sony Pictures Hackers
[22] The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years
[23]Kerner, Sean Michael.: 35 cybersecurity statistics to lose sleep over in 2024, Utal: WORLD ECONOMINC FORUM-Global Risks Report 2023; Vulnerability and Threat Trends Report 2023

a kiberbiztonsági kockázat azonosítását, észlelését és az erre történő reagálást, amelynek alapjait a korábban kiemelt Cybersecurity Framework teremtette meg. A káros kihatású kibertérben történő események ugyanis jelentős befolyással lehetnek a szervezet további működésére. Ezzel összefüggésben problémák merülhetnek fel az adott szolgáltatással összefüggő rendelkezésre állás kapcsán, továbbá teljesen megszűnhet a munkamenet a hiányzó, vagy elérhetetlen adatok miatt a magánszektorban és a közszférában egyaránt. A kibertámadás bekövetkezésétől függetlenül a kiberbiztonság célja így leginkább a szervezetek megfelelő felkészültségének biztosítása a váratlan kibertámadások esetére. A szervezet belső működése képes legyen alkalmazkodni a kedvezőtlen körülményekhez és alkalmas legyen az ellenállásra a fenyegetésekkel szemben. Legszükségesebb esetben pedig képes legyen helyreállítani a belső rendszerének folyamatos működését.[24] A stratégia a kiberbiztonság javítása mellett az IT infrastruktúra modernizálását tűzi ki. Ezzel összefüggésben rendezni kívánja a tervezet a rendszerszintű kockázatokat és a legsürgetőbb biztonsági kihívásokat a meglévő szoftveres szolgáltatások és platformok megzavarása nélkül. Tulajdonképpen ez a tevékenység magában foglalja a digitális ökoszisztéma technikai alapjait is, amelyek sebezhetőségekkel rendelkeznek.[25] A reziliencia fejlesztése közelebbről megvizsgálva összefügg az IT-infrastruktúra folyamatos fejlesztésével. Az IT-rendszerek időszakos frissítése és korszerűsítése elengedhetetlen. Ennek vonatkozásában megfigyelhető a bizalmi elveket mellőző zero trust architecture.

A keretrendszer alapköve a bizalmatlanságra épül és a folyamatos ellenőrzést helyezi előtérbe. A zéró bizalom koncepció célja, hogy minimalizálja a bizonytalanságot. A hozzáférési kérelmeket folyamatosan ellenőrizni kell és alkalmazni kell a többfaktoros hitelesítést a biztonság érdekében. A felhasználók részére a legkevesebb hozzáférést származtatja a feladatelvégzéshez. Kiemelt jelentőséget kap a folyamatos ellenőrzési tevékenység. A zero trust architecture előnye a javított biztonsági helyzet a rendszerek ellenálló képességének vonatkozásában. Jelentősen kisebb az adatszivárgási kockázat is, ugyanis a folyamatos ellenőrzés csökkenti a jogosulatlan hozzáféréseket. Előnyként említhető meg az, hogy a bizalmi alapú megközelítéssel szemben a szervezetek képesek magukat jobban megvédeni és csökkenthető az adatszivárgás. [26] Ellenben a zero trust architecture implementálása bonyolult a hagyományos biztonsági modellekhez képest. Jelentős változtatásokat igényel a belső szervezetekben és fejlesztési folyamatokban, így gyakran nehezen alkalmazható a gyakorlatban ez a modell. A kiberreziliencia fejlesztése azonban elengedhetetlen célnak tekinthető, amelynek javításához szükség van rendszeres gyakorlatokra és szimulációkra. A kiberbiztonság aktív jellegére tekintettel szükséges az életszerű veszélyekre is felhívni a figyelmet laborgyakorlatokkal, akár szimulációkkal. Az előzetes szimulációk és laborgyakorlatok mellett kiemelendő a széles spektrumra kiterjedő adatelemzés jelentősége. Kiemelendő, hogy a különböző országok kiberbiztonsági gyakorlótereinek együttműködésére teremt lehetőséget.

