



INTÉZMÉNYI TUDOMÁNYOS DIÁKKÖRI KONFERENCIA

2023. május 12.

ÉLELMISZER ELLÁTÁSI LÁNC DIGITALIZÁCIÓJÁNAK LEHETŐSÉGEI

Opportunities for the Digitalisation of the Food Supply Chain

Készítette: **Elek Vilmos András**
CCX9UL
Élelmiszermérnök B.Sc.
Nappali
Budai Campus

Témavezető: Dr. Baranyai László
központvezető/tanszékvezető/egyetemi tanár, MATE
Élelmiszertudományi és Technológiai Intézet

Témavezető: Üveges András József, tudományos segédmunkatárs,
NKE NBI / NKE KMDI

Lehetséges OTDK szekció: „agrártudományi”

**Budapest
2023.**

Tartalomjegyzék

Bevezetés	3
Tudományos probléma	6
Tudományos eredmények	7
Egyértelműsítés	7
Forráskutatás	8
Milyen problémákra lehet megoldás a digitális transzformáció?	9
Szabályzási környezet.....	19
Adatbiztonság, informatikai biztonság, információbiztonság és kiberbiztonság	23
Az információbiztonsággal kapcsolatos problémák és fenyegetések.....	24
Intézkedések incidensek esetén.....	34
Az ellátó láncok információbiztonságával kapcsolatos problémák és fenyegetések	37
Összefoglalás	45
Irodalomjegyzék.....	47

Bevezetés

A korszerű mezőgazdaságot, élelmiszeripart és élelmiszerkereskedelmet, így az élelmiszer ellátó láncokat is elérték az IPAR4.0¹ vívmányai és a fogyasztók is egyre több igényt fogalmaznak meg a láncok szereplői felé. Mindez arra kényszeríti a szereplőket, hogy a legfejlettebb műszaki megoldásokat alkalmazzák a versenyképességük fenntartása, a fogyasztók bizalmának megőrzése érdekében. A modern ellátási láncok kifinomultságának növekedésével, valamint azzal, hogy ezek az ágazatok egyre inkább az intelligens technológiákra és az összekapcsolt rendszerek (IoT-rendszerek) folyamataira támaszkodnak, egyre több kiber- és nemzetbiztonsági kockázatot hordoznak magukban.

Az élelmiszeripari és a mezőgazdasági rendszereket kiszolgáló informatikai infrastruktúra egyike azon létfontosságú információs infrastrukturális ágazatoknak, amelyek potenciális célpontjai lettek a kiberbűnözőknek, ezért nemcsak az emberi hibákból és szakmai ismerethiányból eredő problémákkal kell megküzdenie az élelmiszerellátó láncoknak, hanem a rosszindulatú, komplex támadásokkal is. Emellett fontos kiemelni azt, hogy egyre több esetről ad hírt a média, ez pedig tovább fokozhatja a „dicsőségre”, illetve jelentős profitra vágyó bűnözők elszántságát.

Az ágazat szereplőinek számtalan problémával kell szembenéznük:

- a fogyasztók igényei (biztonságos élelmiszerellátás, széleskörű tájékoztatás, speciális igények kielégítése stb.),
- új élelmiszerbiztonsági követelmények,
- a versenytársak innovatív megoldásai,
- a különböző, a láncban érdekelt gazdasági szektorok követelményei (logisztika, IT²),
- a láncok összetettségének problémái (pl. kommunikáció, szervezetek különböző szintű rugalmassága, eltérő vállalati kultúrák, eltérő finanszírozási hajlandóság a fejlesztések terén, öröklött rendszerek állapota, a digitális transzformáció³ különböző foka, joghatósági problémák stb.),

¹ Az IPAR 4.0 célkitűzése, hogy rugalmasabbá, hatékonyabbá és ügyfélközpontúvá tegye a fejlesztési és gyártási folyamatokat. A legkorszerűbb intelligens információ- és kommunikációtechnológia szorosabbra fűzi a termékfejlesztés, a gyártás és a logisztika, valamint az ügyfelek közötti kapcsolatot.

² Információtechnológia - Information Technologies

³ A digitális transzformáció egy széleskörű, sok mindenre kiterjedő fogalom, amely magában foglal minden olyan kezdeményezést, amely a digitális technológia felhasználásával javítja az üzleti folyamatokat és tevékenységeket, hogy azok jobban megfeleljenek a mai fogyasztók igényeinek és maximalizálják a nyereséget. (Iron Mountain vállalat definíciója,

- az új technológiák bevezetésének kockázatai,
- a szabályozási környezet problémái (jogalkotás, jogalkalmazás és a jogkövető magatartás kikényszerítése),
- a társadalom általános elvárásai (etikus termelés és kereskedelem, minél kisebb ökológiai lábnyom, klímavédelem stb.),
- a fizikai térből kibertérbe áthelyezett folyamatok biztonsági problémái,
- előre nem prognosztizálható események, például a mesterséges intelligencia alkalmazásának hihetetlen sebességű térhódítása, a COVID19 világjárvány, vagy az orosz-ukrán fegyveres konfliktus, amely akár az élelmiszer láncok időleges vagy végleges megszakadását is okozta⁴.

A mezőgazdaság és az élelmiszergyártás, valamint kereskedelem területén ezen problémák kezelése elválaszthatatlan egymástól és mind a napi működés, mind pedig a fejlesztések és az új technológiák bevezetése során figyelemmel kell lenniük az ezekből fakadó kockázatokra.

A szervezetek „egyéni” problémái mellett új kihívásokat is generált az IPAR 4.0. Az ellátó láncok összetettsége miatt a mezőgazdasági és az élelmiszeripari ágazat elér arra a pontra, amikor a szektor szinte minden szereplője vagy befolyásoló vagy kikényszerített tagja egy, vagy akár több láncnak. A „farmtól az asztalig” ökoszisztémák akár több ezres nagyságrendben is tartalmaznak különböző súlyú szereplőket, a koordinálásukra pedig olyan rendszereket kell kiépíteni, amelyek már csakis új műszaki megoldások, innovatív technológiák alkalmazásával működtethetők. Az ágazat kénytelen olyan technológiákra támaszkodni, mint a kapcsolódó eszközök (IoT-rendszerek, „dolgok internete”⁵), a felhőalapú számítástechnika⁶, a nagy adat⁷

https://assets.website-files.com/5fd507477771ae17633bd8f8/600ad2c05d76ad3b46c6b66b_im_digital-transformation_hu_web01.pdf

⁴ Szegedi, Karine: COVID-19 has broken the global food supply chain. So now what? Deloitte.

<https://www2.deloitte.com/ch/en/pages/consumer-business/articles/covid19-has-broken-the-global-food-supply-chain.html>

⁵ A dolgok internete az összes alrendszerrel, folyamattal, belső és külső tárgyakkal, beszállítói és vevői hálózattal összekapcsolt informatikai rendszerekre utal, amelyek egymással és az emberekkel kommunikálnak és együttműködnek. European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 22.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

⁶ A felhőalapú számítástechnika az interneten keresztül történő, igény szerinti hozzáférést jelent a számítási erőforrásokhoz - alkalmazásokhoz, szerverekhez (fizikai és virtuális szerverekhez), adattároláshoz, fejlesztési eszközökhöz, hálózati képességekhez és más eszközökhöz -, amelyeket egy felhőszolgáltató (cloud services provider, CSP) által kezelt távoli adatközpontban tárolnak. A felhőszolgáltató ezeket az erőforrásokat havi előfizetési díj ellenében bocsátja rendelkezésre, vagy a felhasználás alapján számlázza ki. What is cloud computing? <https://www.ibm.com/topics/cloud-computing>

⁷ A nagy adatmennyiségű, nagy sebességű és/vagy nagy változatosságú információs eszközök, amelyek az információfeldolgozás költséghatékony, innovatív formáit igénylik, amelyek lehetővé teszik a jobb betekintést, a döntéshozatalt és a folyamatok automatizálását. Gartner Glossary. <https://www.gartner.com/en/information-technology/glossary/big-data>

kezelés, a mesterséges intelligencia⁸, a blokklánc⁹, a virtualizáció¹⁰ és sok más egyéb, jelenleg fejlesztés alatt álló elgondolás.

