



**37. Országos Tudományos Diákköri Konferencia
Állam- és Jogtudományi Szekció**

Budapest, 2025. március 24–26.

Rendező intézmény:
Károli Gáspár Református Egyetem
Állam- és Jogtudományi Kar



Állam- és Jog-
tudományi Szekció

***CYBER RESILIENCE ACT: A “CSODA” FEGYVER – AZ
AMERIKAI EGYESÜLT ÁLLAMOKAT KÖVETVE AZ EURÓPAI
UNIÓ IS SZIGORÍTJA A KIBERBIZTONSÁGI SZABVÁNYOKAT!?***

Kézirat lezárásának dátuma:

2024/11/26

A dolgozat készítőjeként nyilatkozom, hogy a dolgozat érdemi tartalmát illetően a mesterséges intelligencia közreműködését nem vettem igénybe.

Mottó:

„A technológia mindig is kétélű fegyver lesz. Óriási hatalom, amelyet az egész emberiség javára kell felhasználni.”

(Ray Kurzweil)

TARTALOM

I. Bevezető gondolatok	1
II. A kiberbiztonság szerepe a szoftverfejlesztésben és alkalmazásban.....	3
II.1. Az informatikai termékek rendszerfejlesztési életciklusának jelentősége a kiberbiztonság vonatkozásában	6
III. A szabályozás rendszerének elemzése az Amerikai Egyesült Államok vonatkozásában	11
III.1. Az amerikai kiberbiztonsági stratégia pilléreken nyugvó rendszere	12
III.2. A kiberreziliencia jelentősége a kibertérben bekövetkező támadások tekintetében.....	17
III.3. A kiberbiztonsági stratégia harmadik pillérének elemzése és kihatása az ipari környezetre	19
IV. Cyber Resilience Act jelentősége	26
V. Összegzés.....	35
Irodalomjegyzék:	38

I. BEVEZETŐ GONDOLATOK

A kiberbiztonság jelentősége az utóbbi években egyre inkább előtérbe került, különösen a digitális szolgáltatások és a szoftverfejlesztés területén. Az Amerikai Egyesült Államok és az Európai Unió egyaránt nagy hangsúlyt fektetett arra, hogy reagáljon a kibertérből érkező egyre összetettebb és gyakoribb fenyegetésekre. Az Európai Unió megalkotta a Cyber Resilience Act-et, amely komoly változást hozott az uniós kiberbiztonsági szabványok terén. Dolgozatomban az amerikai és az európai szabályozások összehasonlító elemzésére fókuszál, vizsgálva azok hatását a szoftverek fejlesztésére, forgalmazására és a kritikus infrastruktúrák biztonságára.

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 és az adatoktól. Tulajdonképpen elengedhetetlenné válnak a hatékony kiberbiztonsági intézkedések. Az Amerikai Egyesült Államok korán felismerte a terület fontosságát, és számos szabályozást vezetett be, amelyek célja, hogy növeljék a szoftverek kiberrezilienciáját, és erősítsék az IT-biztonságot. Az európai megközelítés, amely mostanra a Cyber Resilience Act keretében öltött formát, szintén bevezette a szoftverfejlesztési életciklus minden szakaszában a kiberbiztonsági követelményeket, valamint kiterjesztette azokat a digitális termékek biztonságos alkalmazására és forgalmazására.

A dolgozat áttekinti a Cyber Resilience Act és az amerikai szabályozások közötti hasonlóságokat és különbségeket. Tárgyalja különösen a szoftverfejlesztési életciklus során alkalmazott kiberbiztonsági intézkedések és követelmények integrációját. Az elemzés során külön figyelmet fordítunk a szabályozások hatására a szoftvergyártókra, a forgalmazókra és a fogyasztókra, valamint a magán- és az állami szféra eltérő kockázatkezelési módszereire. Emellett részletesen bemutatjuk a kiberreziliencia szerepét a kibertámadásokkal szembeni védekezésben, valamint a két kontinens szabályozásának következményeit a gyártói felelősség, a fogyasztói tudatosság és az iparági szabványok terén.

Célunk átfogó képet nyújtani az Amerikai Egyesült Államok és az Európai Unió szabályozási rendszereinek megközelítéseiről, különös tekintettel a szoftverek rendszerfejlesztési életciklusára és az iparági követelmények szigorítására. Az amerikai szabályozások részletesen bemutatott elemei, például az IoT Cybersecurity Improvement Act és az elnöki

rendeletek, illetve a Cyber Resilience Act új szabályozási kerete, amely a szoftverek és digitális termékek biztonságára vonatkozó előírásokat szigorítja, olyan témakörök, amelyek jelentős hatással vannak a globális szoftverpiacra, valamint a kiberbiztonság jövőbeli alakulására.

E dolgozat célja annak bemutatása, hogy az Amerikai Egyesült Államok és az Európai Unió szabályozási rendszerei miként képesek választ adni a modern digitális kihívásokra, valamint hogyan erősíthetik a kiberbiztonságot egy átfogó és egységes szabályozási rendszer kiépítésével. Az összehasonlító elemzés nemcsak a két szereplő közötti eltérő szabályozási szemléletet tárja fel, hanem rávilágít arra is, hogy a Cyber Resilience Act és az amerikai szabályozások milyen hatással lehetnek a jövőbeni globális kiberbiztonsági normák kialakítására.

II. A KIBERBIZTONSÁG SZEREPE A SZOFTVERFEJLESZTÉSBEN ÉS ALKALMAZÁSBAN

A szoftverek kiberbiztonsági célzatú vizsgálata leginkább a forráskódok csoportosításának jellegéből adódhat. Számos módszer létezik annak érdekében, hogy a szoftverek stabilitása fenntartható legyen. A vizsgálatok célja az adatok fokozott védelme és a jogszabály révén is optimális szoftverkörnyezet kialakítása. A módszerek közül kiemelendő a code review esetköre. Az említett manuális és automatizált áttekintésre irányuló folyamat különösen fontos, ugyanis célja a szoftver teljes forráskódjának átvizsgálása. A felmerülő sebezhetőségek azonosítására és megszüntetésére szolgál. A szoftverek kódjainak auditálása mellett jelentős módszernek tekintendő a network sniffing és a pentesting. A sniffing egy passzív jellegű módszerként jellemezhető, amely figyeli a hálózattal összefüggő kommunikációt, dekódolja a protokollokat és keresi a releváns információkat. Penetrációs tesztek alapján valós támadások szimulációja által törekednek felderíteni a szoftverek biztonsági funkcióinak megkerülési lehetőségeit. A módszer lényege abban rejlik, hogy a szimulációban a támadók által alkalmazott technikákat és eszközöket használnak.¹ Fontos a szoftverek biztonsági tesztelése és vizsgálata, ugyanis ez rendkívüli segítség a gyártóknak termékeik sebezhetőségi pontjainak megállapításában. Kiemelendő a kiberbiztonsági elemzési módszerekkel összefüggésben a szoftverek rendszerfejlesztési életciklusa. A szoftverek életciklusának összes fázisában szükséges integrálni a vizsgálatokat. Ennek következtében garantálható az, hogy kezdetektől a megfelelően vizsgált szoftver ellenállóbb lesz a kiberfenyegetésekkel szemben.²

A zárt forráskódú szoftverek biztonsága alapvetően a szoftvercégek működésével áll összefüggésben. A piacvezető szoftvercégek rendszeres belső fejlesztési irányelvek alapján, folyamatos frissítésekkel igyekeznek megtartani vezető szerepüket különböző biztonsági funkciók beépítése révén. A nagy szoftvervállalatok szándékosan nem teszik nyilvánossá forráskódjaikat. Ezzel a korlátozással minimalizálhatóak a potenciális támadások a szoftverek hibáiból eredően. A korlátozásból eredően a felhasználók nem képesek módosítani és átalakítani a szoftver forráskódját. Ezért a felhasználók szoros függőségi viszonyba kerülnek a szoftvergyártókkal, amelynek értelmében a szoftvergyártók saját térrétegükben

¹ NIST SP: 800-115 (2008.09.) F-1, F-2 (76-77.o.)

² NIST SP: 800-115: i. m. C-1 (70.o.)

gondoskodnak minden szoftverrel kapcsolatos frissítésről és hibaelhárításról. Másik lényeges aspektus a nyílt forráskódú szoftver. A Linux operációs rendszere és az Apache webkiszolgáló szoftvere is széles körben ismert és elterjedt, annak ellenére, hogy nyílt forráskódú megoldásokon alapulnak. A nyílt forráskódú szoftverek közösségi alapú fejlesztése nyilvános, amely elősegíti a közös megoldásokat és gyorsabb hibajavítást a fejlesztők között. Megvizsgálva a közösségi alapú fejlesztésből származó szoftverek igen kedvezőnek tűnnek, azonban potenciális sebezhetőséggel rendelkezhetnek.³ A könnyű hozzáférhetőség előnyétől eltekintve hátrányként emelhető ki a támogatás részleges, vagy adott esetben teljes hiánya. Ennek értelmében kiberbiztonsági kockázatot is jelenthet, amennyiben a forráskódokat nem megfelelően ellenőrzik, vagy nem kapnak frissítéseket. Ezzel szemben a zárt forráskód sokkal inkább a magas szintű megbízhatóságra és kiemelt biztonságra helyezi a hangsúlyt alapvetően.⁴

A kritikus szemléletet a nyílt forráskódú szoftverek vonatkozásában megalapozza az, hogy a közösségi fejlesztések nem esnek át alapos biztonsági ellenőrzéseken. Komoly kockázatok igazolására szükséges tanulmányozni a sérülékenységi esetköröket, amelyekben a nyílt forráskódú szoftverek biztonsági réseit használhatják ki. Hangsúlyozandó a Log4Shell sebezhetőség esetköre. Az említett sebezhetőség a korábbiakban említett Apache webkiszolgáló naplózási könyvtárában volt megtalálható. Ez a sebezhetőség azért is volt igen jelentős, mert távoli kódfuttatási lehetőségeket biztosított a névtelen támadások végrehajtásához. Ez a probléma különösen fontos, ugyanis szinte bármely felületet érinthetett ez a sebezhetőség, amely az említett Log4j sebezhetőséggel rendelkező naplózási könyvtárat használta fel.⁵ Példaként említhető a Java alapú Minecraft videójáték, amely hasonlóan az említett sebezhetőséggel rendelkező, nyílt forráskódú naplózási könyvtárat alkalmazta. A támadók képesek voltak távoli kódfuttatást lefolytatni a Minecraft szerverein rövid szöveges üzenetek beillesztésével a csevegőmezőbe. A felmerült hiba kijavítása nem okozott különösebb problémát, azonban rávilágított a nyílt forráskódú szoftverek és komponenseknek rendszeres frissítésének igényére, szükségességére.⁶

Lényeges a szoftverfejlesztési folyamatok vonatkozásában a nemzetközi kiberbiztonsági szabványok jelentősége. A nemzetközi szabványok hatással vannak a szoftverfejlesztési

³ Kerekes Gábor: Nyílt forráskódú szoftver – A felhasználás jogi vonatkozásai – Tévhitek oszlatunk!