[24] Bart Lenaerts-Bergmans.: What Is Cyber Resilience?
[25] Jindal, Soliman: i. m.
[26] NIST SP: 800-207 4.-8. o.

Ez magában foglalhatja a technikai infrastruktúra vonatkozásában a hálózatok és esetleges kiberbiztonsági megoldások integrálását.[27] Részletes vizsgálat következtében ugyanis nem jelenthet meglepetést a támadások valós időben történő visszaverése sem.[28]

A kiberreziliencia fejlesztése azonban elengedhetetlen célnak számít, amelynek javításához szükség van szabványoknak megfelelő gyakorlatokra és szimulációkra. Az Amerikai Egyesült Államok és más harmadik országok egyre nagyobb rendszerességgel rendeznek szimulációs gyakorlatokat, hogy felkészüljenek az esetleges támadásokra. Szimulációs példaként említhető az Egyesült Államok Storm szimulációs sorozata, amelyet az amerikai Belbiztonsági Minisztérium szervez meg rendszeresen. A kiberreziliencia fejlesztésével összefüggésben kiemelendő az automatizált rendszerek és a mesterséges intelligencia növekvő szerepe. Az AI alapú rendszerek képesek valós időben felismerni a potenciális fenyegetéseket, valamint ezzel összefüggésben gyors válaszreakciókat képesek adni. Az automatizált rendszerek egy része SOAR[29] technológia alapján működik, amelynek lényege a különböző biztonsági eszközök integrálása. A SOAR technológia kulcsszerepet játszik a kiberbiztonság terén. Lehetővé teszi a hatékonyabb reagálást a fenyegetésekre. A rendszer automatizálja és optimalizálja a biztonsági folyamatokat, csökkentve a válaszidőt és növelve a hatékonyságot a fenyegetésekkel szembeni harcban.[30]

IV. A KIBERBIZTONSÁGI STRATÉGIA HARMADIK PILLÉRÉNEK ELEMZÉSE ÉS KIHATÁSA AZ IPARI KÖRNYEZETRE

A harmadik pillér értelmében az amerikai kormányzat a piaci erők átalakítására törekszik a kiberbiztonsági felelősséggel összefüggésben. A nagyvállalatok a piaci erők behatására sem igyekeztek a megfelelő kiberbiztonsági gyakorlatok kialakítására. A stratégia azonban javaslatot tesz a szükséges óvintézkedések alkalmazására.

Alapvető elemnek tekinthető a biztonságos konfigurációs rendszer használata és az ágazati biztonsági előírások betartása. Ezenfelül alapos átvilágítás alá kell vetni a harmadik felektől származó komponenseket tartalmazó szoftvereket és egyéb eszközöket.[31] Ennek kapcsán szükséges a felelősséget a nagy behatással bíró adatgazdálkodók részére áthárítani a fogyasztónak minősülő felhasználókról.[32] A harmadik pillér elemzésének rendszerét a stratégiában megtalálható felosztás alapján végzem el. A harmadik pillér a piaci erők

[27]Szabó András (2018): TECHNIKAI KIBERBIZTONSÁGI GYAKORLATOK – NEMZETKÖZI KITEKINTÉS In: *HADMÉRNÖK*, XIII. Évfolyam 1. szám – 2018. március, NKE, Budapest.298. o.
[28] Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. In: Honvédségi Szemle – Hungarian Defence Review, Évf. 148 szám 5, Honvéd Vezérkar, Budapest. 16. o.
[29] Security Orchestration, Automation, and Response
[30]What is SOAR?
[31]Teske, David S. – Oh, Hyun Jai. Intellectual Property Advisory: New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable
[32] PERETTI, Kimberly Kiefer - BARTOLOTTA, Kristen: White House Releases National Cybersecurity Strategy

alakításának érdekében több lényeges célkitűzést emel ki, amelyet a következő ábra szemléltet.[33]

