

SLRG Research Paper – Nr. 2025/1.



SmartLaw Research Group

**Kiberbiztonság beépítése a
szoftverfejlesztésbe: A Cyber Resilience Act
szabályozási hatása**

Kelemen Roland – Medváczy Ádám

Az infokommunikációs technológiák elterjedése a kétezres évek elején rávilágított arra, hogy egyre jelentősebb mértékben válnak mindennapi életünk szerves részévé. A technológiákat működtető szoftverek elterjedése és gyors fejlődése számos kiberbiztonsági kihívást vetett fel. Kutatásomban a mindennapokban használt szoftverek kiberbiztonsági jelentőségét vizsgálom, különös tekintettel az alapvető követelményekre. Kiemelem az informatikai termékek szempontjából a szoftverek rendszerfejlesztési életciklusának fontosságát. Elemzem az Európai Unió szoftverekre vonatkozó kiberbiztonsági rendeletét, különösen a Cyber Resilience Act jelenlegi hatásait a szoftveriparban.

Kulcsszavak: Szoftverbiztonság; kiberreziliencia; kiberbiztonság, szabályozás

I. BEVEZETŐ

A kiberbiztonság jelentősége az utóbbi években egyre inkább előtérbe került, különösen a digitális szolgáltatások és a szoftverfejlesztés területén. Az Európai Unió 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 és szabályozás terén. Tanulmányom az európai szabályozás 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. Tulajdonképpen elengedhetetlenné válnak a

hatékony kiberbiztonsági intézkedések. Az Európai Unió korán felismerte a terület fontosságát és számos változtatást vezetett be. Kiemelt cél, hogy növeljék a szoftverek kiberrezilienciáját, és erősítsék az IT-biztonságot. Az európai szabályozás általi megközelítés, amely mostanra a Cyber Resilience Act keretében öltött formát. Előírta a szoftverfejlesztési életciklus minden szakaszában a kiberbiztonsági követelményeket, valamint kiterjesztette azokat a digitális termékek biztonságos alkalmazására és forgalmazására.

A tanulmány áttekinti különösen a szoftverfejlesztési életciklus során alkalmazott kiberbiztonsági intézkedések és követelmények integrációját. Az elemzés során külön figyelmet fordítok 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 szabályozás következményeit a gyártói felelősség, a fogyasztói tudatosság és az iparági szabványok terén.

Célom átfogó képet nyújtani az Európai Unió szabályozási rendszerének megközelítéséről, különös tekintettel a szoftverek rendszerfejlesztési életciklusára és az iparági követelmények szigorítására. A Cyber Resilience Act szabályozási kerete, amely a szoftverek és digitális termékek biztonságára vonatkozó előírásokat szigorítja. Jelentős hatással van a globális szoftverpiacra, valamint a kiberbiztonság jövőbeli alakulására.

E tanulmány célja annak bemutatása, hogy az Európai Unió szabályozási rendszere miként képes választ adni a modern digitális kihívásokra, valamint hogyan erősíthetik a kiberbiztonságot egy átfogó és egységes szabályozási rendszer kiépítésével. Az elemzés rávilágít arra is, hogy a Cyber Resilience Act szabályozása milyen hatással lehet 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 terepükben

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

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.)

³KEREKES Gábor: Nyílt forráskódú szoftver – A felhasználás jogi vonatkozásai – Tévhiteket 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.

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 folyamatokra. Az ISO/IEC 27001 az információbiztonságmenedzsment 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 tesztek 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

⁵ Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

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

⁷ Understanding ISO 27001 and Its Relevance to Software Development

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 frissítések 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 lejártá 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.