⁴László Gábor (2020): A nyílt forráskódú szoftverek szerepe a közigazgatásban. In Sasvári Péter szerk.: Informatikai rendszerek a közszolgálatban II., Dialóg Campus, Budapest. 105-106. o.

⁵ Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

⁶ What You Need to Know About Log4Shell, the Vulnerability Affecting Log4j

folyamatokra. Az ISO/IEC 27001 az információbiztonság-menedzsment egyik legismertebb szabványának tekinthető. Célja az adatok védelme és a biztonsági kockázatok minimalizálása. Az adatvédelem szempontjából az említett szabvány hangsúlyt fektet a titkosítás alkalmazására a fejlesztési folyamatok során. Ezenfelül a szabvány folyamatos kockázatértékelést ír elő, amely segít a szoftverek életciklusának fázisain keresztül azonosítani a sebezhetőségeket. Kötelező biztonsági ellenőrzések lefolytatásával kívánja csökkenteni a szabvány a kibertámadások számát. A szoftverfejlesztésre történő hatása már tapasztalható a biztonsági követelmények beépítésére történő ösztönzés kapcsán a szoftverfejlesztési folyamat fázisában. A fejlesztési folyamatokban a tesztelések és a korábban említett auditok játszanak kiemelt szerepet. Lényeges még ezzel összefüggésben a szoftver fejlesztésével járó folyamatos változás és az erre vonatkozó dokumentáció. A szoftverek biztonságának kialakításában kulcsszerepet játszanak a folyamatos frissítések és hibajavítások.⁷ A folyamatos frissítések tulajdonképpen elengedhetetlenek a felmerülő szoftveres hibák kezelésére. Ezzel összefüggésben kulcsfontosságú a patch management jelentősége a modern kiberbiztonsági stratégiák vonatkozásában.⁸ A sérülékenységek kihasználhatóságából adódóan a frissítések késedelme komoly biztonsági kockázatot rejthet. Ennek magyarázataként szolgál a szoftvercégek átgondolt patch management stratégiája, amely lehetővé teszi a fejlesztések és javítások megfelelő időben történő alkalmazását. Támadási felületet hordoz magában a már nem támogatott Microsoft XP operációs rendszert alkalmazó felhasználó. A példaként kiemelt Microsoft XP frissítéses támogatása 2014. április 8-án megszűnt a Microsoft fejlesztésében. A Microsoft ennek eredményeképpen nem készített új biztonsági frissítéseket, biztonsági gyorsjavításokat az említett operációs rendszerre. A szoftvercég kiemelte, hogy az operációs rendszert a támogatási dátum lejárta után továbbra is alkalmazó felhasználók potenciális kockázatoknak vannak kitéve.⁹ A folyamatos frissítések biztosítják a szoftverek új kihívásokhoz alkalmazkodó védelmi mechanizmusát, csökkentve a támadásra lehetőséget adó felületeket. Fontos megemlíteni, hogy a nyílt forráskódú és zárt forráskódú szoftverek tekintetében egyaránt lényeges cél a felfedezett hibák lehető leggyorsabban történő kijavítása. A patch management ennek értelmében egy rendkívül kifinomult része a vállalatok kiberbiztonsági stratégiájának tekintetében a folyamatosan fejlődő fenyegetésekkel szemben.

⁷ Understanding ISO 27001 and Its Relevance to Software Development

⁸ Patch Management

⁹ A Windows XP, az Office 2003 és az Exchange 2003 támogatása véget ért.

II.1. AZ INFORMATIKAI TERMÉKEK RENDSZERFEJLESZTÉSI ÉLETCIKLUSÁNAK JELENTŐSÉGE A KIBERBIZTONSÁG VONATKOZÁSÁBAN

A nyílt forráskódú szoftverek szabad hozzáférhetősége mellett kiemelt szempontként szükséges vizsgálni az informatikai termékek rendszerfejlesztési életciklusát¹⁰. A védelem kialakításának szempontjából történő megközelítés vonatkozásában az egyik legalapvetőbb szempont az, hogy a fejlesztési folyamat elejétől az adott szoftver forgalomból történő kivételéig minden egyes lépésnél be tudjuk integrálni a kiberbiztonsági előírásoknak megfelelő követelményeket. A korai hibaelhárítás csökkenti a későbbi életciklusi fázisokban felmerülő problémákat. Lényeges továbbá kiemelni, hogy a kiberbiztonsági incidensek bekövetkezésekor a károk minimalizása is elérhető. Kiemelendő a szoftverek életciklusával összefüggésben az, hogy a kiberbiztonsági intézkedések elhanyagolása milyen következményekkel járhat. Amennyiben nem alkalmazzuk a rendszerfejlesztési életciklus valamennyi fázisában megfelelően a biztonsági intézkedéseket, akkor komoly következményekkel kell számolnunk. Példaként kihangsúlyozandó az Equifax 2017-ben történt adatvédelmi incidense, amelynek következtében több százmillió ügyféladatot szivárogtattak ki a hitelinformációs ügynökségtől. A vállalatot egy fogyasztói panaszokkal foglalkozó internetes portálon keresztül törték fel. A támadók egy széles körben ismert sebezhetőségi pontot használtak ki, amelyet javítani kellett volna a forráskódban. Az Equifax belső szervezeti problémák miatt nem végezte el a hibaelhárítást. Az Apache Struts keretrendszeréből származó biztonsági résben található sebezhetőséget hónapokkal az incidens bekövetkezése előtt kijavították, ellenben a frissítést nem hajtották végre központilag. Ez az esettanulmány jól szemlélteti a biztonsági követelmények elhanyagolását a szoftverek életciklusának későbbi szakaszaival összefüggésben.¹¹ Ebből a megközelítésből kiindulva lényeges szempontként kell tekintenünk az adott szoftverek életciklusának változásaira, azok szabályozási megoldásaira nemzeti és nemzetközi szinten egyaránt.

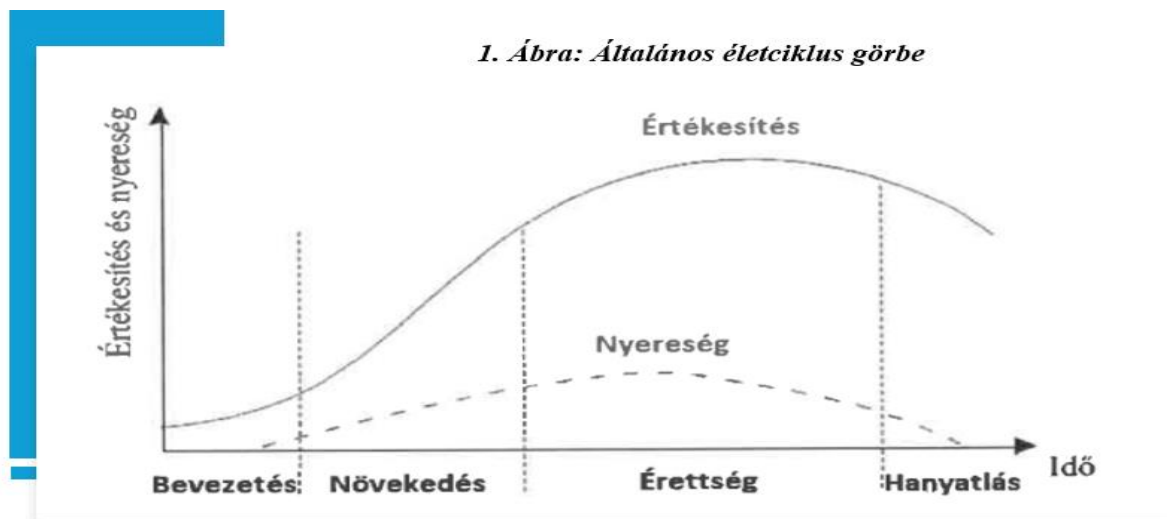
Fontos kiemelni az életciklus fogalom jelentőségét, amely a mikrogazdaság ciklikusságához kapcsolódó innovációt testesíti meg. Ezzel összefüggésben a „kreatív rombolás”¹² tekinthető összességében a folyamatos változás alapjának az IT-szektor vonatkozásában. A szoftverfejlesztés területén a megújulás vonatkozásában az említett fogalom különösen releváns, mivel a technológiai fejlődés gyors ütemét tekintve a szoftvertermékek gyorsan

¹⁰ System Development Life Cycle

¹¹ Josh Fruhlinger: Equifax data breach FAQ: What happened, who was affected, what was the impact?

¹² Joseph Schumpeter amerikai közgazdász kifejezése az új technológiák előnyének kihangsúlyozására a régi megoldások felváltásával a gazdaság növekedésével kapcsolatban.

elavulnak. Egyszerű ösztönzésként hat a szoftvercégek közötti versenyre a versenytársak által létrehozott innovációk kérdésköre. A versenyképesség megőrzése jelentős mértékű erőforrások felhasználását követeli meg a szoftvercégektől, amennyiben nem próbálnak meg alkalmazkodni a piaci trendekhez, iparági újdonságokhoz, akkor könnyen elveszíthetik vezető pozíciójukat a szoftverpiacon. Az életciklust tekinthetjük az adott szektoron belül a piaci, gazdasági folyamatok egyik mozgatórugójának. Az alábbi ábra reprezentálja, hogy melyik az a 4 lényeges fázis, amelyen egy szoftver végighalad az életciklusa alatt.¹³



Az IT-piac diverzifikáltságát megvizsgálva megállapítható az, hogy különböző technológiákat, valamint azonos technológián belül különböző gyártók termékeit alkalmazzuk a mindennapokban rendszeresen. A piac telítettségét megfigyelve fontos kialakítani azt a koherenciát a szoftverek között, hogy egy egységes környezetben szabványok alapján rendeltetésszerűen működhessenek egymással.¹⁴ Lényeges alapvetően azt megjegyezni, hogy a fent hivatkozott táblázat általános jellegűnek tekintendő a szoftverek életciklusának vizsgálatára. A piac telítettsége mellett számos más olyan tényező is megtalálható, amely az említett görbének az alakulására jelentős kihatással bír.