A digitalizáció lépéseit azonban nem mindig lassú, megfontolt döntések előzik meg, hanem olyan váratlan események is kikényszerítenek radikális változtatásokat, mint például a COVID19 világjárvány idején a távmunka¹¹ gyors elterjedése¹² vagy egy jelentős zsarolóvírusos támadás.¹³ A napi szokásos problémák mellett még a leggondosabban megtervezett új projektek bevezetése és működtetése során is merülhetnek fel olyan körülmények, amelyek újdonság erejével érik a szereplőket. Ilyenek lehet pl. interoperabilitási¹⁴ problémák, a digitalizációs eltérések, a szervezetek rugalmatlansága, véletlenszerű és kiszámíthatatlan jogalkotás stb., a rapid, tűzoltásszerű megoldások pedig tovább növelik a sebezhetőséget. Ilyen, a kiberbiztonsági statisztikákban is megjelenő problémát jelentett – többek között – a világjárvány alatt a pár nap alatt a teljes adminisztratív állomány távmunkára átállítása és a biztonságos kommunikációs csatornák kialakítása.

A szereplők helyzetét tovább bonyolítja, hogy többnyire nem csak egy ellátólánc tagjai, így a biztonságot fenyegető támadás bármikor és számos irányból érkezik.

Az új helyzetekhez nemcsak az élelmiszerlánc ellátó lánc tagjai alkalmazkodnak, hanem a különböző motivációjú, bűncselekmények elkövetésében jártas személyek is. A hagyományos fizikai támadások (pl. betörés, kamion rakományának eltulajdonítása stb.) és fehérgalléros bűncselekmények („corporate fraud”¹⁵) mellett a kibertérbe megjelent folyamatok miatt

⁸ A mesterséges intelligencia (MI) fejlett elemzési és logikai alapú technikákat alkalmaz, beleértve a gépi tanulást is, az események értelmezésére, a döntések támogatására és automatizálására, valamint a cselekvések végrehajtására. Gartner Glossary. <https://www.gartner.com/en/information-technology/glossary/artificial-intelligence>

⁹ A blokklánc egy hálózat összes résztvevője által megosztott, kriptográfiailag aláírt, visszavonhatatlan tranzakciós feljegyzések bővülő listája. Minden rekord tartalmaz egy időbélyeget és hivatkozási linkeket a korábbi tranzakciókra. Ezen információk segítségével bárki, aki hozzáférési jogokkal rendelkezik, vissza tudja követni egy tranzakciós eseményt, annak történetének bármely pontján, bármely résztvevőhöz tartozóan. A blokklánc az elosztott főkönyvek tágabb koncepciójának egyik architektúráis kialakítása. Gartner Glossary. <https://www.gartner.com/en/information-technology/glossary/blockchain>

¹⁰ Virtualizálás: az intelligens gyár virtuális másolata az érzékelőadatok virtuális üzemmódokkal és szimulációs modellekkel való összekapcsolásával jön létre. European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 21.

¹¹ Például WorkFromHome és a WorkFromEverywhere

¹² <https://www.enisa.europa.eu/topics/wfh-covid19>

¹³ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>

¹⁴ a kiber-fizikai rendszerek (munkadarab-hordozók, összeszerelő állomások és termékek) lehetővé teszik, hogy az emberek és az intelligens gyárak összekapcsolódjanak és kommunikáljanak egymással. European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 21. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

¹⁵ A „vállalati csalás” természetes személy(ek) vagy vállalat által elkövetett olyan illegális tevékenységek összefoglaló elnevezése, amelyeket tisztességtelen vagy etikátlan módon hajtanak végre. Általában az ilyen jellegű „vállalati csalás” és egyéb bűncselekmények célja, hogy az elkövető személy, személyek csoportja vagy vállalat előnyhöz jusson. A vállalati csálási sémák túlmutatnak az egyes alkalmazottak alkalmazotti pozícióján és összetettségük, valamint a vállalkozásra, a többi alkalmazottra és a külső felekre gyakorolt gazdasági hatásuk jellemzi őket.

Bár a „vállalati csalás” sokféleképpen történhet és gyakran úgy valósul meg, hogy kihasználják a bizalmas információkhoz vagy az érzékeny eszközökhöz való hozzáférés lehetőségét használják ki, majd ezeket az eszközöket hasznosítás céljából

támadására is fel kell készülnie a biztonsági szakembereknek. Ráadásul a támadás nemcsak a „saját” élelmiszerlánc megtámadásából eredhet, hanem az ellátóláncon keresztül is¹⁶.

Tudományos probléma

Napjainkban az élelmiszerellátó lánc szereplői kénytelenek azzal szembesülni, miszerint nem az a kérdés, hogy éri-e az adott szervezetet (kiber)támadás, hanem az, hogy mikor. Miközben a vállalatok működésének, illetve a lánc célja nem a folyamatos készenlét a támadások kivédésére, hanem a fogyasztók számára biztonságos, gazdaságos és zavartalan élelmiszerellátás biztosítása. Az iparág jellegzetessége továbbá, hogy egy támadás hatása az élelmiszerellátó láncban többirányú lehet, azaz kihat a kiskereskedőkre (kiürülnek az üzletekben a polcok), másik irányban pedig a termelőknek okozhat kárt. Lehetséges azonban olyan esemény is, amely mindkét irányba hat, különösen akkor, ha az szezonális munkálatok (pl. aratás, szüret stb.) idején következik be.

A szektorban használt automatizált rendszerek különösen sérülékenyek. Ha például egy szelepeket vezérlő, hőmérsékletet figyelő vagy az élelmiszerhez adott adalékanyagok keverékét szabályozó számítógépes rendszert manipulálnak, üzemszerű működését megzavarják, az komoly élelmiszerbiztonsági problémát jelenthet, ha pedig a médiába is bekerül a támadás híre, az akár országos méretű pánikot okoz. Következménye lehet a támadásnak továbbá, hogy az érintett vállalat hírneve és cégértéke károsodik, a helyreállításhoz pedig professzionális hírnévmenedzsmentre és komoly erőforrások bevonására van szükség. A helyzetet súlyosbítja az is, hogy az incidens a fogyasztókban nemcsak a megtámadott, hanem a versenytársak termékeivel szemben is bizalmatlanságot kelthet. A kibertámadás ráadásul akár verseny-eszköz is lehet, különös tekintettel a DarkNeten megrendelhető zsarolóvírusos támadásokra¹⁷.

felhasználják. A bűncselekményeket gyakran törvényes üzleti gyakorlatok vagy cserék mögé rejtik az elkövetők annak érdekében, hogy a tiltott tevékenységüket leplezzék.