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

⁸ Patch Management

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

¹⁰ System Development Life Cycle

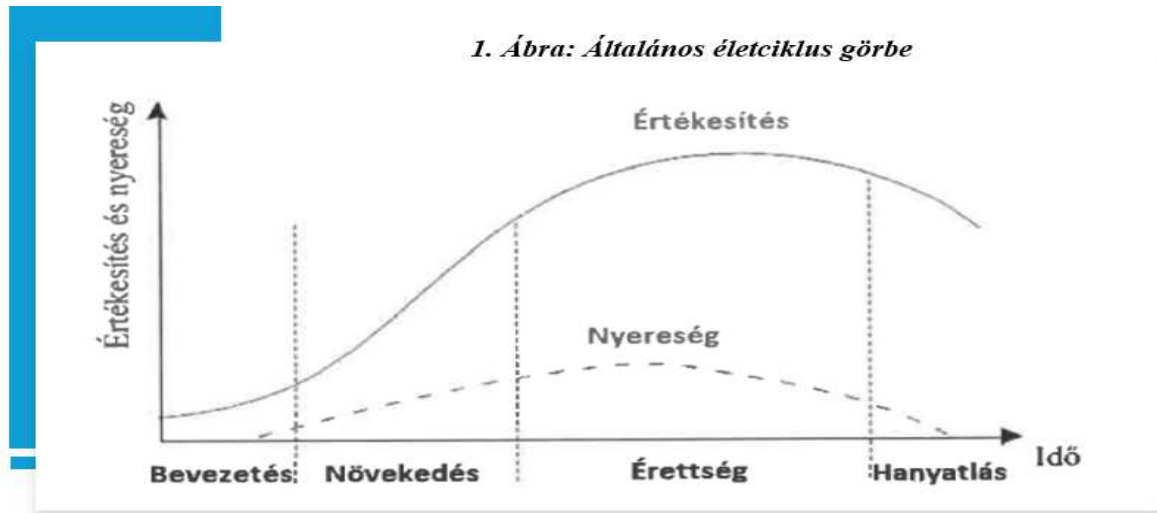
intézkedéseket, akkor komoly következményekkel kell számolnunk. Példaként kihangsúlyozandó az Equifax 2017-ben történt adatvédelmi incidense, amelynek következtében több százmillió ügyféladatot szivárogtattak ki a hitelinformációs ügynökségtől. A vállalatot egy fogyasztói panaszokkal foglalkozó internetes 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 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

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.

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-termékpolitika



(Forrás: PANKOTAY, Et al. (2020): i.m. 67. o. Utal Bíró-Szigeti, S. (2016.) Marketing-termékpolitika)

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 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

¹⁴ LÁSZLÓ Gábor: i.m. 108. o.

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 fázisa* 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.

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

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.

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 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

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.

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

²⁰ What is DevOps?

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.

III. 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.²¹ 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.²²

Az Európai Unió folyamatosan törekszik a reziliencia kialakítására kiberfenyegetésekkel

²¹ LÁSZLÓ: i.m. 114.o.

²² MUECK, M. D.; ON, A. E. B.; BOISPEAN, 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, 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 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.²³ 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 teszteléseket végezni az érzékeny adatok biztonsága érdekében. A frissítési szakaszban a gyártóknak szintén kötelező olyan adatvédelmi struktúrákat kialakítaniuk, amelyek minimalizálják a sebezhetőségeket.²⁴ 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.²⁵ 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.²⁶

²³ Itt utalnék a korábbi fejezetekben elhangzottakra a szoftverek életciklusára és az amerikai szabványok kapcsolódási pontjaira.

²⁴ AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE - 25. cikk.

²⁵ Miért fontos a kiberbiztonság és mibe kerülhet egy kibertámadás az érintettnek?

²⁶ KRASZNAY Csaba (2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban, In: *Nemzet és Biztonság* –

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 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.²⁷ 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.²⁸ A CRA megteremti a körülményeket a NATO Kibervédelmi Kiválósági Központjával²⁹ 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

Biztonságpolitikai Szemle. Évf. 10 szám 3. Ludovika Egyetemi Kiadó, Budapest. 47. o.

²⁷BIHALY Barbara (2022): Kibervédelem a NATO-ban és az EU-ban. In: *Hadtudományi Szemle*, Évf. 15. szám 4, Ludovika Egyetemi Kiadó, Budapest. 46-47. o.

²⁸RUGGE, 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.

²⁹Cooperative Cyber Defence Centre of Excellence (CCDCOE).



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.³⁰ 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 szabályrendszer, mivel a nemzetközi együttműködések szempontjából kedvezőbb megvilágításba kerül a védekező jelleg kiemelése a kiberbiztonsági kérdésekben.

A Gazdasági Együttműködési és Fejlesztési Szervezet³¹ 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 rendelkezéseihez 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.³² 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.

³⁰ 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.

³¹ Economic Co-operation and Development- OECD.

³² OECD (2022), *OECD Policy Framework on Digital Security*. 14. o.

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.³³ 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 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.³⁴

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.

³³The CRA, explained <https://www.cyberresilienceact.eu/the-cra-explained/>.