A hivatkozott életciklus görbéjének *Bevezető* fázisa a szoftverek vizsgálatában testesíti meg az adott szoftver piacra kerülését. Az optimális szoftverfejlesztési életciklus kezdetén már jellemző a kiberbiztonsági követelmények megjelenése a tervezési tevékenységek kezdetén. A kiberbiztonsági követelmények kezdeti szakaszban való elhanyagolása már kezdetben

¹³ Pankotay Fruzsina Magda, Et al. (2020): Az informatikai termékek életciklusának sajátosságai. In: Menedzsment válaszok a XXI. század gazdasági és társadalmi kihívásaira, Inform Kiadó és Nyomda Kft., Budapest. 67. o. Utal: Bíró-Szigeti, S. (2016.) Marketing-termékpólitika

¹⁴ László Gábor: i.m. 108. o.

potenciálisan sebezhető szoftvert eredményezne, ezért lényeges már a fejlesztési tevékenységek elején koncentrálni a security by design elv érvényesülésére. Az említett fejlesztési elv kiemeli a biztonsági intézkedések szükségességét már a szoftver fejlesztésének megkezdésekor. Ez szervezeti szinten is megjelenik, ugyanis a szoftvercégeknek a kezdetektől biztosítaniuk kell, hogy a szoftverfejlesztőik biztonságos fejlesztési gyakorlatokat alkalmazzanak. Alapvetően jellemző intézkedésként meghatározott szervezeti protokollok és az adatvédelmi intézkedések jelentik a kulcsfontosságú biztonsági súlypontokat. A kezdeti fázisban a kiemelt ábra alapján a kereslet az adott szoftver iránt még jelentősen csekély. Azonban a fejlesztési folyamatokat követően a tesztelések lezajlottak. Már megtörtént az adott szoftver részletes elemzése funkcionális szempontból, valamint a hozzáférés kiberbiztonsági szempontok szerinti szabályozása.¹⁵

A *Növekedés fázisa* során további folyamatos teszteléseket folytathatnak a különböző biztonsági jellegű ellátások eszközölése végett. A szoftverre vonatkozó kereslet is növekvő tendenciát mutat ebben a fázisban. A szoftvercégek tevékenysége a kiadott szoftverek minden komponensének a védelmére irányul, védelemben részesül többek között a jogosulatlan hozzáférésektől.¹⁶ Jelen fázisban alkalmazhatók a korábbiakban említett penetrációs tesztek és egyéb biztonsági ellenőrzési módszerek. Az ábrával összefüggésben megállapítható, hogy a felhasználók számának növekedésével egyenes arányosságban növekszik a szoftvereket támadók száma a szoftverek elterjedtebb használata során. Késedelem nélkül jelen esetben szintén irányadók a hibajavítások és frissítések ütemezett elvégzése a sebezhetőségek elkerülése végett.

Az *Érettség fázisra* általánosságban jellemző, hogy ez minősül a szoftverek tekintetében is leghosszabb fázisnak. Ebben a fázisban zajlik a finomhangolási időszak folytatódása és érkeznek a rendszeres frissítések és javítások. A szoftver gyártója folyamatos kapcsolattartás során a felhasználók visszajelzéseire kivizsgálja az aktuálisan felmerülő problémákat.¹⁷ A stabilitás megőrzése érdekében folyamatos karbantartásra és frissítésekre szorul továbbra is a folyamatosan fejlődő kiberfenyegetésekkel szemben. Kiemelten fontos a patch management jelen fázis vonatkozásában, ugyanis ütemezve így biztosítható a felhasználók teljeskörű naprakész védelme a fenyegetésekkel szemben.

¹⁵ Veer, Rob van der; Valkema, Menno; Guasconi, Fabio(2020): The role of the EU cybersecurity certification framework. In: Drogkaris, Prokopios ; Bourka, Athena: Advancing software security in the EU. Publications Office. 6.-8. o.

¹⁶ NIST SP: 800-218 4. o.

¹⁷ Pankotay Fruzsina Magda, Et al. (2020): i.m. 67-68. o.

Az elemzés vonatkozásában a leginkább releváns helyzetet azonban a hivatkozott ábra utolsó fázisa teremti meg. A szoftver *Hanyatlásának fázisa* során az adott szoftver tudatos és folyamatos kivezetése kezdődik meg a piaci forgalomból. A támogatottság az adott szoftverre a készítő oldaláról jelentősen csökken. Jellemző a szoftverek gyártóira az a magatartásforma, hogy igyekeznek még előirányozni a hanyatlás fázisában a szoftverekkel összefüggésben megszerzett, tárolt információk védelmét. Meghatározott időközönként lehetőséget biztosíthatnak arra is, hogy kedvezőbb feltételek mellett átállhassanak a felhasználók új rendszerekre. Amikor egy szoftver támogatottsága megszűnik, akkor jelentősen megnő a sebezhetőségi kockázat azok számára, akik továbbra is a régebbi verziót alkalmazzák. Fontos szempontként merülhet fel azonban az, hogy mégis mi történhet egy adott szoftver piacról történő helytelen kivezetése esetén. A piacról kivezetett szoftverek nem támogatott verziói többek között továbbra is működőképesek maradnak, ellenben a felhasználóknak nem biztosítanak megoldásokat az adott szoftver verziójával később felmerülő problémákra. Nem készülnek folyamatos frissítések és biztonsági jellegű frissítések és javítások.¹⁸ Ebből az aspektusból merülhet fel az a probléma, hogy az adott szoftver frissítésben nem részesült verziója ki lesz téve számos előre nem látható veszélynek a kibertérben. Ennek értelmében sebezhetővé válik a szoftver, amely a kibertámadások megnövekedését eredményezi. A támogatásban nem részesülő szoftverek kiberbiztonsági fenyegetéseknek való kitettsége igen jelentős, ugyanis ezen rendszerek sebezhetőségük miatt a rosszindulatú támadók célpontjává válnak. Az idő múlásával egyre elavultabbá válnak ezen támogatásban nem részesülő szoftverek. Jelen esetben is kimondottan irányadó a kreatív rombolás szemlélete a szoftverekre vonatkozóan. A hanyatló fázissal szoros összefüggésben áll a legacy rendszerek esetköre, amelyek kiberbiztonsági szempontból jelentős kockázatot hordoznak. A legacy rendszerek kimondott jellemzője a sebezhetőségek mellett a régi rendszerek költséges karbantartása. További negatív jellemzője az elavult rendszereknek a kompatibilitás hiánya az újabb szoftverekkel és azok komponenseivel.¹⁹

A szoftverfejlesztés vonatkozásában hangsúlyos fogalomként kezelendő a DevOps fogalma. A DevOps egy kifinomult fejlesztési módszertan, amely összehangolja a szoftverfejlesztők és üzemeltetési csapatok tevékenységét. A DevOps a tevékenységek összehangolásával célozza a jobb minőségű szoftverek és szolgáltatások elérését. A hibák csökkentése érdekében

¹⁸ Radack, Shirley (2009): The System Development Life Cycle (SDLC) In: Computer Security Division - National Institute of Standards and Technology Publication, Gaithersburg. 4-5. o.

¹⁹ Christopher Burgess: Legacy systems are the Achilles' heel of critical infrastructure cybersecurity

automatizált teszteléssel törekednek a szoftverek minőségének biztosítására. Ez a folyamat az innovációkat, fejlesztéseket és hibajavításokat képes rövidebb időn belül piaci igényeknek megfelelően megvalósítani.²⁰ Kiberbiztonsági szempontok figyelembevételével szükséges megvizsgálni a SecDevOps jelentőségét, amely a DevOps kiberbiztonsági szabványoknak való megfelelés érdekében kibővített változatának tekinthető. Jellemzője a korábbiakban ismertetett security by design elv, amely a biztonsági intézkedések alkalmazását követeli meg a szoftverfejlesztési életciklus kezdeti fázisától. Hasonlóan tartalmaz rendelkezéseket a folyamatos biztonsági ellenőrzésekre és sebezhetőségi tesztekre.

²⁰ What is DevOps?

III. A SZABÁLYOZÁS RENDSZERÉNEK ELEMZÉSE AZ AMERIKAI EGYESÜLT ÁLLAMOK VONATKOZÁSÁBAN

Napjainkban a kibertér egyre jelentősebb szerepet tölt be az országok védelmi stratégiájának kidolgozásában. Jelen fejezet vizsgálódási fő szempontjában az Amerikai Egyesült Államok hatályos kiberbiztonsági szabályozási rendszere és stratégiai 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 Technology²¹ 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 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.²²

A szabályozási keretrendszer vonatkozásában tapasztalható volt a preventív jellegű védekezés kialakítása Donald Trump elnökségének ciklusa alatt is.²³ Lényegesebb azonban megvizsgálni a következő elnöki ciklus 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

²¹ NIST

²² Cyber Defense Agency: It's time to build cybersecurity into the design and manufacture of technology products

²³ Krizsán Bence.: Az Amerikai Egyesült Államok új Nemzeti Kibervédelmi Stratégiája

minisztérium közreműködését szabályozta a rosszindulatú szoftverek azonosításával és a kockázatos tevékenységek megszakításával.²⁴

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.²⁵

III.1. 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.²⁶ A megfelelő beruházások összpontosítása érdekében továbbra is törekszik az Egyesült Államok vezető szerepének biztosítására a rugalmas és virágzó digitális jövő terén.²⁷

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.²⁸

²⁴ Divyanshu Jindal, Mohammed Soliman: The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?

²⁵ Roberta Freeman: White House releases National Cybersecurity Strategy

²⁶ Gerhard Peters, John T. Woolley.: FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy Online

²⁷ Jindal, Soliman: i. m.

²⁸ NCSI Plan Version 2

2. Ábra: Az Amerikai Egyesült Államok kiberbiztonsági stratégiája

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 infrastruktúrák²⁹ 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 2020³⁰ 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 Act³¹ rendelkezéseivel, amely előírta 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 sebezhetőségi felületek száma a kormányzati hálózatokban. A Cybersecurity Improvement

²⁹ Ide tartoznak az energiahálózatok, a vízellátás és a pénzügyi szektor.

³⁰ Az internet tárgyainak kiberbiztonságát javító törvény

³¹ Szövetségi információbiztonsági korszerűsítési törvény

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 rendelet³² 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 történő tartását.³³ 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.³⁴ 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

³² Executive Order 14028, Improving the Nation's Cybersecurity

³³ 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.

³⁴ Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order

fogyasztók számára a vásárlás előtt elérhetőnek kell lenniük fizikailag és digitális formátumban egyaránt.³⁵

Jelentős válaszlépésként szolgált jelen rendelet a magánszektor és közszektor fenyegető kiberfenyegetésekkel szemben. Rögzítette a szövetségi kormányok fellépését a kiberbiztonsági fenyegetésekkel felmerülő események azonosítására, felderítésére és orvoslására. Alapvetően 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 biztosítani 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 megfelelése az alaposan kimunkált kiberbiztonsági szabványokhoz és követelményekhez.³⁶ 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.³⁷ 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.³⁸ Az IoT biztonsági címkézési program az irányelvek következtében 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

³⁵ National Institute of Standards and Technology: Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products 18-19. o.