Ábra.: Az Amerikai Egyesült Államok kiberbiztonsági stratégiájának 3. pillérének célkitűzései

1. Az adataink kezelőinek elszámoltathatósága	2. A biztonságos IoT-eszközök fejlesztésének ösztönzése	3. A felelősség áthelyezése a nem biztonságos szoftvertermékekért és szolgáltatásokért	4. Szövetségi támogatások és egyéb ösztönzők felhasználása a biztonság beépítéséhez	5. A szövetségi közbeszerzés kihasználása az elszámoltathatóság javítása érdekében	6. A szövetségi kiberbiztosítási háttérintézkedés feltárása

A célkitűzések értelmében a kormányzat kiemeli a fogyasztók magánéletének és a személyes adatainak védelmét. Ennek megfelelően előtérbe kerülnek azok a jogalkotási erőfeszítések, amelyek szilárd, egyértelmű korlátokat szabnak a személyes adatok gyűjtésének, felhasználásának, továbbításának és a megőrzésének képességére. Ezenfelül a célkitűzésekben megállapított korlátok erősebb védelmet biztosítsanak az érzékeny adatok számára, valamint olyan jogszabályokat szorgalmaz, amelyek a Nemzeti Szabványügyi és Technológiai Intézet által kidolgozott szabványokkal és iránymutatásokkal összhangban nemzeti követelményeket határoznak meg a személyes adatok biztonságára vonatkozóan.[34]

Az első célkitűzés kiemeli az adatvédelem jelentőségét és ezzel összefüggésben irányul az adatok kezelőinek felelősségre vonására. Kimondott korlátokat határoz meg taxatíve ezen témakörben, amelyek többek között a személyes adatok gyűjtésére, felhasználására, továbbítására és az ezzel felmerülő karbantartásra tekintettel.[35] A NIST által kidolgozott szabványok és iránymutatások alapján a szilárd és egyértelmű korlátok közül kiemelendő a földrajzi helymeghatározás és az egészségügyi információk, hiszen jelentőséggel bírnak számos amerikai kritikus infrastruktúrában. A célkitűzés azért számít különös módon jelentősnek, ugyanis megteremti az összekapcsolódási pontot a kiberbiztonság és az adatvédelem között. Fontos kiemelni, hogy az említett stratégiának végrehajtással kapcsolatos kiegészítése jelen kérdésekről hiányosan rendelkezik.[36] Rendkívül nehéz olyan szabályozást kidolgozni a

[33] Saját készítésű ábra az Amerikai Egyesült Államok kiberbiztonsági stratégiájának alapján.: 36.-43. o.
[34] PERETTI, - BARTOLOTTA: i. m.
[35] LIAO, Annie,- JOHNSON, Rex :Summary of the 2023 National Cybersecurity Strategy Part 2.
[36] Eugenia Lostri, Stephanie Pell: The Biden Administration's Implementation Plan for the National Cybersecurity Strategy.

nagyvállalatok adatkezelésével összefüggő felelősségre, amely lehetővé teszi a kitűzött cél életképes megvalósítását.