³⁴ AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/2847 RENDELETE a digitális elemeket

tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet)

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.³⁵

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 szoftvertermékek jellemzőiről és a szoftver környezetének biztonsági minőségéről. 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.³⁶ A fogyasztói tudatossággal szoros összefüggésben áll a szabványokhoz való megfelelés kapcsán a rendeletben említett CE-jelölés³⁷, amely a kiberbiztonsági

³⁵ CRA- Article 24.

³⁶ CRA- Article 10.

³⁷ Azt jelzi, hogy értékelésük során az EGT-ben értékesített termékekről megállapítást nyert, hogy

referenciát jelképezi. Érdeemes kiemelni a kiberbiztonsági megfelelést szimbolizáló CE-jelzés megszerzésének folyamatát. Alapvetően szükséges, hogy a gyártóknak szoftvertermékekkel 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 értékelésén 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.³⁸ 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.³⁹ A CRA szerinti tanúsítás alapként szolgálhat az európai és nemzetközi szabványok kidolgozásában és fenntartásában.

megfelelnek a magas szintű kiberbiztonsági, egészségügyi és környezetvédelmi követelményeknek.

³⁸ CRA-Article 30.

³⁹MANTELERO, 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.

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 kockázatsökkentést elősegítő tevékenységekről és az incidens hatásainak mérséklésére alkalmazható korrekciós intézkedésekről is.⁴⁰ 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

⁴⁰ CRA- Article 14 – (3), (8)

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.⁴¹ A szoftverek életciklusával összefüggésben a gyártók a támogatási időszakot úgy határozzák meg, hogy az tükrözze azt az időtartamot, amely alatt a termék várhatóan használatban lesz, különösen figyelembe véve a felhasználók ésszerű elvárásait, a termék jellegét és rendeltetését.⁴²

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

⁴¹CRA, 8-9. o.

⁴² CRA- Article 13.

intézkedésekkel és további szankciókkal sújtható. A szabályozás meglehetősen szigorú rendelkezéseket fogalmaz meg a szoftverek biztonságának kialakítása érdekében.⁴³

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.⁴⁴ 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 esetben, 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.⁴⁵

ÖSSZEGZÉS

Alapvetően szükséges megállapítani, hogy a kiberbiztonság vonatkozásában mérföldkőnek tekintendő Cyber Resilience Act. Az Európai Unió kiemelt hangsúlyt fektet a szoftverek biztonságos működtetésére és folyamatosan védett fejlesztésére. A CRA 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 tervezésre és a frissítésekre.

A fogyasztói oldal vizsgálata alapján megállapítható, hogy a CRA előmozdítja a fogyasztói tudatosságot a kiberbiztonság területén. Növeli a gyártók felelősségét, és egyben bővíti a fogyasztók látókörét is. A szigorú előírások lehetővé teszik, hogy kisebb szereplők is beléphessenek a biztonságos szoftverpiacra, amennyiben megfelelnek a követelményeknek. A CRA így ösztönzi a versenyképességet és átláthatóbb piacot alakít ki.

A CRA előírja a sebezhetőségek kezelésére és a transzparenciára vonatkozó gyakorlatok alkalmazását. Kiemelten fontos a fokozott felülvizsgálat és ellenőrzés annak érdekében,

⁴³ CRA-Article 64.

⁴⁴ CRA-Article 13 -(1), (5).

⁴⁵CRA- Article 25.

hogy a szoftverek biztonsági hibáit időben kezeljék. A szabályozás a korszerű kiberbiztonsági eljárásokra épít, és megköveteli a fejlesztők és gyártók aktív közreműködését a biztonsági kockázatok csökkentésében.

A CRA keretében hangsúlyt kap az úgynevezett SBOM (Software Bill of Materials) is, amely a szoftverek komponenseinek átláthatóságát hivatott biztosítani, amely eszközként szolgál a sebezhetőségek és ellátási láncban rejlő kockázatok csökkentésére. A szabályozás részét képezik a frissítésekre és hibabejelentésekre vonatkozó követelmények, különös tekintettel az életciklus teljes szakaszaira.

A Cyber Resilience Act egyik legfontosabb jellemzője az átfogó hatály, amely minden hálózatra kapcsolódó termékre vonatkozik. A CRA kötelező bejelentési kötelezettségeket is előír a szoftverek és az ellátási lánc biztonsága érdekében. Ezáltal egy szigorúbb, strukturáltabb rendszer jön létre, amely biztosítja a transzparens piacot és a gyors reagálást a kiberbiztonsági kihívásokra.