³⁶ Executive Order on Improving the Nation's Cybersecurity

³⁷ Critical Software - Definition & Explanatory Material

³⁸ BORGIA, Michael; AUSTIN, Patrick: Overview of the National Cybersecurity Strategy

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 kiberbiztonsági célok rögzítése, amelyek minden létfontosságú ágazatban következetesen betarthatóak.³⁹

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 előmozdításáról.⁴⁰

³⁹ National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

⁴⁰ Gerhard Peters, John T. Woolley.:i. m.

III.2. A KIBERREZILIENCIA JELENTŐSÉGE A KIBERTÉRBEN BEKÖVETKEZŐ TÁMADÁSOK TEKINTETÉBEN

A Világgazdasági Fórum 2023-ban kiadott jelentésében a kiberbiztonsági kockázatok továbbra is állandó aggodalomra adott okot. Jelentős kockázati tényezőnek minősítették a zsarolóvírusok elterjedését és az szoftverellátási láncokat célzó támadásokat. Továbbá a kockázati tényezők tekintetében 2024-ben további növekedés várható a technológiaalapú erőforrások és szolgáltatások vonatkozásában. Lényeges a reziliencia 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.⁴¹ 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.⁴² Az elmúlt évek statisztikai vizsgálata alapján megállapítható, hogy éves szinten 25% mértékű emelkedés következett be az amerikai kormány sebezhetőségi adatbázisában.⁴³

A harmadik pillér részletes elemzését megelőzően azonban elengedhetetlen megvizsgálni a kiberreziliencia jelentőségét. A helyreállítással és a védelemmel kapcsolatban fontos kiemelni a kiberbiztonsági kockázat azonosítását, észlelését és az erre történő reagálást, amelynek alapjait a korábban kiemelt Cybersecurity Framework teremtette meg. A káros hatású 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

⁴¹ Crooks Behind \$81M Bangladesh Bank Heist Linked To Sony Pictures Hackers

⁴² The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

⁴³ Kerner, Sean Michael.: 35 cybersecurity statistics to lose sleep over in 2024, Ural: WORLD ECONOMIC FORUM- Global Risks Report 2023; Vulnerability and Threat Trends Report 2023

működése képes legyen alkalmazkodni a kedvezőtlen körülményekhez és alkalmas legyen az ellenállásra a fenyegetésekkel szemben. Legszerűségesebb esetben pedig képes legyen helyreállítani a belső rendszerének folyamatos működését.⁴⁴ A stratégia a kiberbiztonság javítása mellett az IT infrastruktúra modernizálását tűzi ki. Ezzel összefüggésben rendezni kívánja a tervezet a rendszerszintű kockázatok 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.⁴⁵ 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 feladatvégzéshez. 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.⁴⁶ 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 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. Ez magában foglalhatja a technikai

⁴⁴ Bart Lenaerts-Bergmans.: What Is Cyber Resilience?

⁴⁵ Jindal, Soliman: i. m.

⁴⁶ NIST SP: 800-207 4.-8. o.

infrastruktúra vonatkozásában a hálózatok és esetleges kiberbiztonsági megoldások integrálását.⁴⁷ Részletes vizsgálat következtében ugyanis nem jelenthet meglepetést a támadások valós időben történő visszaverése sem.⁴⁸

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 reagálni a potenciális fenyegetéseket, valamint ezzel összefüggésben gyors válaszreakciókat képesek adni. Az automatizált rendszerek egy része SOAR⁴⁹ 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.⁵⁰

III.3. 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

⁴⁷ Szabó András (2018): TECHNIKAI KIBERBIZTONSÁGI GYAKORLATOK – NEMZETKÖZI KITEKINTÉS In: *HADMÉRNÖK*, XIII. Évfolyam 1. szám – 2018. március, NKE, Budapest. 298. o.

⁴⁸ 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.

⁴⁹ Security Orchestration, Automation, and Response

⁵⁰ What is SOAR?

származó komponenseket tartalmazó szoftvereket és egyéb eszközöket.⁵¹ Ennek kapcsán szükséges a felelősséget a nagy behatással bíró adatgazdálkodók részére áthárítani a fogyasztónak minősülő felhasználókról.⁵² A harmadik pillér elemzésének rendszerét a stratégiában megtalálható felosztás alapján végzem el. A harmadik pillér a piaci erők alakításának érdekében több lényeges célkitűzést emel ki, amelyet a következő ábra szemléltet.⁵³

3. 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 biztosítanak 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.⁵⁴

Az első célkitűzés kiemeli az adatvédelem jelentőségét és ezzel összefüggésben irányul az adatok kezelőinek felelősségre vonására. Kimondott korlátokat határoz meg taxatívén ezen témakörben, amelyek többet között a személyes adatok gyűjtésére, felhasználására, továbbítására és az ezzel felmerülő karbantartásra tekintettel.⁵⁵ A NIST által kidolgozott szabványok és iránymutatások alapján a szilárd és egyértelmű korlátok közül kiemelendő a

⁵¹ Teske, David S. – Oh, Hyun Jai. Intellectual Property Advisory: New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable

⁵² PERETTI, Kimberly Kiefer - BARTOLOTTA, Kristen: White House Releases National Cybersecurity Strategy

⁵³ Saját készítésű ábra az Amerikai Egyesült Államok kiberbiztonsági stratégiájának alapján.: 36.-43. o.

⁵⁴ PERETTI, - BARTOLOTTA: i. m.

⁵⁵ LIAO, Annie,- JOHNSON, Rex :Summary of the 2023 National Cybersecurity Strategy Part 2.

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.⁵⁶ Rendkívül nehéz olyan szabályozást kidolgozni a 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 programja⁵⁷. Ezzel kapcsolatban érdemes kiemelni az IoT-eszközök hiányos kiberbiztonsági gyakorlatának kockázata 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 korábbiakban felvetett 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 működik. Azonban komplex feladat megvizsgálni, hogy egy ipari IoT-infrastruktúra megfeleltethető a meghatározott szabványokban található követelményrendszereknek.⁵⁸

⁵⁶ Eugenia Lostri, Stephanie Pell: The Biden Administration's Implementation Plan for the National Cybersecurity Strategy.

⁵⁷ Cybersecurity Labeling for Internet of Things.

⁵⁸ 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.

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 14028.⁵⁹ számú végrehajtási rendelet 4. szakasza rendelkezik. A táblázatban szereplő ötödik célkitűzésben a kormányzat 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.⁶⁰

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. A korábban említett Equifax adatvédelmi incidens szorosan kapcsolódik jelen esetkörhöz a felelősség átcsoportosításának vonatkozásában.

Összegezve ez a fejezet a rosszul megírt kódokkal, valamint a helytelen biztonsági intézkedésekkel áll összefüggésben. Jelentősséggel 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.⁶¹ 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 kiemelendők 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

⁵⁹ A nemzet kiberbiztonságának javításáról.

⁶⁰ PERETTI, - BARTOLOTTA: i. m.

⁶¹ PERETTI, - BARTOLOTTA: i. m.

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.⁶²

Hangsúlyos elemként kezelendő, hogy az iparágak 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 kiemelő szempont az együttműködés mellett az SBOM⁶³ 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 korábbi fejezetekben említésre került Log4Shell sebezhetőség tökéletes példa arra, hogy milyen súlyos következményeket von maga után egy átláthatatlan szoftverkomponens.⁶⁴ A szoftverterv tágabb értelemben a 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 korábbiakban az II.1. fejezetben részletesen bemutatott rendszerfejlesztési életciklus végső fázisban lévő szoftverek globálisan hozzáférhető adatbázisaira alkalmazandó követelményeket. Ezenfelül elősegíti a szoftvertervekkel foglalkozó közreműködők munkacsoportjainak működését.⁶⁵

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

⁶² Critical Software - Definition & Explanatory Material.

⁶³ Szoftverterv- software bill of materials.

⁶⁴ NIST SP: 800-161r1, 89. o., 192. o., 303. o.

⁶⁵ Lostri, Pell (2023).: i. m.

érdekében, hogy a kiberbiztonsági követelmények ne akadályozzák a digitális kereskedelmi forgalmat.⁶⁶ A tervezet elemként kiemeli a szoftvergyártók felelősségével összefüggésében továbbá azt, hogy korlátozásra kerül a biztonsági felelősség szerződéses⁶⁷ úton történő kizárása.⁶⁸ 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.⁶⁹

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 kénytelené 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 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.⁷⁰

⁶⁶ Jindal, Soliman :i. m.

⁶⁷ Ebben az esetben a szoftvergyártók piaci helyzetüket kihasználva az ÁSZF-ben foglaltak alapján minimalizálják felelősségüket.

⁶⁸ BORGIA,– AUSTIN: i. m.

⁶⁹ Teske,– Oh,: i.m.

⁷⁰ NIST SP 800-161r1 i. m.: 233. o.

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.⁷¹ 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.⁷² A speciális biztosítási fajta a szervezeteket érintő információbiztonsági támadásokra összpontosít. Az adattörlésekkel összefüggő kockázatok miatt a hagyományos kereskedelmi felelősségbiztosítások nem tartalmazzak 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 elengedhetlenné vált.⁷³ 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.⁷⁴

⁷¹ Teske, – Oh.: i.m.

⁷² Maia Hamin, Trey Herr, Will Loomis, Emma Schroeder, and Stewart Scott: How will the US counter cyber threats?

⁷³ Violino, Bob: Rising premiums, more restricted cyber insurance coverage poses big risk for companies

⁷⁴ Teske, – Oh.: i.m.

IV. CYBER RESILIENCE ACT JELENTŐSÉGE

Az elmúlt évek során a szoftverek rendkívül gyors fejlődése rámutatott arra a szempontrendszerre, hogy egyre jelentősebb mértékben válnak a közeljövőben mindennapi életünk szerves részévé. Ezzel összefüggésben elengedhetetlen, hogy az államok olyan szabályozási környezetet hozzanak létre, amely elősegíti az innovációt és lehetővé teszi a fejlesztések előrehaladását, így biztosítva, hogy a szoftvertermékeket forgalomba hozhassák és elérhetővé tehessék a felhasználói igények kielégítése érdekében.⁷⁵ A szoftverek gyakori sebezhetőségei miatt kibertámadások célpontjává válhatnak. A sebezhetőségek kihasználása láncreakciót indíthat el, amely hatalmas károkat okozhat bármely szervezetrendszerben. Emellett a megbízhatatlan szoftverek közvetlen veszélyt jelenthetnek az adatokra és a kritikus infrastruktúrákra, ezért elengedhetetlen az alapvető követelmények globális meghatározása.