¹⁶ Pl.: a támadók a Kaseya szoftveren lévő megbízható kapcsolat kihasználásával szereztek kezdeti hozzáférést a Kaseya ügyfeleihez, az MSP-khez (managed services providers, menedzselt szolgáltatók); a támadók utasításokat és parancsokat tudtak küldeni az ügyfelekre telepített szoftvereknek. A végrehajtási fázisban a támadók REvil zsarolószoftvert telepítettek a célpontra. A zsarolóprogram ezután folytatta a fájlok és mappák titkosítását. A támadók – egyéb követelések mellett – 70 millió dolláros összeget követeltek a Kaseyától és közvetve az ügyfeleitől, cserébe egy olyan fájldekódolóért cserébe, amely lehetővé teszi az érintett eszközök elérhetőségének helyreállítását az összes érintett rendszerben. A tárgyalások eredményeként sem a Kaseya, sem az érintett ügyfelek nem fizették ki a váltságdíjat. Egy fájldekódolót szereztek, nem tudni, hogyan, és sok rendszert sikerült helyreállítani. Összességében az ellátási láncot érintő incidens több mint 50 MSP-t és 800-1500 vállalatot érintett (összesen 37 000 Kaseya-ügyfelet). ENISA Threat Landscape for Ransomware Attacks. July 2022. p. 34-35.

¹⁷ Ransomware as a Service, RaaS: olyan üzleti modell, amelyben a fenyegetést jelentő csoportok felajánlják szoftverplatformjukat külső partnereknek, hogy támadásokat hajtsanak végre

Tudományos eredmények

Jelen dolgozatomban azt vizsgálom, milyen új technológiákkal, információbiztonsági fenyegetésekkel és egyéb problémákkal szembesülhetnek az élelmiszerellátó láncok. Két olyan projektet mutatok be közelebbről azért, hogy felhívjam a figyelmet arra, milyen területeken és milyen gondolatok mentén vágnak bele jelentős digitalizációs projektekbe a vállalkozások úgy, hogy a legmodernebb technológiát hívják segítségül (jelen esetben a blokklánc technológiát). Ezen kívül bemutatok egy olyan esetet is, amely során egy nagy multinacionális cég, a JBS Foods úgy vált zsarolóvírus áldozatává, hogy ez több országban is jelentős problémát okozott az élelmiszerellátásban. Céлом az, hogy számba vegyem, a digitalizáció milyen kockázatokat és fenyegetéseket jelent, illetve az információbiztonság terén milyen lehetőségei vannak a szervezeteknek és az élelmiszerellátó láncoknak annak érdekében, hogy a láncok biztonsága elvárt szintű legyen.

Egyértelműsítés

Az első ipari forradalom időszaka az 1700-as évek végén kezdődik, amikor a gőzerő a mechanikus termeléssel kombinálva a termelés iparosodásához vezetett. A második ipari forradalom – többek között – az elektromosság elterjedésének és a futószalagok rendszerbe állításának köszönhető, és az 1800-as évek közepétől kezdve tömegtermeléshez vezetett. A harmadik ipari forradalom az elektronika és az informatika a globalizációval együtt nagymértékben felgyorsította az iparosodást, és az 1970-es években kezdődött.

Az IPAR 4.0 kifejezést először a német kormány használta. „Ez a kifejezés a gyártás technológiai változásainak egy sorát írja le és foglalja össze, valamint meghatározza egy koherens politikai keret prioritásait, amelynek célja a német ipar globális versenyképességének megőrzése. Koncepcionális, mivel egy megfigyelt jelenség megértésének módját határozza meg, és intézményi, mivel keretet biztosít a kormány és az üzleti élet képviselői által meghatározott és támogatott politikai kezdeményezésekhez, amelyek egy kutatási és fejlesztési programot mozgatnak.

Az IPAR 4.0 a termelési folyamatok olyan szervezését írja le, amely az értéklánc mentén egymással autonóm módon kommunikáló technológián és eszközökön alapul: a jövő »intelligens« gyárának¹⁸ modellje, ahol a számítógépes rendszerek figyelemmel kísérik a fizikai

¹⁸ Intelligens gyár (smart factory) és a kapcsolódó "jövő gyára" ("factory of the future") kifejezés példázza az IPAR 4.0 keretében megvalósuló néhány technikai újítást, például az információs és kommunikációs technológiák integrációját a termelési folyamatba, és azt, hogy ezek hogyan valósulhatnak meg a gyakorlatban. European Parliament. Directorate General

folyamatokat, létrehozzák a fizikai világ virtuális másolatát, és önszerveződési mechanizmusok alapján decentralizált döntéseket hoznak. A koncepció figyelembe veszi a feldolgozóipar fokozódó számítógépesítését, ahol a fizikai tárgyak zökkenőmentesen integrálódnak az információs hálózatba. Ennek eredményeképpen »a gyártórendszerek vertikálisan hálózatba kapcsolódnak a gyárakon és vállalatokon belüli üzleti folyamatokkal, horizontálisan pedig a térben szétszórott értékhálózatokkal, amelyeket valós időben lehet kezelni - a megrendelés leadásának pillanatától egészen a kimenő logisztikáig«¹⁹.²⁰

A "tárgyak internete", mind a "szolgáltatások internete"²¹ kifejezés az IPAR 4.0 elemeinek tekinthető, a digitalizációs technológiák (felhőalapú számítástechnika, nagy adat technológia, mesterséges intelligencia, blokklánc stb.) a fizikai korlátokat lebontják, és a folyamatok digitalizálása megkönnyíti azok optimalizálását, és a hatékonyabb, versenyképesebb termelést.

Forráskutatás

Az IPAR 4.0 hatásairól és a digitális transzformációról számos önálló tanulmány és tanulmánykötet jelent meg, és bár a szakirodalom – a témára tekintettel – csak rövid időtávra nyúlik vissza, számtalan forrás található az interneten. Ezek jellemzője, hogy gyakran elméleti felvetéseket tartalmaznak és olyan technológiák alkalmazására tesznek javaslatot, amelyek jelenleg még kísérleti stádiumban vannak, bevezetésük jelentős anyagi erőforrást igényel úgy, hogy előnyeik és hátrányaik meg nem teljeskörűen ismertek. Az új technológiák veszélyeit általában a különféle nemzeti hatóságok, illetve a nemzetközi szervezetek is hangsúlyozzák, ezért ezek megismerése feltétlen ajánlott.

A gyakorlati tapasztalatok terén alapvetően az általam bemutatott három esettel kapcsolatban kerestem az Interneten olyan forrásokat, amelyek – a lehetőségekhez mérten – objektíven mutatják be az eseményeket, valamint a lehetséges következmények leírásához a WHO

for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 22.

¹⁹ Forschungunion/acatech, Securing the future of German manufacturing industry Recommendations for implementing the strategic initiative INDUSTRIE 4.0, 2013. http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf p. 9.

²⁰ European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 20. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

²¹ A szolgáltatások internete olyan belső és szervezetközi szolgáltatásokra utal, amelyeket az értéklánc résztvevői kínálnak és használnak, és amelyeket a big data és a felhőalapú számítástechnika hajt. European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 22. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

tanulmányát²² hívtam segítségül. A szabályozási környezet feltárása során kibervédelmi és adatvédelmi szakemberektől kértem segítséget, hogy minél több információt szerezhessenek az információbiztonság és a modern technológiák kapcsolatáról, valamint a fenyegetésekről. Itt elsősorban az uniós jogalkotásra, illetve a hazai szabályozásra hívták fel a figyelmemet.