A második célkitűzés középpontjában a biztonságos IoT- eszközök fejlesztése áll. Ennek kapcsán kiemelendő a korábbiakban említett IoT Cybersecurity Improvement Act of 2020 és az amerikai kormány címkézési programja[37]. Ezzel kapcsolatban érdemes kiemelni az IoT- eszközök hiányos kiberbiztonsági gyakorlatának kockázatát az ipari automatizációval összefüggésben. Problémaként merülnek fel legfőképpen a hiányosan védett, legtöbb esetben nem támogatott rendszerekkel működő eszközök hozzáférési kockázatai. Ezen gyenge biztonsági kiépítettséggel rendelkező eszközök könnyű támadási felületet biztosítanak a támadóknak a rendszer feletti uralom teljes átvételéhez, vagy lehetőséget teremt az adatlopásra. A DDoS támadásra hivatkozva jelentős károk okozhatóak egy adott ipari hálózat elérhetetlenné tételével, ami komoly pénzügyi veszteségeket és a szolgáltatókba vetett bizalom elvesztését eredményezheti. Problémaként merül fel továbbá az IoT eszközök vonatkozásában a biztonsági incidenskezelések mellőzése és a monitorozási feladatok felszínes elvégzése. Ez megalapozza azonban a támadások lassú észlelését és kivédésének csekély lehetőségét. Az említett problémák elkerülése érdekében szükséges egy olyan bevett belső gyakorlat kiépítése, amely folyamatos frissítésekkel, folyamatosan felülvizsgált hálózati hozzáférésekkel és egyéb intézkedésekkel minimalizálja a kiberbiztonsági kockázatokat. Az ipari IoT rendszerek esetében a biztonságkritikus alkalmazások esetében önmagában nem elegendő a megfelelő biztonsági és adatvédelmi mechanizmusok bevezetése. A hatóságok elvárhatják annak igazolását, hogy a rendszerek valóban az elvárt módszer alapján biztonságosan működnek. Azonban komplex feladat megvizsgálni, hogy egy ipari IoT-infrastruktúra megfeleltethető a meghatározott szabványokban található követelményrendszereknek.[38]

A második célkitűzés adminisztrációjából arra a következtetésre lehet jutni, hogy a napjainkban forgalomban és használatban lévő számos eszköz és szoftver nem rendelkezik megfelelő kiberbiztonsági védelemmel a kibertérben rejlő fenyegetésekkel szemben. Az amerikai kormányzat kötelezettséget vállal arra, hogy követi a korábbiakban alkalmazott folyamatokat a megkezdett címkézési programok továbbfejlesztését illetően, amelyről a korábbiakban említett 14028.[39] számú végrehajtási rendelet 4. szakasza rendelkezik. A táblázatban szereplő ötödik célkitűzésben a kormányzat a közszféra vonatkozásában továbbra is fenntartja, hogy a kiberbiztonság javításának eszközeként fogja használni a szövetségi kormányzatnak értékesítő szállítókra vonatkozó szerződéskötési követelményeket. A kormányzattal szerződéses jogviszonyban álló szervezeteknek nagy figyelmet kell fordítaniuk a biztonsági követelményekben bekövetkező szabályozási változásokra. [40]

[37] Cybersecurity Labeling for Internet of Things.
[38] Gebremichael T.; Et al.:"Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," in IEEE Access, vol. 8, pp. 152351-152366, 2020, 152351-152353. o., 152362. o.
[39] A nemzet kiberbiztonságának javításáról.
[40] PERETTI,- BARTOLOTTA: i. m.

A stratégia harmadik célkitűzésében a kormányzat megismétli annak szükségességét, hogy a felelősséget az amerikai állampolgárokról azokra a piacvezető vállalatokra és szervezetekre csoportosítsa át, amelyek megfelelő biztonság nélkül bocsátanak ki szoftvertermékeket és szolgáltatásokat.