A Cyber Resilience Act az Európai Unió legátfogóbb kiberbiztonsági szabályrendszerének tekinthető. A forgalomban lévő szoftvertermékek biztonságát célozza. Szabályozása részben túlmutat az Európai Unió határain és jelentős hatást gyakorolhat a nemzetközi piacra. A rendelet az egységes uniós piacra helyezi a hangsúlyt, ugyanakkor hatással van az Európai Unión kívüli szoftvergyártókra és fejlesztőkre is, akik az előírt feltételek betartása mellett szeretnék termékeiket forgalmazni az uniós piacon. A szigorú kötelezettségek versenyelőnyt is jelenthetnek az amerikai és ázsiai vállalatok számára a kisebb uniós vállalatokkal szemben, amelyek nehezen képesek megfelelni a követelményeknek. A szabályozás ugyanakkor növelheti a globális versenyképességet, és ösztönözheti a szoftvergyártókat a biztonságos termékek létrehozására.⁷⁶

Az Európai Unió folyamatosan törekszik a reziliencia kialakítására kiberfenyegetésekkel szemben, hogy garantálja a gazdaság biztonságát és védelmét. Napjainkban elengedhetetlen a kibertámadások időben történő azonosítása, felderítése, elhárítása. A CRA bevezetése hangsúlyos lépés volt az Európai Unió részéről, különösen az Amerikai Egyesült Államok kiberbiztonsági törekvéseinek mintájára. A szabályozási rendszer célja az Európai Unióban forgalmazott szolgáltatások és digitális eszközök - így például a szoftverek - biztonsági szintjének növelése. A CRA alapvető követelményeket támaszt a szoftvergyártók termékeivel

⁷⁵ László: i.m. 114.o.

⁷⁶ Mueck, M. D.; On, A. E. B.; Boisper, S. Du: (2023). Upcoming European Regulations on Artificial Intelligence and Cybersecurity. In: Communications Magazine, Évf. 61 szám 7. IEEE, New York. 98-102.o.

szemben. A rendelet megköveteli a fejlesztési és tervezési szakaszban, hogy a szoftverek képesek legyenek ellenállni az esetleges kibertámadásoknak. Ezzel összefüggésben lényeges kiemelni a security by design elvet, amelyet már a fejlesztés korai szakaszától alkalmazni kell. Fontos figyelembe venni a titkosítási megoldásokat a hozzáférések kezelése során, és törekedni kell a sebezhetőségek csökkentésére. Kiemelt szerephez jutott továbbá a frissítési szakasz, ahol alapvető követelmény a biztonságos frissítési mechanizmusok kialakítása. A gyártóknak ennek értelmében folyamatosan naplózniuk kell a frissítéseket és felülvizsgálniuk a fenyegetésekre okot adó eseteket.⁷⁷ A biztonsági jellegű tervezés mellett kiemelendő az adatvédelmet középpontba állító privacy by design elv. A fejlesztési szakasztól kezdve hasonlóan fontos szerepet kap az adatgyűjtés minimalizálása. A fejlesztés során folyamatosan szükséges adatvédelmi teszteleseket végezni az érzékeny adatok biztonsága érdekében. A frissítési szakaszban a gyártóknak szintén kötelező olyan adatvédelmi struktúrákat kialakítaniuk, amelyek minimalizálják a sebezhetőségeket.⁷⁸ Az Európai Unió felismerte a szoftverek forráskódjaiban rejlő potenciális kockázatokat, amelyek sebezhetőségi pontokat jelenthetnek a vállalatok és a fogyasztók számára. Egy 2021-ben készült uniós felmérésre utalva kiemelendő, hogy az európai kkv-k 28%-a tapasztalt kibertámadásra irányuló jelenséget.⁷⁹ Ennek érdekében átfogó szabályozás került kialakításra a szoftverfejlesztők és gyártók számára a termékeik kiberbiztonsági védelme érdekében. A kiberbiztonság preventív jellegével összefüggésben kiemelendő a műszaki ismeretekkel nem rendelkező alkalmazottak oktatása. Az incidensmenedzsment képességeinek fejlesztése elősegíti a kiberbiztonsági kockázatok időben történő észlelését.⁸⁰

Szükséges kiemelni a CRA hatásait az Európai Unión túli viszonylatokban is. Lényeges aspektusként kezelendők az Európai Unió és a NATO közös céljai a kiberbiztonság ellenálló képességének biztosítására. Vitathatatlan, hogy az Európai Unió határozott célt és közös irányt határozott meg tagállamai számára a kiberbiztonság területén. A NATO-nak összességében számos közös együttműködésre irányuló fellépése van az Európai Unióval a kiberbiztonság területén. Hangsúlyozandó, hogy a NATO sajátos kiberbiztonsági politikát és stratégiát folytat. A két szervezetrendszer közötti szoros együttműködés mindig is kihívást jelentett, ugyanakkor a kapcsolatok folyamatosan épülnek. A kölcsönös információmegosztás

⁷⁷ Itt utalnék a korábbi fejezetekben elhangzottakra a szoftverek életciklusára és az amerikai szabványok kapcsolódási pontjaira.

⁷⁸ AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE - 25. cikk.

⁷⁹ Miért fontos a kiberbiztonság és mibe kerülhet egy kibertámadás az érintetteknek?

⁸⁰ Krasznay Csaba(2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban, In: *Nemzet és Biztonság – Biztonságpolitikai Szemle*. Évf. 10 szám 3. Ludovika Egyetemi Kiadó, Budapest. 47. o.

vonatkozásában az együttműködés pozitív irányt mutat. A kiberbiztonsági stratégiákra irányuló tevékenységek kiterjednek az alapvető szolgáltatások biztonságára, mint például a kórházak és az energiahálózatok. A nagyobb kibertámadásokra adott válaszreakcióként szükséges kiemelni a partnerekkel való kölcsönös együttműködést, amely mélyíti a két szervezetrendszer közötti kapcsolatot. Ezt igazolja továbbá a CRA szabályozási rendszere, amely mind a szervezeti, mind a nemzeti szinten hangsúlyozza és kiegészíti a NATO stratégiai erőfeszítéseit.⁸¹ A CRA előtérbe helyezi az Európai Unió és a NATO közötti intézményi együttműködést, amely magában foglalja a kibertámadásokkal összefüggő válságkezelési eljárások kidolgozását és végrehajtását. Ezenfelül hangsúlyozódik a közös kiberbiztonsági jellegű továbbképzési események szervezése a közös oktatási és képzési követelmények tekintetében.⁸² A CRA megteremti a körülményeket a NATO Kibervédelmi Kiválósági Központjával⁸³ való szorosabb együttműködés érdekében. A CCDCOE nemcsak a kiberbiztonsági oktatás és kutatás terén jelentős, hanem a valós idejű kibertámadások elleni védekezési mechanizmusok gyakorlati tesztelésében és szimulációs képzésekben is kiemelkedő szerepet játszik. A CCDCOE kiemelt szerephez juthat a CRA rendelkezéseivel összefüggésben, ugyanis a szabványok közös megtervezése és a minimális követelményrendszerek kialakítása növelheti az Európai Unióval fennálló szervezeti kapcsolatokat. A rendelet szabályozása, amely a kibertér ellenálló képességének fejlesztésére irányul, összhangban áll a NATO stratégiai céljaival. Ennek keretein belül a CRA a legjobb kiberbiztonsági gyakorlatok alkalmazásával és biztonsági minimumszabványok meghatározásával segíti a tagállamokat a pontos és alapos kibervédelmi infrastruktúra kiépítésében. A CRA modellként szolgálhat a nemzetközi együttműködés szempontjából, mivel a védekezőközpontú kiberstratégiát helyezi a középpontba. A rendelet a védelmi képességek fejlesztésére összpontosít, és összhangot teremt az Európai Unió globális kiberstabilitási álláspontjával, ellentétben Kína és Oroszország offenzív kiberbiztonsági politikájával.⁸⁴ Ez a megkülönböztethetőség lehetőséget ad az Európai Unió számára, hogy megfelelő keretrendszert építsen ki a CRA alapján, amely hatékonyan képes kezelni a fejlődő kibertámadásokból eredő kihívásokat. Az uniónak előnyt jelent a védekező jellegű

⁸¹ Bihaly Barbara(2022): Kibervédelem a NATO-ban és az EU-ban. In: *Hadtudományi Szemle*, Évf. 15. szám 4, Ludovika Egyetemi Kiadó, Budapest. 46-47. o.

⁸² Rugge, F. (2012): "The case for NATO-EU cooperation in the protection of cyberspace,". In: *Third Worldwide Cybersecurity Summit (WCS)*, New Delhi, India, 1-10. o.

⁸³ Cooperative Cyber Defence Centre of Excellence (CCDCOE).

⁸⁴ Su, F.; Dovgal, L.; Saalman, L.:(2023) Advancing the Role of the European Union in Promoting Global Cyber Stability. In: Research Policy Paper, 2023/DECEMBER. SIPRI,Stockholm. 11. o.

szabályrendszer, mivel a nemzetközi együttműködések szempontjából kedvezőbb megvilágításba kerül a védekező jelleg kiemelése a kiberbiztonsági kérdésekben.

A Gazdasági Együttműködési és Fejlesztési Szervezet⁸⁵ irányelveivel összhangban a CRA törekszik a biztonságosabb digitális környezet kialakítására a következetes kiberbiztonsági követelmények meghatározásával a szoftverek vonatkozásában. Fontos megvizsgálni az OECD kiberbiztonsággal összefüggő irányelveit, mivel a kiberbiztonsági rendszernek olyan alapelvekre van szüksége, amelyek átfogó és szilárd alapot adnak. Az OECD kiberbiztonsági irányelvei alapvetően hasonlóan rögzítik a kockázatalapú megközelítést a sebezhetőségek szempontjából. Kiemelt szerepet tulajdonít az OECD a digitális tudatosságnak és a kiberbiztonsági szempontból történő kultúra elmélyítésének. A CRA rendelkezéseire hasonlóan az OECD irányelvei is hangsúlyozzák a felelősség kérdését. Az OECD felelősségi irányelvei a CRA alapkövének tekinthetők a szoftvergyártói felelősség megalapozásával összefüggésben. Az OECD jelentőséget tulajdonít a nemzeti és nemzetközi szinten túlmutató együttműködéseknek, amelyet a CRA megőrzött és alaposan kidolgozott.⁸⁶ Az OECD kiberbiztonsági alapelveinek és szabályozási mechanizmusainak integrálása jelentős hatással lehet a nemzetközi kiberbiztonsági szabványok formálására. Az OECD kiberbiztonsági alapelvei nemcsak a tagországok közötti együttműködést erősítik, hanem megteremtik a kiindulási alapot a CRA egyes rendelkezéseinek kidolgozásához.