A kiberbiztonsági kockázatok ismertetése esetében – alapvetően – az Európai Kiberbiztonsági Ügynökség (ENISA)²³ dokumentumaira támaszkodom, illetve a személyes adatokkal kapcsolatban (adatbiztonság terén) az Európai Adatvédelmi Testület (EDPB)²⁴ iránymutatásaira. A téma aktualitása miatt számtalan egyéb forrást is felhasználtam, például a kiberfenyegetettséget kutató vállalkozások dokumentumait, illetve nem uniós hatóságok jelentéseit, mivel a globalizáció és az ellátó láncok komplexitása miatt ezek is hasznos információkat tartalmazhatnak az élelmiszerellátó láncok tagjai számára.

Milyen problémákra lehet megoldás a digitális transzformáció?

A nagy élelmiszerkereskedelemmel foglalkozó vállalkozások, illetve ellátó láncok számos olyan problémával szembesülnek, amelyek esetében a hagyományos eszközök²⁵ körében nem találunk megoldást²⁶. Jelen dolgozatomban két olyan példát mutatok be, amelyek esetében a kiemelt problémák megoldása érdekében digitális transzformációhoz folyamodtak a szereplők.

Termékvisszahívások menedzselése

Az élelmiszerláncban az egyik kiemelt tevékenység a termékek visszahívásának menedzselése. Ennek prioritását mutatja, hogy emberéletek múlnak a gyors és hatékony intézkedésen, mivel a fogyasztókat és az üzleteket is időben tájékoztatni kell arról, milyen terméket vigyenek vissza,

²² WHO's first ever global estimates of foodborne diseases find children under 5 account for almost one third of deaths, 3 December 2015 GENEVA, <https://www.who.int/news/item/03-12-2015-who-s-first-ever-global-estimates-of-foodborne-diseases-find-children-under-5-account-for-almost-one-third-of-deaths>

²³ European Union Agency for Cybersecurity (ENISA) – az Európai Unió Kiberbiztonsági Ügynöksége az Európai Unió azon 2004-ben létrehozott ügynöksége, amely a kiberbiztonság magas szintű, közös európai szintű megvalósítását tűzte ki célul. Az ENISA hozzájárul az EU kiberpolitikájához, a kiberbiztonsági tanúsítási rendszerekkel fokozza az IKT-termékek, IKT-szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és más uniós szervekkel, valamint segíti Európát a jövő kiberbiztonsági kihívásaira való felkészülésben. Az ENISA a tudásmegosztás, a kapacitásépítés és a tudatosság növelése révén a legfontosabb érdekelt felekkel együttműködve azon dolgozik, hogy erősítse a bizalmat az összekapcsolt gazdaságban, növelje az Unió infrastruktúrájának ellenálló képességét, és végső soron elősegítse az európai társadalmak és polgárok digitális biztonságát. (<https://www.enisa.europa.eu/about-enisa/what-we-do>)

²⁴ European Data Protection Board (EDPB) - az Európai Adatvédelmi Testület független európai szerv, mely egy ernyő alatt egyesíti az Európai Gazdasági Térség országainak nemzeti adatvédelmi hatóságait, valamint az európai adatvédelmi biztost (EDPS). Az EDPB biztosítja az általános adatvédelmi rendelet (GDPR) és a bűnüldözési irányelv (LED) következetes alkalmazását, és biztosítja az együttműködést, többek között a végrehajtás terén (https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_hu)

²⁵ például hagyományos könyvelési-ügyviteli technikák, számlázó rendszerek

²⁶ Például: nagy mennyiségű, számos helyről származó adat analízise, reklámok testre szabása stb.

illetve vegyenek le az üzletek polcairól. A gyors intézkedés nemcsak életet menthet, hanem ellensúlyozhatja a cég hírnevét ért károkat, sőt az elkötelezett, a fogyasztókért „minden követ megmozgató” reakálás növelheti a vásárlók bizalmát az adott üzletlánc, illetve gyártó irányába.

A termékvisszahívások azonban jelentős többlet költséget is okozhatnak akkor, ha nem egyértelmű, pontosan mely terméket kell visszahívni – azaz nem sikerül gyorsan meghatározni, honnan is származik az adott áru, pontosan melyik termelő vagy gyártó a felelős az egészségre káros élelmiszerért.

A probléma nagyságrendjét egy 2015-ös Egészségügyi Világszervezet (WHO²⁷) jelentés²⁸ is alátámasztja, mely szerint évente tízből egy ember betegszik meg szennyezett élelmiszer fogyasztása miatt, és 420 ezer ember hal meg ennek következtében. Az öt év alatti gyermekek különösen nagy kockázatnak vannak kitéve. Évente 125 ezer gyermek hal meg élelmiszer eredetű betegségben, azaz az összes ilyen haláleset csaknem egyharmada (30%) gyermek, miközben a népességnek csak 9%-át teszik ki ez a korosztály.

Ez a WHO jelentés 31 kórokozó - baktériumok, vírusok, paraziták, toxinok és vegyi anyagok - által okozott élelmiszer eredetű betegségek számát becsüli meg. A megállapításai alapján

- a **hasmenéses betegségek** felelősek az élelmiszer eredetű betegségek globális számának több mint feléért, évente 550 millió megbetegedést és 230 ezer halálesetet okozva.
- a **gyermekek** különösen ki vannak téve az élelmiszer eredetű hasmenéses betegségek kockázatának, évente 220 millióan betegszenek meg és 96 ezren halnak meg.
- a hasmenéses megbetegedéseket gyakran a norovírussal²⁹, Campylobacterrel³⁰, nem tífuszos szalmonellával és patogén *E. coli* baktériummal³¹ szennyezett nyers vagy nem kellően feldolgozott hús, tojás, friss termékek és tejtermékek fogyasztása okozza.
- az élelmiszerből eredő betegségeknek globális szinten további fő okozói a tífusz, a hepatitis A, a *Taenia solium*³² és az aflatoxin³³.

²⁷ World Health Organization - Egyesült Nemzetek Szervezetének egyik szervezete, a nemzetközi közegészségügy koordináló hatóságaként működik. Székhelye a svájci Genf városban található. A szervezet alapokmánya 1948. április 7-én lépett életbe.

²⁸ WHO's first ever global estimates of foodborne diseases find children under 5 account for almost one third of deaths, 3 December 2015 GENEVA, <https://www.who.int/news/item/03-12-2015-who-s-first-ever-global-estimates-of-foodborne-diseases-find-children-under-5-account-for-almost-one-third-of-deaths>

²⁹ A norovírus hirtelen kialakuló, súlyos hányással és hasmenéssel járó, gyomor- és bélgyulladást okozó fertőzést vált ki.

³⁰ A Campylobacter-fajok általában az állatok, jellemzően a madarak ürülékében találhatók meg.

³¹ Tekintettel arra, hogy az *E. coli* jellemzően vastagbél-baktérium, a jelenléte vízben vagy élelmiszerben székletszennyezettségre utalhat. A közegészségügyben az *E. coli*, indikátorbaktériumnak tekintendő, ez jelzi a víz és az élelmiszer tisztaságát/szennyezettségét.

³² Egy galandféreg.