Összegezve ez a fejezet a rosszul megírt kódokkal, valamint a helytelen biztonsági intézkedésekkel áll összefüggésben. Jelentőséggel bír továbbá a kormányzat álláspontja azzal kapcsolatban, hogy a szoftvereket gyártó vállalatok gondossági kötelezettséggel tartoznak a termékeiket használó vállalkozások, kritikus infrastruktúrák és a szoftvereket felhasználó fogyasztók felé.[41] Ezzel összefüggésben kiemelendő, hogy a kongresszussal és a magánszektorral együttműködve megkezdődött a jogszabályi környezet megalkotása a szoftvertermékekre és egyéb szolgáltatásokra vonatkozó felelősség vonatkozásában. Az 14028. végrehajtási rendelettel összefüggésben kiemelendőek a Nemzeti Szabványügyi és Technológiai Intézet megállapításai a kritikus szoftverekkel kapcsolatban a kiberbiztonsági stratégia végrehajtási folyamatának vonatkozásában. A NIST által meghatározott kategória alapján kritikus szoftvernek minősül minden olyan szoftver, amely egy vagy több olyan szoftverkomponenssel rendelkezik, amelyek példának okán bizalmi szempontból kritikus funkciók ellátására szolgálnak. Emellett megemlíti a felsorolás a minősített jogosultsági jelleg behatását, az adatokhoz való hozzáférés kérdéskörét, valamint a közvetlen hálózati hozzáférést számítástechnikai erőforrásokhoz. A kritikus szoftver definíciója minden olyan szoftverre alkalmazható, amelyet adott esetben a termelési rendszerek számára vásároltak, vagy telepítettek, illetve üzemeltetési célokra használnak. Magában foglalja ez az önálló szoftvereket, az egyes hardverkomponensek szerves részét kitevő szoftvereket, valamint a felhőalapú szoftvereket.[42]

Hangsúlyos elemként kezelendő, hogy az iparágnak és a kormányzatnak méltányos együttműködés alapján kell lefolytatni a piac hiányosságainak kijavítását és az amerikai társadalom legkiszolgáltatottabb tagjainak okozott károk bekövetkezésének minimalizálását. A stratégiai együttműködés szerinti megközelítés világszerte alkalmazható példát mutathat azoknak az országoknak, amelyek a politikai inputok szilárd mechanizmusának alapvető kialakítására törekednek. Ennek kapcsán a kiterjesztett együttműködési elv kulcsszerepet játszik. A második kiemelendő szempont az együttműködés mellett az SBOM[43] fejlesztésére és a továbbiakban a gyártók által már nem támogatott szoftverek kockázatának csökkentésére helyezi a hangsúlyt. Az SBOM a szoftverkomponensek átláthatóságának kialakításában jelentős szerepet játszik, ugyanis elősegíti a szervezetek számára a szoftver tartalmának részletes megismerését. Listaként szolgál a felhasznált könyvtárakról, modulokról. A Log4Shell sebezhetőség tökéletes példa arra, hogy milyen súlyos következményeket von maga után egy átláthatatlan szoftverkomponens.[44] A szoftverterv tágabb értelemben a

[41] PERETTI, - BARTOLOTTA: i. m.
[42] Critical Software - Definition & Explanatory Material.
[43] Szoftverterv- software bill of materials.
[44] NIST SP: 800-161r1, 89. o., 192. o., 303. o.

szoftverkomponenseket alkotó összetevők részletes listájának tekintendő. Kulcsfontosságú alapkövévé vált a szoftverbiztonságnak és a szoftverellátási láncnak. Az SBOM a célkitűzés vonatkozásában a nem támogatott szoftverekkel kapcsolatban felmerülő kockázatok mérsékléséhez kapcsolódik. Ezen folyamatba bekapcsolódva a CISA meghatározza a rendszerfejlesztési életciklus végső fázisban lévő szoftverek globálisan hozzáférhető adatbázisaira alkalmazandó követelményeket. Ezenfelül elősegíti a szoftvertervekkel foglalkozó közreműködők munkacsoportjainak működését.[45]