A CRA vonatkozásában lényeges megvizsgálni a tárgyi, területi és személyi hatályát. A rendelet a gazdasági szereplőkre vonatkozik, akik kapcsolatban állnak a szoftverekkel. Többek között rendelkezik a gyártókról, szoftverfejlesztőkről és forgalmazókról, valamint a viszonteladókról, akik digitális termékeket szállítanak az európai piacra.⁸⁷ Alapvetően kijelenthető, hogy az Európai Unióban piacra kerülő összes olyan szoftverre vonatkozik a hatálya, amely a digitális rendszerekkel áll összefüggésben és hálózatokhoz kapcsolódhat. A rendelet magában foglalja ennek értelmében a kereskedelmi céllal forgalomba hozott nyílt forráskódú rendszerekhez, beágyazott rendszerekhez és IoT-eszközökhöz kapcsolódó szoftvereket. Számos szoftverkategóriát érint a rendelet kritikus jellegük miatt. Példaként említendő az operációs rendszerek, amelyek a korábbi fejezetekben kiemelt jellemzőkkel összefüggésben a számítógépes rendszerek alapvető működésében játszanak jelentős szerepet. Ezenfelül kiemelendők az alkalmazások, amelyek széles spektrumban kerülnek alkalmazásra

⁸⁵ Economic Co-operation and Development-OECD.

⁸⁶ OECD (2022), *OECD Policy Framework on Digital Security*. 14. o.

⁸⁷ <https://www.cyberresilienceact.eu/the-cra-explained/>.

az állami szektorokban és a magánszférában egyaránt. Az IoT-eszközök tekintetében lényeges kiemelni az Egyesült Államokban alkalmazott IoT Cybersecurity Improvement Act kapcsolatát a CRA szabályozásával. Alapvetően a CRA egy átfogó kiberbiztonsági keretrendszert teremt meg, amely magában foglalja az IoT-eszközök tanúsítási rendszereit és biztonsági felülvizsgálatát. Ezzel szemben megemlítendő a korábbi fejezetekben vizsgált szűkebb spektrumú amerikai szövetségi ügynökségeknek előírt beszerzési követelményrendszer az IoT-eszközökkel összefüggésben.

A CRA nyílt forráskódú szoftverekre gyakorolt hatása igencsak jelentős. A nyílt forráskódú szoftverek üzemeltetői kötelesek olyan belső kiberbiztonsági stratégiát bevezetni és a változásokat dokumentálni, amely elősegíti a biztonságos termékfejlesztést a szoftverek életciklusának kezdetétől. A rendelet kötelezi a gyártókat és forgalmazókat, hogy minden bekövetkezett kiberbiztonsági incidenst dokumentáljanak és jelentsenek az illetékes szerveknek. A folyamatos dokumentáció kiemelt szerepet játszik a sebezhetőségek kezelésében, mivel lehetővé teszi a fejlesztők számára a hatékonyabb problémaelhárítást. A stratégiai szervezet elősegíti a fejlesztők számára a sebezhetőségek gyors és átlátható bejelentését, amelyet a rendelet is megkövetel. A sebezhetőségek dokumentálása és kezelése mellett kiemelt szerepkörbe kerül a sebezhetőségi információk megosztása a nyílt forráskódú alkalmazó közösségi fejlesztőkkel. A rendszeres frissítések minimalizálják a sebezhetőségeket és segítenek folyamatosan megfelelni a CRA követelményeinek. A rendelet kiemeli a szoftverek üzemeltetőinek együttműködését a piacfelügyeleti hatóságokkal annak érdekében, hogy a nyílt forráskódú szoftvereket tartalmazó termékek kiberbiztonsági kockázatai minimalizálódjanak. Ez az együttműködés tájékoztatási kötelezettséget teremt a felek vonatkozásában, ugyanis a piacfelügyeleti hatóság indokolt kérésére a nyílt forráskódú szoftverek fejlesztői kötelesek transzparens tájékoztatást adni a hatóság számára.⁸⁸

Hasonlóan az amerikai kiberbiztonsági stratégiához, a CRA is előtérbe helyezi a fogyasztói tudatosság növelését. A rendelet középpontjában álló szoftvergyártók és forgalmazók keretrendszerének megteremtése mellett hangsúlyt fektet a fogyasztók kiberbiztonsággal összefüggő készségeinek fejlesztésére is. Az Európai Unió célja, hogy a felhasználók tájékozottan dönthessenek a digitális termékek vásárlásakor és alkalmazásakor. A rendelet kötelezettséget állít ezzel összefüggésben a gyártóknak, hogy részletes tájékoztatást kötelesek nyújtani a szoftvertermékeik jellemzőiről és a szoftver környezetének biztonsági minőségéről.

⁸⁸ CRA- Article 24.

A CRA deklarálja, hogy a gyártók kötelesek értesíteni a fogyasztókat a kiberbiztonsági incidensekről, amelyek kihatással lehetnek adataikra. Az értesítés nemcsak negatív incidensek jelentését foglalhatja magában, ugyanis értesítésként értelmezhető egy új frissítés közeljövőben történő bevezetése is. A fogyasztók jogosultak megvásárolt szoftvereik biztonságos használatára és az ütemezett fejlesztésekre. Ezzel összefüggésben a gyártók kötelesek hozzáférhetővé tenni szoftvereik verzióját és az ezekhez kapcsolódó frissítéseket. A szoftverek biztonságos alkalmazásából ered a fogyasztók adatainak fokozott védelme. Az értesítés kötelező jellegéből fakadóan a fogyasztóknak joguk van tudni, mikor kerülhetnek személyes adataik veszélybe. A kiberbiztonsági tudatosság növelésével összefüggésben cél a magánszektorban lévő gazdasági szereplők együttműködésének ösztönzése. A szabályozás középpontjába helyezi a fiatalok számára a kiberbiztonsági szektorban való elhelyezkedés lehetőségét szakképzésekkel.⁸⁹ A fogyasztói tudatossággal szoros összefüggésben áll a szabványokhoz való megfelelés kapcsán a rendeletben említett CE-jelölés⁹⁰, amely a kiberbiztonsági referenciát jelképezi. Érdemes kiemelni a kiberbiztonsági megfelelést szimbolizáló CE-jelzés megszerzésének folyamatát. Alapvetően szükséges, hogy a gyártóknak szoftvertermékeikkel kapcsolatban kockázatelemzést folytassanak az esetleges sebezhetőségek azonosítása érdekében. A kockázatelemzések következtében végrehajtott javító intézkedések elősegíthetik a termék megfelelését a biztonsági jelölés megszerzéséhez. A másik szükséges szempont az előírt központi szabványoknak való megfelelés, ugyanis biztosítani kell a gyártók számára a szoftvertermékek megfelelését az európai és nemzetközi előírásoknak és iránymutatásoknak. Szükséges jelen esetben is kiemelni a szoftverek életciklusának megfelelő fejlesztési és naplózási folyamatait. A fejlesztés kezdetétől zajló részletes dokumentáció is kiemelt követelmény a megfeleléssel kapcsolatos értékelési folyamat szempontjából. A jelzés megszerzéséhez szükségesek továbbá a gyártók és fejlesztők nyilatkozatai a termékek biztonságos állapotáról. A szoftvertermékek értékelésen esnek át, amelyet kockázati szempontok alapján végeznek el a gyártók önértékelése alapján, továbbá közreműködhetnek harmadik személyek a szakszerű értékelés érdekében. A CE-jelölést jól láthatóan, olvashatóan és letörölhetetlenül kell elhelyezni a terméken digitális elemekkel. A jelölést a digitális elemekkel ellátott termék forgalomba hozatala előtt kell elhelyezni, amely tartalmazza ezenfelül a gyártói szervezet azonosítóját.⁹¹

⁸⁹ CRA- Article 10.

⁹⁰ Azt jelzi, hogy értékelésük során az EGT-ben értékesített termékekről megállapítást nyert, hogy megfelelnek a magas szintű kiberbiztonsági, egészségügyi és környezetvédelmi követelményeknek.

⁹¹ CRA-Article 30.

A CRA célja összefoglalva egy edukált fogyasztói társadalom megteremtése. Ennek érdekében a szigorúan szabályozott jelentési kötelezettségek elősegítik a termékek biztonsági állapotát a piacon. A rendszeresen elvégzendő kötelező auditok a CE-jelzések vonatkozásában a kiberbiztonsági előírásoknak való megfelelést szolgálják. Ezzel összefüggésben egy új szemléletmód kialakítása figyelhető meg az Európai Unió kiberbiztonsági stratégiájában, amely a fogyasztók aktív résztvevőként történő bevonására összpontosít. Ennek következtében érvényre juthat teljes mértékben az elveken alapuló rendelkezések és technikai szabályok egyensúlya az európai adatbiztonsági és kiberbiztonsági célkitűzések vonatkozásában, amely a kockázatértékeléstől a tanúsítási rendszerek kialakításáig egy összehangolt rendszert teremt.⁹² A CRA szerinti tanúsítás alapként szolgálhat az európai és nemzetközi szabványok kidolgozásában és fenntartásában. Kiindulópontként említésre méltó a kölcsönös elismerés elve, amely a tagállamok vonatkozásában a tanúsított szoftvertermékek kölcsönös elismerését tükrözi a határokon átvéelő kereskedelem szempontjából. Lényeges kiemelni a közös tanúsítási keretrendszer vonatkozásában a gyártók közreműködését, amely a szabványok harmonizációjához vezethet. Ez csökkentené a tagállamok és gyártók közötti széttagoltságot, továbbá növelné a szoftvertermékek biztonsági szintjét európai és nemzetközi szinten is.