³³ A mikotoxinok közül az aflatoxinokat tekintik a legveszélyesebb mérgezőanyagoknak.

- bizonyos betegségek, például a nem tífuszos szalmonella által okozott betegségek a világ minden régiójában, azaz a magas és az alacsony jövedelmű országokban egyaránt közegészségügyi problémát jelentenek.
- más betegségek, mint például a tífusz, az élelmiszerből származó kolera és a kórokozó *E. coli* által okozott betegségek sokkal gyakoribbak az alacsony jövedelmű országokban, míg a *Campylobacter* gyakori kórokozó a magas jövedelmű országokban.

A jelentés az európai régióval kapcsolatban kiemeli, hogy

- itt a legalacsonyabb az élelmiszer eredetű megbetegedések becsült száma. Európában évente több mint 23 millió ember betegszik meg nem biztonságos élelmiszer miatt és ötezer ember hal meg ennek következtében.
- a hasmenéses megbetegedések teszik ki az élelmiszer eredetű megbetegedések többségét, a leggyakoribb a norovírusfertőzés (becslések szerint 15 millió eset), ezt követi a campylobacteriosis (közel ötmillió eset).
- a nem tífuszos szalmonellózis okozza a legtöbb halálesetet (évente kétezer).
- az élelmiszerből származó toxoplazmózis az összes élelmiszer eredetű betegség akár 20%-át is okozhatja és évente több mint egymillió embert érint a régióban.
- a *Listeria* spp. fertőzés becslések szerint évente 400 ember halálát okozza.

Az európai régióval kapcsolatban mindenképpen kiemelendő az a fertőzés, amely egyben az *E. coli* fertőzés veszélyességét is jelzi. Ez az a 2011-es észak-németországi eset, amelyben a zöldségekben található *Escherichia coli* O104:H4 baktériumtörzs okozott halálos megbetegedéseket. Több mint négyezer ember fertőződött meg és több, mint 50 ember halt meg a járványban. Azt feltételezik, hogy a fertőzés forrása egy alsó-szászországi csírafarm volt.

A Nemzeti Élelmiszerlánc-biztonsági Hivatal (NÉBIH) honlapja is tartalmaz fontos információkat az *E. coli* fertőzésekkel kapcsolatban,³⁴³⁵ illetve kiemeli, a termékvisszahívások esetén „nehézséget jelent a vásárlók elérése, értesítése”. Nagyon fontos az is, hogy a gyártó, illetve forgalmazó a teljes élelmiszerellátási láncban nyomon tudja követni, hogy a

³⁴ <https://portal.nebih.gov.hu/-/kerdezz-felelek-az-e-coli-fertozesekrol>

³⁵ https://portal.nebih.gov.hu/veszelyzona?p_p_id=com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_mvcPath=%2Fview_record.jsp&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_redirect=https%3A%2F%2Fportal.nebih.gov.hu%2Fve-szelyzona%3Fp_p_id%3Dcom_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_recordId=1833815&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_version=1.0&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_editable=true&_com_liferay_dynamic_data_lists_web_portlet_DDLDisplayPortlet_INSTANCE_UVUpLWPxptBA_formDDMTemplateId=0

visszahívással érintett termékek honnan származnak, illetve a visszahívás elrendelésének időpontjában hol vannak – azaz az adott egészségre veszélyes termék még a logisztikai rendszerben, az üzletekben vagy már a vásárlók asztalán van.

A Walmart³⁶ római salátás incidense³⁷ mutatott rá arra, hogy mennyire fontos az, hogy a termékek gyorsan visszahívhatók legyenek. A visszahívásos folyamatnak alapvető követelménye, hogy gyorsan beazonosítható legyen a fertőzött (veszélyes termék) pontosan honnan származik (melyik mezőgazdasági termelőtől, annak is melyik üzeméből/telepéről), hol csomagolták, hogyan szállították, mely üzletekben kerültek ki a polcokra és kik vásárolták meg. A „farmtól az asztalig” követés egyik legnagyobb nehézsége a pontos származási hely beazonosítása, a római salátás ügyben például hét napot vett igénybe ez a folyamat. Ez az egy hetes időtartam ráadásul a szakemberek szerint nem is számított rossz teljesítménynek figyelembe véve a Walmart méretét és a beszállítói összetettségét.

A sebesség azonban kiemelkedően fontos egy olyan ügyben, amelyben az Amerikai Egyesült Államok 36 állama érintett és 210 ember fertőződött meg, 96 embert kezeltek kórházban és öt személy meghalt az *E. coli* O157:H7 fertőzés miatt. A Walmart éppen ezért úgy döntött, szükséges a termékkövetés digitális transzformációja.

A római salátás esemény során a származást felderítő csapatnak – követve a „hagyományos” eljárásrendet – kapcsolatba kellett lépnie a beszállítóval, papíralapú nyilvántartásokat kellett beszereznie és ezek alapján kapcsolatba kellett lépnie azzal a céggel, amelyik a terméket importálta, illetve a Walmart elosztóközpontjába szállította. A római saláta teljes útját fel kellett deríteni, melynek része

- a termelő (termesztés/betakarítás);
- a feldolgozóüzem (megtisztítás, szeletelés és becsomagolás);
- elosztóközpont (szétválogatás és teherautókra rakás a kiszállításhoz);
- üzletek (teherautóról lepakolás, hűtőbe tétel majd eladótérbe kerülés);
- eladótérből a vásárlóhoz kerül (személyes vásárlás vagy kiszállítás).

³⁶ Az amerikai Wal-Mart Stores céget 1962-ben alapította Sam Walton. A világ egyik legnagyobb kiskereskedelmi cége és árbevétele alapján a világ legnagyobb vállalata.

³⁷ In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens, <https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens>

Azonban egy üzletben nemcsak egy termék van, így amennyiben ezt a folyamatot megszorozzuk egy átlagos Walmart élelmiszerboltban található 70 ezer különféle élelmiszerrel, akkor szinte leküzdhetetlen, „tű a szénakazalban” típusú kihívással szembesül a cég.

A hét napig tartó kutatási idő következménye az volt, hogy további megbetegedések megelőzése érdekében – a pontos származási hely beazonosításának hiánya miatt – nemcsak a ténylegesen fertőzött terméket kellett eltávolítani a polcokról, hanem a más helyről származó római saláta termékeket is. Ráadásul a pénzügyi veszteség mellett egy ilyen akció nemcsak az adott termékkel szembeni bizalmat rombolja, hanem az egész élelmiszerlánc biztonságába vetett hitet is.

„Bár az FDA³⁸ és a CDC³⁹ tájékoztatni tudta a fogyasztókat, a termelőket és a kiskereskedőket arról, hogy a betegségekkel összefüggésbe hozott római saláta a Yuma termesztési régióból származik, az egészségügyi tisztviselők és az iparági szakemberek nem tudták gyorsan meghatározni, hogy mely tételek voltak érintettek és melyek nem.

Ez azt eredményezte, hogy több millió zsák és fej római salátát kellett kivonni a piacról, és a termesztési régiótól függetlenül elvesztette a fogyasztók bizalmát a római salátával szemben, valamint sokak, köztük a termelők gazdasági megélhetését is negatívan érintette.”⁴⁰

A Walmart elhatározta, hogy a papír alapú, illetve számtalan különféle adatbázisban megtalálható adatokból álló, a termékviSSzahívás teljesítését emberfeletti erőfeszítéssé tevő „hagyományos” rendszerét új alapokra helyezi. Az IBM-mel közösen blokklánc alapú⁴¹ termék nyomon követést vezettek be⁴² - többek között – az epernél, a mangónál, a zöld leveles termékeknél. Az új technológia alkalmazása az adott termék hét napos visszakövetési idejét – a termék csomagolásán található QR-kód⁴³ beolvasásával – 2,2 másodpercre csökkentette le.