A stratégiai célkitűzések összegzéseként a szabályozásoknak teljesítményalapúnak kell lenniük. A jelenlegi politikai irányokkal és a jogszabályokkal összhangban álló módon kell felhasználni a meglévő kiberbiztonsági keretrendszereket és nemzetközi szabványokat. Szükség esetén törekedniük kell a határokon átnyúló szabályozási harmonizációra annak érdekében, hogy a kiberbiztonsági követelmények ne akadályozzák a digitális kereskedelmi forgalmat.[46] A tervezet elemeként kiemeli a szoftvergyártók felelősségével összefüggésében továbbá azt, hogy korlátozásra kerül a biztonsági felelősség szerződéses[47] úton történő kizárása.[48] A szabályozás részleges hiányával kapcsolatban a gyakorlatban gyakran merül fel az a nézőpont, amely hangsúlyozza a piac ösztönző hatását a sebezhető termékek létrehozására. Azonban jelen problémára egyszerű válaszként szolgál az, hogy a jelenlegi szabályozási környezet még csak most próbálja meg átlépni a gyenge szankcionálási lépéseket a biztonsági gyakorlatokat ignoráló technológiai vállalatokra nézve.[49]

A negyedik célkitűzés tekintetében a szövetségi kormányzat a kritikus infrastruktúrák kiberbiztonságának és ellenálló képességének megerősítését szorgalmazza, amely tekintetében kutatási és fejlesztési célok finanszírozását prioritásként kezeli. A kutatási támogatások jelentősége azt a célt szolgálja, hogy jobban megértsük a kiberbiztonságra gyakorolt társadalmi és egyéb hatásokat, valamint ennek az esetnek a fordított nézőpontjának elemzését is szolgálja.

Az ötödik célkitűzés a közbeszerzések összpontosítására helyezi a hangsúlyt az elszámoltathatóság érdekében. Tulajdonképpen egy meghatározott pénzforrásból történő szabályozás nagy hatással lehet a biztonságos szoftverek kialakításához. Ez összefüggésben áll azzal, hogy előtérbe kerülnek a biztonságosan kifejlesztett és védett szoftverek. A szövetségi kormány úgy ösztönzi a szállítókat, hogy csak olyan szoftvertermékeket vásárolnak, amelyek megfelelnek a NIST biztonsági szabványoknak. Ez ugyanis megmagyarázza azt a felvetést, hogy a pénzbeli támogatásokhoz való hozzáférés érdekében a szoftvergyártók kénytelenné válnak megfeleltetni szoftvereiket az előírásoknak a kritikus infrastruktúrákban történő alkalmazáshoz. Itt is körvonalazódni látszik a FISMA által meghatározott irány megvalósulása, ugyanis a rendszer elképzelései alapján fejlesztett szoftvereknek meg kell felelniük a szabványoknak a

[45] Lostri, Pell (2023).: i. m.
[46] Jindal, Soliman:i. m.
[47] Ebben az esetben a szoftvergyártók piaci helyzetüket kihasználva az ÁSZF-ben foglaltak alapján minimalizálják felelősségüket.
[48]BORGIA– AUSTIN: i. m.
[49] Teske– Oh: i.m.

kockázatkezelés szempontjából. Az esetkör jelentősége különösen megfigyelhető az energiaipar és az egészségügy tekintetében, ahol a szoftverek biztonsága közvetlen hatással bír a közbiztonságra és a szolgáltatásnyújtás folyamatosságára egyaránt.[50]