A sebezhetőségek kezelése érdekében a rendelet előírja a szoftvergyártók és forgalmazók számára, hogy speciális rendszereket alakítsanak ki a kibervédelmi incidensek bejelentésére és kezelésére. A szoftvergyártók kötelesek jelenteni minden súlyos biztonsági incidenst, amely a digitális elemeket tartalmazó termék biztonságára hatással van. A gyártóknak és forgalmazóknak világos és hatékony értesítési mechanizmusokat kell kialakítaniuk. Elsősorban az erre kijelölt uniós platformokon kell a jelentéseket megtenniük. Ezenfelül lehetőség van a fogyasztók közvetlen értesítésére, valamint automatizált jelzőrendszerek alkalmazására a sebezhetőségek jelzésére. A fogyasztók értesítése mellett fontos a nemzeti hatóságokkal való együttműködés, akik közreműködhetnek a fogyasztók tájékoztatásában és az incidensek kezelésében. Ezzel összefüggésben kiemelendő a digitális elemeket tartalmazó termék érintett felhasználóinak, és adott esetben valamennyi felhasználó részletes tájékoztatásának szükségessége az aktívan kihasznált sebezhetőségről. Lényeges tájékoztatást adni a kockázatcsökkentést elősegítő tevékenységekről és az incidens hatásainak mérséklésére

⁹² Mantelero, Alessandro; Et al (2020): The common EU approach to personal data and cybersecurity regulation. In: *International Journal of Law and Information Technology*, Évf. 28 szám 4. Oxford University Press, Oxford. 327-328. o.

alkalmazható korrekciós intézkedésekről is.⁹³ A nyílt forráskódú szoftverek fejlesztőinek be kell tartaniuk a jogszabály előírásait, amennyiben részt vesznek olyan termékek fejlesztésében, amelyek digitális elemeket tartalmaznak. A hálózatot és az érzékeny adatokat érintő súlyos biztonsági incidensek esetében a nyílt forráskódú szoftverek fejlesztőire tájékoztatási és egyéb helytállási kötelezettségek vonatkoznak.

A digitális elemeket tartalmazó termékek forgalomba hozatala esetén a szoftvergyártóknak biztosítaniuk kell termékeik megfelelőségét az előírt szabványoknak, amelyek részletes követelményeket támasztanak a tervezés, fejlesztési és gyártási szakaszra. A CRA konkrét követelményeket határoz meg a szoftverfejlesztők és gyártók számára, amelyek célja, hogy a szoftverek megbízhatóbbá és biztonságosabbá válhassanak a piacon. Lényeges kiemelni a biztonsági tervezés aspektusát, ugyanis szükséges, hogy a szoftverek fejlesztésének kezdeti szakaszától gondoskodjanak a biztonsági intézkedések érvényesítéséről. Már a tervezés során ügyelni kell a potenciális sebezhetőségekre. Ezzel összefüggésben utalok a korábbi fejezetekben kiemelt security by design elvre, amelynek célja, hogy a szoftverek forráskódja alapvetően a védelemre legyen megtervezve a sebezhetőségekkel szemben. A következő lényeges szempont a követelményrendszer kötelező frissítések szükségessége. A szoftvergyártók kötelesek biztosítani a rendszeres biztonsági frissítéseket a feltárt sebezhetőségek kezelésére. A frissítések közzétételével összefüggésben kiemelt hangsúlyt kap a gyors és hatékony együttműködés a végfelhasználó fogyasztók általi alkalmazhatóság vonatkozásában. Az ellenőrzés és átláthatóság érdekében kiemelten fontos a szoftverek fejlesztési és felhasználási láncának visszakövethetőségének rögzítése. A rendelet rögzíti a gyártók kötelezettségét az átláthatóságot elősegítő dokumentáció biztosítására, továbbá előírja az együttműködési kötelezettséget.

A rendelet megalkotása során problémaként merült fel a szoftverek életciklusával összefüggésben a frissítések fenntartásának időtartama. Kétséges ugyanis egy adott szoftver várható élettartalmát meghatározni, amennyiben az a piactól jelentős mértékben függ. Fontos kiemelni, hogy a rendelet jelenleg általános esetként legalább 5 éves intervallumot határozott meg. Ez azonban problémákhoz vezethet például az intelligens otthoni biztonsági rendszerek vonatkozásában, amelyek jelentősen 5 évnél hosszabb ideig kerülnek felhasználásra.⁹⁴ A szoftverek életciklusával összefüggésben a gyártók a támogatási időszakot úgy határozzák meg, hogy az tükrözze azt az időtartamot, amely alatt a termék várhatóan

⁹³ CRA- Article 14 – (3), (8)

⁹⁴EU cyber-resilience act , 8-9. o.

használatban lesz, különösen figyelembe véve a felhasználók ésszerű elvárásait, a termék jellegét és rendeltetését.⁹⁵

Kiemelt figyelmet kell fordítani a rendelet vonatkozásában a felelősségi rendszernek a szankciók tükrében. A rendelet értelmében a tagállami szintre kerül a kötelezettségek megsértésére irányadó szankciók mértékének megállapítása. A megállapított szankcióknak hatékonynak és arányosnak kell lenniük, hogy visszatartó erőként szolgáljanak. A CRA deklarálja, hogy a szoftverfejlesztők és forgalmazók kötelesek felelősséget vállalni termékeik biztonságáért. Amennyiben egy szoftver biztonsági problémák vonatkozásában sebezhetőségek miatt jelentős kárt okoz felhasználóinak, akkor a gyártó pénzbírsággal, korlátozó intézkedésekkel és további szankciókkal sújtható. A szabályozás meglehetősen szigorú rendelkezéseket fogalmaz meg a szoftverek biztonságának kialakítása érdekében.⁹⁶

A megfelelés érdekében a gyártók kötelesek körültekintően eljárni a harmadik féltől származó szoftverkomponensek beépítésekor. Biztosítaniuk kell, hogy a harmadik féltől származó szoftverkomponensek ne veszélyeztessék a digitális elemeket tartalmazó termékek biztonságát.⁹⁷ A körültekintő szemléletmódot megkívánó átvilágítási kötelezettség eredményes teljesítése érdekében az Európai Bizottság felhatalmazást kap jogi aktusok kiegészítésére és módosítására a részletszabályok kialakításának érdekében. Jelen aspektus vonatkozásában releváns ez a felhatalmazás abban az esetkörben, amikor nyílt forráskódú szoftverkomponenseket építenek be digitális elemeket tartalmazó termékekbe. Ezzel összefüggésben kiemelendő a biztonsági tanúsítási program létrehozása, amely lehetővé teszi a nyílt forráskódú szoftvereknek minősülő digitális elemeket tartalmazó termékek fejlesztői, felhasználói és más harmadik felek számára, hogy értékeljék az ilyen termékek e rendeletben meghatározott valamennyi követelménynek való megfelelését.⁹⁸

⁹⁵ CRA- Article 13.

⁹⁶ CRA-Article 64.

⁹⁷ CRA-Article 13 -(1), (5).

⁹⁸CRA- Article 25.

V. ÖSSZEGZÉS

Alapvetően szükséges megállapítani, hogy a kiberbiztonság vonatkozásában mérföldkőnek tekintendő Cyber Resilience Act keretein belül az Európai Unió kiemelt hangsúlyt fektet a szoftverek biztonságos működtetésére és folyamatosan védett fejlesztésére. A Cyber Resilience Act előtérbe helyezi az egységes uniós követelmények kialakítását, különös tekintettel a szoftverek rendszerfejlesztési életciklusára. A szabályozás szigorú követelményeket támaszt a szoftvergyártókkal szemben a sebezhetőségek kezelésére, a biztonság alapú tervezésére és a frissítésekre. A fogyasztói oldalt megvizsgálva megállapítható, hogy a CRA előtérbe helyezi a fogyasztói tudatosság fejlesztését a kiberbiztonság témakörével kapcsolatban. A CRA szabályozása egy kétoldalú helyzetet teremt, amely egyrészt szélesíti a szoftverfejlesztők és gyártók felelősségét, másrészt kiszélesíti a fogyasztók látókörét a kiberbiztonság tekintetében. A rendelet által előírt szigorú követelmények nagyobb felelősséget telepítenek a gyártókra; ugyanakkor fontos megvizsgálni ennek pozitív hatását a piacra. A követelményeknek való megfelelés tekintetében esélyt kapnak a piac kisebb szereplői is a kiberbiztonságilag biztonságos szoftverpiacra való bekerülés tekintetében. A szabályozás további céljaként tehát az fogható fel, hogy ösztönzi a piaci szereplők versenyképességét, és kialakít egy átláthatóbb piac a fogyasztóknak. Az Európai Unió hasonlóan az amerikai szabályozáshoz célként tűzte ki a sebezhetőségek csökkentését és a transzparencia elvének érvényesülését. Fontos azonban azt kiemelni, hogy a CRA és az amerikai szabályozások között számos hasonló kapcsolódási pont fedezhető fel. Ugyanakkor lényeges, hogy a két kiberbiztonsági rendszer közötti különbségek megértése érdekében összehasonlítást végezzünk.

A két rendszer közötti kapcsolat elemzésének egyik fő szempontja a célkitűzések jelentős hasonlósága. Alapvetően kijelenthető, hogy átlátható biztonsági szabályok és szabványok kialakítása szükséges a biztonságos szoftverek és komponenseik fejlesztése érdekében. A keretrendszerek központi elemeinek tekinthető mindkét oldalról a proaktív sebezhetőségkezelés. Ennek magyarázataként az amerikai oldalról a korábban elemzett 14028. számú rendelet szolgál. Ezzel összefüggésben az Európai Unió oldaláról a CRA is fokozott felülvizsgálati gyakorlatokat és ellenőrzéseket követel meg a szoftverek sebezhetőségeinek javítása érdekében. További azonos szempont figyelhető meg a gyártók és szoftverfejlesztők tekintetében, amely megköveteli a sebezhetőségek minimalizálását a korszerű kiberbiztonsági gyakorlatok alapján.

Az Európai Unió mellett az Egyesült Államok is törekszik a szoftverek átlátható fejlesztésére és az előzmények részletes listázására. Ennek érdekében említtem 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. Kiemelendő a NIST SP 800-53 szabvány, amely átfogó útmutatóként szolgál az adatvédelmi kontrollról a szoftverek biztonságos fejlesztése tekintetében. A CRA szabályozásához hasonlóan ez a szabvány is kiemelt jelentőséggel kezeli az életciklussal összefüggő szakaszokat, a frissítések eszközölését, valamint a sebezhetőségek központi bejelentését.

Az alapvető eltérés a két rendszer között a szabályozás jellegében figyelhető meg. Az Egyesült Államok aspektusát vizsgálva jellemző az ajánlott, megengedőbb követelményrendszer, amely irányadó a kidolgozott stratégia és szabványok vonatkozásában. Főként az önkéntes iparági szabványokra helyeződik a hangsúly. Ezzel szemben kiemelendő az Európai Unió kötelező érvényű és szigorú szabályozási keretrendszere a CRA vonatkozásában. A rendelet kötelezően ír elő ellenőrzéseket és felülvizsgálatokat a szoftverek tekintetében. Fontos azonban kiemelni, hogy az amerikai ajánlott jelleg szigorodását idézheti elő a hatályos kiberbiztonsági stratégia, különösen a 14028-as rendelettel összefüggésben.