³⁸ Food and Drug Administration, anyaszervezet: United States Department of Health and Human Services

³⁹ Centers for Disease Control and Prevention, anyaszervezet: United States Department of Health and Human Services

⁴⁰ részlet a Walmart beszállítóknak írt leveléből, Food Traceability Initiative Fresh Leafy Greens, September 24, 2018, https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001

⁴¹ a blokklánc egy megváltoztathatatlan, decentralizált főkönyvet biztosít a szervezetek számára, amely lehetővé teszi az adatok és a digitális eszközök nyomon követését az interakciók során. Bármilyen nyomon követhető a blokklánc segítségével, és ez az ígéret és előfeltételezés az, ami vonzó lehet a logisztikai és egyéb - belső és külső - folyamataikat racionalizálni kívánó vállalkozások számára.

⁴² „Hyperledger Fabric”, Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric/blockchain, https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf (Case Study)

⁴³ Quick Response, azaz „gyors válasz”-t jelent, mivel a felhasználó általi beolvasás, valamint a beolvasás utáni válaszügy is rendkívül gyors.

A Walmart a beszállítóitól megkövetelte a blokklánc alapú nyilvántartást, így nemcsak az üzletlánc, hanem a fogyasztó is ma már pillanatok alatt megtudhatja, hogy a kezében tartott római saláta pontosan melyik farmról származik.

„A friss zöldségek beszállítóitól elvárjuk, hogy termékeiket másodpercek - és nem napok - alatt vissza tudják követni a gazdaság(ok)hoz (termelési tételenként). Ennek érdekében a beszállítóknak az IBM Food Trust hálózat segítségével digitális, végponttól végpontig tartó nyomonkövethető eseményadatokat kell rögzíteniük.

Megértjük, hogy ehhez Önnek is együtt kell működnie a beszállítóival. Ezért lehetővé tesszük, hogy ezt a követelményt két szakaszban teljesítsék.

1. Közvetlen beszállítók - közvetlen beszállítóinknak 2019. január 31-ig meg kell felelniük az egylépéses visszakövethetőségnek a blokklánc-hálózaton.

2. Végponttól végpontig - ezt követően beszállítóinknak a vertikális rendszereiken belül vagy a beszállítóikkal együtt 2019. szeptember 30-ig kell dolgoznia azon, hogy lehetővé tegyék a gazdaságig tartó végponttól végpontig tartó nyomon követhetőséget.

Annak érdekében, hogy segítsük Önöket a Walmart ezen új üzleti követelményének teljesítésében, szorosan együttműködtünk az IBM-mel és más élelmiszeripari vállalatokkal egy felhasználóbarát, alacsony költségű, blokklánc-alapú nyomonkövetési megoldás létrehozásában, amely megfelel a követelményeinknek, és közös értéket teremt a teljes leveles zöld farmtól az asztalig tartó folyamatosság számára.

Az induláshoz kövesse a <http://ibm.com/food/getstarted> oldalon található utasításokat, és válassza ki az Önnek megfelelő beilleszkedési lehetőséget és részvételi modult. A Walmart és az IBM emellett egy sor előre felvett webináriumot is közzétesz, amelyeken elmagyarázzák az új követelményt és azt, hogyan kezdheti el a munkát. Készítettünk egy listát is a Gyakran Ismételt Kérdésekről, amely hasznos lehet.

Végezetül, bár a blokklánc-alapú nyomon követhetőség nagymértékben megnöveli a levélzöldségek forrásig történő visszakövetésének lehetőségét, nem helyettesíti vagy csökkenti az Ön által követendő, élvonalbeli jó mezőgazdasági gyakorlatok betartásának szükségességét.”⁴⁴

⁴⁴ részlet a Walmart beszállítóknak írt leveléből, Food Traceability Initiative Fresh Leafy Greens, September 24, 2018, https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001

Az új nyilvántartási módszer sikerességét jelzi, hogy az IBM rendszerhez⁴⁵ újabb és újabb cégek csatlakoznak, pl. az Unilever⁴⁶ és a Nestlé⁴⁷. Ezen kívül a Walmart a blokklánc technológiát használja a kínai érdekeltségei esetében a sertéshús nyomon követésére is.

Az eltelt időszak azonban megmutatta a digitális transzformációval kapcsolatos problémákat is, például azt, hogy a különböző tőkeerősségű beszállítók egy részének komoly gondot jelenthet az új technológia finanszírozása (pl. a jelentős számítási kapacitás igény miatt), illetve a különféle korú és származású rendszerek összehangolása (interoperabilitás biztosítása) is hosszadalmas, valamint drága folyamat. Ezen kívül az Európai Unióban a blokklánc alapú rendszerek elterjedésének gátja lehet az is, hogy az adatvédelmi szabályok olyan feltételek teljesítését követelhetik meg a technológiától, amelyre az – jelenleg alkalmazott formájában – nem, vagy csak korlátozottan alkalmas (például a személyes adatok korlátozott tárolhatósága, azaz egy meghatározott időn túl a személyes adatokkal kapcsolatos törlési kötelezettség stb.).

A jelenleg lassú mederben csordogáló termék nyomon követést biztosító digitalizáció azonban felgyorsul a közeljövőben, mivel az Amerikai Egyesült Államok Élelmiszer- és Gyógyszerügyi Hivatala (FDA⁴⁸) 2022. novemberében bejelentette be az új élelmiszer nyomonkövetési követelményeket,⁴⁹ mely szerint több mint egy tucat élelmiszercsoport, például a tejtermékek és a dinnye esetében a vállalatoknak a meglévő szabályozási követelményeken túlmutató nyomon követhetőségi nyilvántartást kell létrehozniuk. Az érintett vállalkozásoknak és beszállítóknak 2026. január 20-ig kell megfelelniük a frissített szabályoknak. Az FDA azt is megköveteli, hogy a résztvevő szervezetek egy egyenrangú hálózat részeként megosszák egymással az információkat.⁵⁰

Digitális transzformáció logisztikai és számlázási megoldásai

A nagy üzletláncok és a számukra szolgáltatást végző logisztikai szolgáltatók állandó problémája az egyes fuvarokkal kapcsolatos elszámolások pontosságának megoldása és a vitás

⁴⁵ Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric, <https://www.hyperledger.org/learn/publications/walmart-case-study>

⁴⁶ Az Unilever multinacionális, fogyasztási cikket gyártó londoni székhelyű brit cég, több mint 400 márka tulajdonosa (élelmiszerek, üdítők, tisztítószer, illetve tisztálkodási és kozmetikai termékek). 2012-es adatok szerint az Unilever a világ legnagyobb fogyasztási cikket gyártó vállalata, globálisan vezető például a margarinok piacán, Európa egyik legértékesebb vállalata.

⁴⁷ A Nestlé S.A. a világ a világ vezető élelmiszeripari, táplálkozás, egészség és életmód vállalata, a központja Svájcban, a Genfi-tó partján, Vevey-ben található

⁴⁸ Food and Drug Administration

⁴⁹ "Requirements for Additional Traceability Records for Certain Foods (Food Traceability Final Rule)"

⁵⁰ PYMNTS. Walmart Puts Pricey Blockchain Food Tracking Platform On Ice. December 19, 2022.