A harmadik pillér technológiai iparágra gyakorolt hatásainak megvizsgálását követően megállapítható, hogy az új amerikai kiberbiztonsági stratégia a technológiai vállalatok felelősségre vonására kezd irányulni. Azt fontos alapvetően leszögezni, hogy a stratégia nem teremt új kötelezettséget, jogi hatással nem rendelkezik. A stratégiának közvetlen kihatása nincs a technológiai iparra, bár rendkívül részletes módon szabályozza a szoftvergyártók biztonsági gyakorlatának keretrendszerét.[51] A költségeket okozó adatszivárgások és zsarolóprogramok megjelenése a vállalati életben egyre inkább népszerűvé teszik az eddig még kevésbé ismert kiberbiztonsági biztosítások megítélését, így a biztosítási díjak is emelkednek. A hatodik pillérrel összefüggésben a kormány felelőssége, hogy stabilizálja a gazdaságot és biztonságot nyújtson, melynek kivitelezése felveti a szövetségi biztosítás szükségességét.[52] A speciális biztosítási fajta a szervezeteket érintő információbiztonsági támadásokra összpontosít. Az adattörlésekkel összefüggő kockázatok miatt a hagyományos kereskedelmi felelősségbiztosítások nem tartalmaznak hasonló biztosítási eseményeket, vagy expressis verbis nem rögzítik. A kibertámadások számának emelkedése következtében a pénzügyi kihatásokra tekintettel a kiberbiztosítási fedezet megléte számos jelentősen kritikus amerikai ipari szereplőnek elengedhetetlenné vált.[53] További szempont az a biztonsági megoldások tekintetében, hogy a hangsúly jelen esetben leginkább szövetségi szintre tolódik át. A stratégia érdemben nem foglalkozik expressis verbis a szövetségi kezdeményezések kölcsönhatásával a meglévő állami szabályozás és törvények tekintetében. Ellenben biztonsági szempontból számos állam megköveteli már az alapos kiberbiztonsági intézkedéseket. Ennek értelmében a stratégiában kimunkált szabályozás inkább iránymutatásként szolgál de lege ferenda javaslatként a jogszabályok megalkotásához. A stratégia általánosságban utal a különböző hatóságok közötti együttműködésre, azonban kimondott mechanizmusokat nem határoz meg az eltérő joghatósági szabályok egyszerűsítésére.[54]

ÖSSZEFOGLALÁS

Az Egyesült Államok törekszik a szoftverek átlátható fejlesztésére és a problémák részletes listázására. Ennek érdekében említem meg ismét a korábban bemutatott követelményeket tartalmazó SBOM kifejezést, amely kiemelt jelentőséggel bír. Lényege a sebezhetőségek és az ellátási láncok kockázatainak csökkentése, utalva a korábban kritikusként említett energiaiparra. Kiemelendőek a NIST szabványai, amelyek átfogó útmutatóként szolgálnak az

[50] NIST SP 800-161r1 i. m.: 233. o.
[51] Teske, – Oh.: i.m.
[52] Maia Hamin, Trey Herr, Will Loomis, Emma Schroeder, and Stewart Scott: How will the US counter cyber threats?
[53] Violino, Bob: Rising premiums, more restricted cyber insurance coverage poses big risk for companies
[54] Teske, – Oh: i.m.

adatvédelmi kontrollról a szoftverek biztonságos fejlesztése tekintetében. Az Egyesült Államok aspektusát vizsgálva jellemző az ajánlott, megengedőbb követelményrendszer, amely irányadó a kidolgozott stratégia és szabványok vonatkozásában. Főként az önkéntes iparági szabványokra helyeződött a hangsúly.

Az Egyesült Államokban kimondottan csak a kritikus infrastruktúrákra és egyes szövetségi alrendszerekre összpontosítanak fokozott biztonsági jelleggel, így a biztonsági keretrendszer kevésbé átfogó. A kiberbiztonsági megfelelőség érdekében az amerikai rendszer azonban kevésbé támaszt szigorú következményeket.

Irányadó a korábban kiemelt fokozatos szigorodás az Egyesült Államokban a hatályos kiberbiztonsági stratégia értelmében, különösen az 14028-as rendeletet követően. Az Egyesült Államokban jellemzőbb a rugalmas, kockázatalapú szabályozási keret, amely az iparágaknak lényegesen nagyobb szabadságot biztosít a kiberbiztonsági intézkedések alkalmazásában.