A következő jelentős különbség a két szabályozási rendszerben az alkalmazásuk köre. A Cyber Resilience Act második legfontosabb jellemzője az átfogó jelleg. Az Európai Unió a CRA által megköveteli a széleskörű szabályozást minden hálózati kapcsolatot igénylő informatikai termék számára. Ezzel szemben az Egyesült Államokban kimondottan csak a kritikus infrastruktúrákra és a szövetségi rendszerekre összpontosítanak a fokozott biztonsági jelleggel, így a biztonsági keretrendszer kevésbé átfogó. A kiberbiztonsági megfeleléség érdekében az amerikai rendszer azonban kevésbé támaszt szigorú következményeket az Európai Unió által megkövetelt megfelelésséggel szemben. A transzparencia elvének érvényre jutásának érdekében a CRA meglehetősen szigorúbb bejelentési kötelezettségeket ír elő az ellátási láncok tisztasága és átláthatósága érdekében a sebezhetőségek orvoslása céljából. Jelen esetben is irányadó a korábban kiemelt fokozatos szigorodás az Egyesült Államokban a közeljövőben a hatályos kiberbiztonsági stratégia értelmében, különösen az 14028-as rendelettel összefüggésben.

A két szabályozási szempontrendszer összegzése megfelelően tükrözi az eltérő kiberbiztonsági preferenciákat és védelmi politikát. Fontos kiemelni, hogy az Egyesült Államokban jellemzőbb a rugalmas, kockázatalapú szabályozási keret, amely az iparágaknak

lényegesen nagyobb szabadságot biztosít a kiberbiztonsági intézkedések alkalmazásában. A pólus másik oldalán azonban kiemelendő az Európai Unió, amely a Cyber Resilience Act által deklarálja az alapvetően fontos követelményeket és szankciókat. Mindkét megközelítés a kiberbiztonsági kockázatok csökkentését célozza, de meglehetősen hasonló eszközökkel igyekeznek megvalósítani.

IRODALOMJEGYZÉK:

SZAKMAI CIKKEK, FOLYÓIRATOK:

1. Bihaly Barbara(2022): Kibervédelem a NATO-ban és az EU-ban. In: *Hadtudományi Szemle*, Évf. 15. szám 4, Ludovika Egyetemi Kiadó, Budapest.
2. 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.
3. Kovács László(2020): A kiberbiztonság és a kibernüveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. In: *Honvédségi Szemle – Hungarian Defence Review*, Évf. 148 szám 5, Honvéd Vezérkar, Budapest.
4. Krasznay Csaba(2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgáltatásban, In: *Nemzet és Biztonság – Biztonságpolitikai Szemle*. Évf. 10 szám 3. Ludovika Egyetemi Kiadó, Budapest.
5. László Gábor (2020): A nyílt forráskódú szoftverek szerepe a közigazgatásban. In Sasvári Péter szerk.: *Informatikai rendszerek a közszolgáltatásban II.*, Dialóg Campus, Budapest.
6. Mantelero, Alessandro; Vaciago Giuseppe; Esposito Maria Samantha; Monte, Nicole (2020):The common EU approach to personal data and cybersecurity regulation. In: *International Journal of Law and Information Technology*, Évf. 28 szám 4. Oxford University Press, Oxford.
7. Mueck, M. D.; On, A. E. B.; Boispéan, S. Du: (2023). Upcoming European Regulations on Artificial Intelligence and Cybersecurity. In: *Communications Magazine*, Évf. 61 szám 7. *IEEE, New York*.
8. Pankotay Fruzsina Magda - Szigeti Zsolt -Sótonyi Tamás - Pataki, László (2020) :Az informatikai termékek életciklusának sajátosságai. In: *Menedzsment válaszok a XXI. század gazdasági és társadalmi kihívásaira*, Inform Kiadó és Nyomda Kft., Budapest.
9. Radack, Shirley (2009): The System Development Life Cycle (SDLC) In: *Computer Security Division* - National Institute of Standards and Technology Publication, Gaithersburg.
10. Rugge, F. (2012): "The case for NATO-EU cooperation in the protection of cyberspace,". In:*Third Worldwide Cybersecurity Summit (WCS)*, New Delhi, India.
11. Su, F.; Dovgal, L.; Saalman, L.:(2023) Advancing the Role of the European Union in Promoting Global Cyber Stability. In: *Research Policy Paper*, 2023/December. SIPRI,Stockholm.

12. Szabó András(2018): TECHNIKAI KIBERBIZTONSÁGI GYAKORLATOK – NEMZETKÖZI KITEKINTÉS HADMÉRNÖK, XIII. Évfolyam 1. szám – 2018. március, NKE, Budapest.
13. Veer, Rob van der; Valkema, Menno; Guasconi, Fabio(2020): The role of the EU cybersecurity certification framework. In: Drogkaris, Prokopios ; Bourka, Athena: *Advancing software security in the EU*. Publications Office.

INTERNETES 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. A Windows XP, az Office 2003 és az Exchange 2003 támogatása véget ért (<https://tinyurl.com/ypwh6frh>)
3. Bart Lenaerts-Bergmans.: What Is Cyber Resilience? (<https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/cyber-resilience/>)
4. Borgia, Michael – Austin, Patrick: Overview of the National Cybersecurity Strategy (<https://tinyurl.com/3f3dhbcz>)
5. Christopher Burgess: Legacy systems are the Achilles’ heel of critical infrastructure cybersecurity (<https://tinyurl.com/5ejnb6f9>)
6. Critical Software - Definition & Explanatory Material, Executive Order 14028, Improving the Nation's Cybersecurity (<https://tinyurl.com/5n8jjz9d>)
7. Crooks Behind \$81M Bangladesh Bank Heist Linked To Sony Pictures Hackers (<https://tinyurl.com/3yuubeu8>)
8. Cyber Defense Agency: It's time to build cybersecurity into the design and manufacture of technology products. (<https://www.cisa.gov/securebydesign>)
9. Divyanshu Jindal, Mohammed Soliman: The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace? (<https://tinyurl.com/4uacp2hb>)
10. EU Cyber Resilience Act (<https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>)
11. EU Legislation in Progress (<https://tinyurl.com/462kse3e>)
12. Eugenia Lostri, Stephanie Pell: The Biden Administration’s Implementation Plan for the National Cybersecurity Strategy (<https://tinyurl.com/578876ru>)
13. Executive Order on Improving the Nation’s Cybersecurity (2021) (<https://tinyurl.com/yby46mmm>)
14. Gerhard Peters, John T. Woolley.: FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy Online (<https://tinyurl.com/ycx32pzy>)

15. Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order (<https://tinyurl.com/3ve2357t>)
16. Josh Fruhlinger: Equifax data breach FAQ: What happened, who was affected, what was the impact? (<https://tinyurl.com/4v4up449>)
17. Kerekes Gábor : Nyílt forráskódú szoftver – A felhasználás jogi vonatkozásai – Tévhiteket oszlatunk! (<https://tinyurl.com/d2h4vpp9>)
18. Kerner, Sean Michael.: 35 cybersecurity statistics to lose sleep over in 2024, Utal: WORLD ECONOMIC FORUM- Global Risks Report 2023(<https://tinyurl.com/5hfff3xc>)
19. Krizsán Bence.: Az Amerikai Egyesült Államok új Nemzeti Kibervédelmi Stratégiája (<https://tinyurl.com/2sj53kjv>)
20. Liao ,Annie - Johnson, Rex :Summary of the 2023 National Cybersecurity Strategy Part 2, (<https://tinyurl.com/2exvrdvr>)
21. 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>)
22. Miért fontos a kiberbiztonság és mibe kerülhet egy kibertámadás az érintettnek? (<https://shorturl.at/Zup0i>)
23. Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (<https://tinyurl.com/4yj6hc77>)
24. National Institute of Standards and Technology :Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (<https://tinyurl.com/5c7up5hv>)
25. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems(<https://tinyurl.com/bddw6x4t>)
26. OECD Policy Framework on Digital Security (<https://tinyurl.com/2xc2vez9>)
27. Patch Management (<https://tinyurl.com/w9bhruet>)
28. Peretti, Kimberly, Kiefer, Bartolotta, Kristen :Privacy, Cyber & Data Strategy Advisory: White House Releases National Cybersecurity Strategy (<https://tinyurl.com/4hnpw947>)
29. Roberta Freeman: White House releases National Cybersecurity Strategy (<https://tinyurl.com/y3apt8dt>)
30. Teske, David S. – Oh, Hyun Jai :Intellectual Property Advisory: New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable (<https://tinyurl.com/2mjwmvzh>)
31. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years (<https://tinyurl.com/hancy6ty>)
32. Understanding ISO 27001 and Its Relevance to Software Development (<https://tinyurl.com/y657aatf>)
33. Violino, Bob: Rising premiums, more restricted cyber insurance coverage poses big risk for companies (<https://tinyurl.com/yck6rsvz>)
34. Vulnerability and Threat Trends Report 2023 (<https://tinyurl.com/2s4f6asu>)

35. What is DevOps? (<https://www.ibm.com/topics/devops>)
36. What is product lifecycle management (<https://tinyurl.com/5n7pzxp7>)
37. What is SOAR? (<https://tinyurl.com/mwjpkp48>)
38. What You Need to Know About Log4Shell, the Vulnerability Affecting Log4j (<https://tinyurl.com/4n942p28>)
39. EU cyber-resilience act (<https://tinyurl.com/462kse3e>)

SZABÁLYOZÁSI HÁTTÉR.:

1. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
2. Cyber Supply Chain Management and Transparency Act
3. Cybersecurity Labeling for Internet of Things (<https://tinyurl.com/4xzu3u72>)
4. Executive Order 14028, Improving the Nation's Cybersecurity
5. ISO/IEC 27001. számú szabvány
6. National Cybersecurity Strategy Implementation Plan Version 2 (NCSI Plan Version 2)
7. National Institute of Standards and Technology Special Publications:
 - 800-115
 - 800-218
 - 800-207
 - 800-161r1
 - 800-53

FELHASZNÁLT ÁBRÁK.:

1. Ábra: Általános életciklus görbe.: Pankotay Fruzsina Magda - Szigeti Zsolt -Sótonyi Tamás - Pataki László: i.m. 67. o. Utal: Bíró-Szigeti, S. (2016.) Marketing-termékpolitika
2. Ábra: Az Amerikai Egyesült Államok kiberbiztonsági stratégiája. (NCSI Plan Version 2)
3. Ábra.: Az Amerikai Egyesült Államok kiberbiztonsági stratégiájának 3. pillére (NCSI Plan Version 2)