<https://www.pymnts.com/blockchain/2022/walmart-puts-pricey-blockchain-food-tracking-platform-on-ice/>

számlák rendezése, illetve jelentős problémát okozhat a logisztikai/fuvarozási szektort erősen sújtó üzemanyag áremelkedés⁵¹ és egy újabb világjárvány lehetősége is.

A Walmart Canada⁵² évente több, mint ötszázezer szállítmányt szállít az elosztóközpontokba és üzletekbe Kanada-szerte, amelyhez igénybe veszi mind a saját, mind harmadik felek teherautó-flottáit. A hatalmas mennyiségű – köztük sok romlandó – áru határokon, időzónákon és különböző éghajlati viszonyokon keresztüli szállítása számos kihívást hordoz. Így többek között minden egyes rakományt nyomon kell követni és szükséges rögzíteni/feldolgozni olyan adatokat – többek között –, mint a megtett út, a megállóhelyek, a felhasznált üzemanyag és a hőmérséklet. Ezek az adatok fontosak, mert később az elszámolások részét is képezik. Egy-egy számlába a Walmart Canada esetében több mint kétszáz különféle adat kerül bele (azaz ennyi adat szükséges a fuvarozási díj végösszegének megállapításához), éppen ezért a számlázási és fizetési folyamat rengeteg adateltérésre ad lehetőséget. A Walmart Canada esetében a számlák 70%-a vitatott volt, ezek egyeztetése pedig jelentősen növelte a tranzakciós költségeket, illetve a kifizetési folyamatok elhúzódása miatt a fuvarozók is elégedetlenek voltak.

A probléma oka az volt, hogy a Walmart Canada és a fuvarozók több információs rendszert is használtak, ezek azonban nem voltak képesek egymással kommunikálni interoperabilitási problémák miatt, ezért az egyeztetéseket manuális módon kellett elvégezni. A Walmart Canada úgy döntött, a kaotikus, nagy emberi erőforrásigényű folyamatokat blokklánc technológia segítségével automatizálja. Ezzel a digitális transzformációs technológiával akarták megoldani az inkompatibilis vállalati rendszerek problémáját, a szkeptikusok viszont kételkedtek, hogy üzletileg kritikus funkcióban ez az új, innovatív technológia beváljon.

A Walmart Canada a DLT Labs⁵³ közreműködésével indította el a projektet,⁵⁴ amelyhez később a Bison Transport, a Walmart Canada egyik fuvarozója csatlakozott. A kísérleti változat kezdetben csak a Walmart Canada és a Bison Transport részvételével működött és hosszas tesztelés után 2019 januárjában élesítették. Az új típusú kezdeményezés sikeresnek bizonyult, így 2021 márciusában DL Freight néven a többi 69 fuvarozóra is kiterjesztették a rendszert, amely folyamatosan gyűjti az információkat a fuvarozó ajánlatától a leszállítás megtörténtéig.

⁵¹ Gowans; Gregor. Az üzemanyag-árak egész Európában térdre kényszerítik a fuvarozókat – kétségbeesés, elégedetlenség, állami beavatkozás sürgetése. Trans.INFO13.03.2022.

<https://trans.info/hu/az-uzemanyag-arak-europaban-279700>

⁵² A Walmart Canada a Walmart kanadai leányvállalata, amelynek központja Mississaugában, Ontario államban található.

⁵³ Kanadai szoftervállalat, a blokklánc technológia úttörője

⁵⁴ Vitasek, Kate; Bayliss, John; Owen, Loudon; Srivastava, Neeraj. How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges, Harvard Business Review. January 05, 2022. <https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges>

igazolásán át a fizetés jóváhagyásáig. A rendszer az információkat automatikusan, valós időben rögzíti és szinkronizálja, és csak a tranzakcióban részt vevő felek számára látható.

Az új rendszer az eddigi tapasztalatok alapján sikeresen működik, mivel míg régebben a számlák több mint 70%-át vitatták, ez kevesebb mint 1%-ra csökkent, és a vitás helyzetek is sokkal gyorsabban rendeződnek, valamint a fuvarozók időben megkapják a pénzüket.

Walmart Canada projekt tanulságai

A kulcsfontosságú szereplők bevonása (Bison Transport) lehetővé tette, hogy a projekt előkészítése, tervezése és megvalósítása során a fuvarozók álláspontja is mindvégig képviselve legyen. Ennek köszönhetően a logisztikai problémák megoldhatóvá váltak. A létfontosságú üzleti funkciók esetében célszerűbb megoldásként a privát blokklánc használatát választották, ahol a hozzáférés az ellenőrzött tagokra korlátozódik, és csakis a közvetlenül együttműködő felek láthatják az általuk kicserélt konkrét információkat. A Walmart a Hyperledger Fabric⁵⁵ nyílt forráskódú platformra épülő magánhálózat használata mellett döntött.

A korrekt elszámolás érdekében egységesíteni kellett a számítási elveket és meg kellett állapodni azokban a szabályokban is, amelyeket az üzleti partnerek (és a hálózat) alkalmaznak. Ebben a projektben minden egyes fuvarozó egyedi adataival (szállító neve, fizetési feltételek, szerződés időtartama és általános szerződési feltételek) kell a rendszernek dolgoznia, és ezeket az adatokat kombinálják olyan adatokkal, mint például az üzemanyagárak és az adókulcsok. A feleknek a szükséges adatok meghatározása után közösen kellett megállapodniuk azokban a képletekben, amelyeket a blokklánc az egyes számlák kiszámításához használ.

A DL Freight blokklánc minden egyes egyedi szállítás során valós időben szintetizálja az összes adatot, figyelembe véve az olyan kiegészítő információkat, mint például az üzemanyagköltség, a megtett távolság és a késések mértéke. A rendszer egy olyan „futó” számlát hoz létre, amely valós időben fejlődik a költségek felmerülésével. A hibák megelőzése érdekében automatizált ellenőrzéseket kellett beépíteni a blokkláncrendszerbe. Ezt a célt szolgálja például a teherautókon lévő független IoT eszközök által jelentett adatokkal a fuvarozó által a megtett kilométerekről és az elfogyasztott üzemanyagról szolgáltatott információk összehasonlítása, amely lehetőséget ad az eltérések vizsgálatára és az okok feltárására.

Az ellenőrzések és eltérések öntanuló rendszerben történő vizsgálata segíti a Walmart és a fuvarozók működésének optimalizálását. Mivel több fuvarozó is szállíthat azonos kezdő- és

⁵⁵ <https://www.hyperledger.org/use/fabric>

végpontok között, a fuvarozók adatait össze lehet vetni és ez segítséget nyújthat a folyamatok racionalizálásában és a hatékonyság növelésében.

A rendszer automatizálta a szállításokkal kapcsolatos pénzügyeket is, ezért bármilyen pénzügyi szolgáltatás - például a fizetendő számlák fuvarozói finanszírozása - is automatizálható. A blokklánc használata a számlákat pontosabbá és érvényessé teszi, ez pedig segítséget nyújthat a pénzügyek hatékony kezelésére, például a pénzügyi intézetek az ellátási lánc bármely szakaszában finanszírozást tudnak nyújtani.