FELHASZNÁLT FORRÁSOK

[1] A Report to the President on Progress in Implementing Section 4 of Executive Order 14028 on Improving the Nation's Cybersecurity (https://tinyurl.com/2nptbdaw)
[2] Bart Lenaerts-Bergmans.: What Is Cyber Resilience? (https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/cyber-resilience/)
[3] Borgia, Michael – Austin, Patrick: Overview of the National Cybersecurity Strategy (https://tinyurl.com/3f3dhbcz)
[4] Critical Software - Definition & Explanatory Material, Executive Order 14028, Improving the Nation's Cybersecurity (https://tinyurl.com/5n8jjz9d)
[5] Crooks Behind $81M Bangladesh Bank Heist Linked To Sony Pictures Hackers (https://tinyurl.com/3yuubeu8)
[6] Cyber Defense Agency: It's time to build cybersecurity into the design and manufacture of technology products. (https://www.cisa.gov/securebydesign)
[7] Divyanshu Jindal, Mohammed Soliman: The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace? (https://tinyurl.com/4uacp2hb)
[8] Eugenia Lostri, Stephanie Pell: The Biden Administration's Implementation Plan for the National Cybersecurity Strategy (https://tinyurl.com/578876ru)
[9] Executive Order 14028, Improving the Nation's Cybersecurity
[10] Gebremichael, T., Ledwaba, L.P., Eldefrawy, M.H., Hancke, G.P., Pereira, N.S., Gidlund, M., & Åkerberg, J. (2020): Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. IEEE Access, Évf. 8.
[11] Gerhard Peters, John T. Woolley.: FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy Online (https://tinyurl.com/ycx32pzy)
[12] Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order (https://tinyurl.com/3ve2357t)
[13] Kerner, Sean Michael.: 35 cybersecurity statistics to lose sleep over in 2024, Utal: WORLD ECONOMINC FORUM- Global Risks Report 2023(https://tinyurl.com/5hfff3xc)

[14] Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. In: Honvédségi Szemle – Hungarian Defence Review, Évf. 148 szám 5, Honvéd Vezérkar, Budapest.
[15] Krizsán Bence: Az Amerikai Egyesült Államok új Nemzeti Kibervédelmi Stratégiája (https://tinyurl.com/2sj53kjv)
[16] Liao ,Annie - Johnson, Rex :Summary of the 2023 National Cybersecurity Strategy Part 2, (https://tinyurl.com/2exvrdvr)
[17] Maia Hamin, Trey Herr, Will Loomis, Emma Schroeder, and Stewart Scott: How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy (https://tinyurl.com/y9raezby)
[18] National Cybersecurity Strategy Implementation Plan Version 2 (NCSI Plan Version 2)
[19] National Institute of Standards and Technolog :Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (https://tinyurl.com/5c7up5hv)
[20] National Institute of Standards and Technology Special Publications: 800-207
[21] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems(https://tinyurl.com/bddw6x4t)
[22] NIST SP: 800-161r1
[23] Peretti,.Kimberly.Kiefer.-.Bartolotta,.Kristen :Privacy, Cyber & Data Strategy Advisory: White House Releases National Cybersecurity Strategy (https://tinyurl.com/4hnpw947)
[24] Roberta Freeman: White House releases National Cybersecurity Strategy (https://tinyurl.com/y3apt8dt)
[25] Szabó András (2018): TECHNIKAI KIBERBIZTONSÁGI GYAKORLATOK – NEMZETKÖZI KITEKINTÉS HADMÉRNÖK, XIII. Évfolyam 1. szám – 2018. március, NKE, Budapest.
[26] Teske, David S. – Oh, Hyun Jai .:Intellectual Property Advisory: New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable (https://tinyurl.com/2mjwmvzh)
[27] The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years (https://tinyurl.com/hancy6ty)
[28] Violino, Bob: Rising premiums, more restricted cyber insurance coverage poses big risk for companies (https://tinyurl.com/yck6rsvz)
[29] What is SOAR? (https://tinyurl.com/mwjpkp48)

Military and Intelligence CyberSecurity Research Paper 2025/1.

Szerző(k) / Author(s):
Medvácz Ádám

Kézirat lezárásának ideje / Manuscript closing time:
2025.04.20.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD | Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. | 9-11. Hungária Blvd., Budapest, H1011

ISSN: ***2786-3778***

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.
The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.