Végül a CRA szabályozása kifejezi az Európai Unió elköteleződését a kiberbiztonság jogilag kötelező erejű szabályozási célja mellett.

A kötelező ellenőrzések és megfeleléségi követelmények megteremtik azt a környezetet, amelyben a gyártók nem csupán

technikai, hanem jogi felelősséggel is tartoznak a termékeik biztonságáért. Véleményem szerint ez a megközelítés növeli a bizalmat a digitális termékek iránt az egységes európai piacon.

FELHASZNÁLT IRODALOM

1. KERÉKES Gábor: Nyílt forráskódú szoftver – A felhasználás jogi vonatkozásai – Tévhiteket oszlatsunk! (<https://tinyurl.com/d2h4vpp9>)
2. LÁSZLÓ Gábor (2020): *A nyílt forráskódú szoftverek szerepe a közigazgatásban*. In Sasvári Péter szerk.: *Informatikai rendszerek a közszolgáltatásban II.*, Dialóg Campus, Budapest.
3. 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.
4. 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.
5. RADACK, Shirley (2009): *The System Development Life Cycle (SDLC)* In:



- Computer Security Division - National Institute of Standards and Technology* Publication, Gaithersburg.
6. MUECK, M. D.; ON, A. E. B.; BOISPEAN, S. Du: (2023). *Upcoming European Regulations on Artificial Intelligence and Cybersecurity*. In: *Communications Magazine*, Évf. 61 szám 7. IEEE, New York.
 7. 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.
 8. BIHALY Barbara (2022): *Kibervédelem a NATO-ban és az EU-ban*. In: *Hadtudományi Szemle*, Évf. 15. szám 4, Ludovika Egyetemi Kiadó, Budapest.
 9. RUGGE, F. (2012): *"The case for NATO-EU cooperation in the protection of cyberspace,"*. In: *Third Worldwide Cybersecurity Summit (WCS)*, New Delhi, India.
 10. 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. 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.
 12. *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities* (<https://tinyurl.com/4yj6hc77>)
 13. *What You Need to Know About Log4Shell, the Vulnerability Affecting Log4j* (<https://tinyurl.com/4n942p28>)
 14. *Understanding ISO 27001 and Its Relevance to Software Development* (<https://tinyurl.com/y657aatf>)
 15. *Patch Management* (<https://tinyurl.com/w9bhruuf>)
 16. *A Windows XP, az Office 2003 és az Exchange 2003 támogatása véget ért* (<https://tinyurl.com/ypwh6frh>)
 17. FRUHLINGER Josh: *Equifax data breach FAQ: What happened, who was affected, what was the impact?* (<https://tinyurl.com/4v4up449>)
 18. BURGESS Christopher: *Legacy systems are the Achilles' heel of critical infrastructure cybersecurity* (<https://tinyurl.com/5ejnb6f9>)
 19. *What is DevOps?* (<https://www.ibm.com/topics/devops>)
 20. *Miért fontos a kiberbiztonság és mibe kerülhet egy kibertámadás az érintettnek?* (<https://shorturl.at/Zup0i>)



21. *OECD Policy Framework on Digital Security*
(<https://tinyurl.com/2xc2vez9>)
22. *The CRA, explained*
(<https://www.cyberresilienceact.eu/the-cra-explained/>)
23. 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
24. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/2847 RENDELETE a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828
- irányelv módosításáról (a kiberrezilienciáról szóló rendelet)
25. National Institute of Standards and Technology Special Publications:
- o 800-115
 - o 800-218



IMPRESSZUM

Szerző(k):
Kelemen Roland
Medváczy Ádám

Kézirat lezárásának ideje:
2025.05.09.

Szerkesztők:
Farkas Ádám PhD
Kelemen Roland
Glavanits Judit PhD
Karácsony Gergely PhD
Keserű Barna Arnold PhD
Király Péter Bálint PhD
Németh Richárd
Spitzer Jenő

Kiadó:
Smart Law Research Group

Elérhetőségek:
<http://smartlawresearch.hu/>

ISSN:
2732-3846

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

A sorozat célja a SmartLaw Research Group, illetve annak tagjai és esetleges külső együttműködők által végzett kutatások részeredményeinek közzététele a szakmai, tudományos megvitathatóság érdekében, illetve a későbbi publikációk előkészítésének támogatása érdekében.