A blokklánc rendszer nem igényelte a régi informatikai rendszerek leselejtezését, mivel az a régi rendszerekre épülhet és használhatja az azokban lévő adatokat, a transzparencia miatt pedig a szerződéses partnerek között nőtt a bizalom, javítva a hosszú távú együttműködést is.

A rendszer forradalmasíthatja a flottakezelést is, mivel a rendelkezésre álló nagy mennyiségű adatokból olyan információk is kinyerhetők, mint például mely konkrét útvonalak a legbiztonságosabbak vagy a legjobbak az idő és az üzemanyag-fogyasztás szempontjából, melyik a legjobb, leghatékonyabb megoldás a jármű, az útvonal, a rakománysúly, vagy akár az optimális utazási idő (azaz nappal vagy éjszaka) szerint, a teherautók várható érkezési idejének folyamatos frissítésével és megosztásával hogyan lehet koordinálni a leghatékonyabban a sok rakomány egyszerre érkezésének problémáját a nagy elosztóközpontokban.

A digitális transzformáció lehetőségei

A vállalkozások számos új technológia közül választhatnak a problémáik megoldása, illetve nem utolsósorban a versenyképességük fenntartása érdekében, napjainkban ilyen például a felhőszolgáltatások⁵⁶ igénybe vétele, az összekapcsolt rendszerek alkalmazása, a nagy adat kezelés (Big Data) és a mesterséges intelligencia (MI) használata, illetve ezen technológiák különböző kombinációi. A digitalizációs projektek megtervezésekor azonban számtalan körülményt kell figyelembe venni, így többek között azt, hogy az új technológia hogyan illeszthető be a már alkalmazott technológiák körébe, illetve milyen új típusú

⁵⁶ Szolgáltatott infrastruktúra (IaaS), amely számítási és tárhelykapacitáshoz biztosít internetes hozzáférést. A felhőalapú számítási típusok legalapvetőbb kategóriájának minősülő IaaS lehetővé teszi, hogy informatikai infrastruktúrát – kiszolgálókat és virtuális gépeket, tárhelyet, hálózatokat és operációs rendszereket – bérelhet használati alapú díjfizetés ellenében.

Szolgáltatásként nyújtott platform (PaaS), amely a fejlesztők számára biztosít eszközöket webalkalmazások készítéséhez és üzemeltetéséhez. A PaaS célja, hogy hozzáférést nyújtson a felhasználóknak azokhoz az összetevőkhöz, amelyekkel gyorsan fejleszthetnek és működtethetnek mobil- vagy webalkalmazásokat az interneten anélkül, hogy a kiszolgálókból, tárhelyszerekből, hálózatokból és adatbázisokból álló háttér-infrastruktúra kialakításával vagy üzemeltetésével kellene foglalkozniuk.

Webalkalmazásokhoz használt szolgáltatott szoftver (SaaS). Ez olyan internetes szoftveralkalmazás-szolgáltatási mód, amelynél a felhőszolgáltatók üzemeltetik és felügyelik a szoftveralkalmazásokat, így egy adott alkalmazás minden eszközön egyszerre elérhető a felhőn keresztül. <https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/types-of-cloud-computing>

információbiztonsági kockázatokat hordoz a fejlesztés. Az ENISA például számos iránymutatást jelentetett meg, amelyek megállapításait és jó gyakorlatait a szervezetek figyelembe vehetik és amelyek segítségével eldönthetnek olyan kérdéseket, mint felhőszolgáltatást vegyenek igénybe vagy saját szerveren tárolják az adataikat, mennyire kockázatos az üzleti titkaikat az új technológiára bízni, milyen védelmi intézkedéseket javasolt életbe léptetniük a gépi tanulás vagy éppen a blokklánc technológia alkalmazása esetén.

A szervezeteknek arra is fel kell készülniük, hogy ezen digitális transzformáció projektek esetében nemcsak az új technológiának van költsége, de áldozniuk kell a már meglévő rendszerekbe integrálásra, a megfelelő szakértelemmel rendelkező humán erőforrásra és az információbiztonság megfelelő szintjét eredményező védelmi intézkedésekre is.

A digitális transzformáció korlátja lehet még a fenntarthatóságra törekvés is, illetve a technológiák jelentős erőforrás-igényessége (pl. a blokklánc, illetve az MI energiaigénye).

Szabályzási környezet

Az élelmiszerellátó lánc tagjai számára alapvető kérdés az információbiztonság követelményeinek megfelelés, mely követelményeket egyrészt jogszabályok határozzák meg, másrészt az iparági normák alapján saját maguknak kell kialakítani azt a környezetet, amelyben tevékenységük folyamatosságát, biztonságát és eredményességét biztosítani képesek.

A hatályos jogi környezet – attól függően, hogy mennyire követi le az adott technológiai fejlettség szintjét – segítheti, de akár akadályozhatja is a fejlődést, illetve arra is kényszerítheti a gazdasági szereplőket, hogy a „szürke zónában” mozogva feszegessék a határokat, kihasználva az azt, hogy az adott terület még nincs szabályozva, illetve a meglévő, elavult szabályokat saját innovációjukra „alakítják”. A különböző technológiák különböző veszélyeket hordoznak, a vállalkozásoknak pedig kezelniük kell azokat a kihívásokat, amelyeket például a mesterséges intelligencia vagy a blokklánc rendszerek támaszthatnak úgy, hogy a vonatkozó jogszabályok még csak tervezet szintjén állnak rendelkezésre.

Az új technológiák használatával kapcsolatban a közeljövőben várható uniós szintű szabályozás pl. a mesterséges intelligencia használatával kapcsolatban, azonban már vannak olyan – jelentős büntetéssel fenyegető – jogszabályok, amelyek technológiásemlegesek és kockázat alapú megközelítést várnak el az élelmiszerlánc tagjaitól. Ilyen például az általános adatvédelmi

rendelet („GDPR”)⁵⁷, mely kimondottan a személyes adatok kezelésével kapcsolatos, azonban a szervezetek rendszereiben a személyes és nem személyes adatok együttes jelenléte miatt a GDPR adatbiztonságra vonatkozó rendelkezései egyértelmű kötelezettségeket jelentenek.

A rendelet alapján „az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.”⁵⁸ A GDPR alapján az élelmiszerellátó lánc tagjainak kötelező a személyes adatok kezelésére használt rendszereik (például a vállalatirányítási rendszereik) és szolgáltatásaik folyamatos bizalmas jellegének biztosítása, valamint integritása, rendelkezésre állása és ellenálló képessége⁵⁹. A GDPR adatvédelmi rendelkezéseinek következetes betartása jelenleg nehezen oldható meg, különös tekintettel a GDPR alapelveire (pl. célhoz kötöttség, korlátozott időbeli tárolhatóság). Azonban vannak olyan intézkedések, amelyek csökkenthetik a nem megfelelőségből adódó kockázatot (pl. privát blokklánc használata, álnevesítés, megfelelő szintű titkosítás, anonimizálás, blokkláncon kívüli adattárházak használata stb.).

Az élelmiszerellátási lánc szereplői kritikus üzleti folyamataikban használt információs rendszereik tekintetében támaszkodhatnak az **ISO/IEC 27001 Információbiztonság Irányítási Rendszerre (IBIR)**⁶⁰ is, mely az információbiztonság irányítás olyan nemzetközi szabványa, amely kereskedelmi, kormányzati és non-profit szervezetekre vonatkozik és meghatározza az IBIR létrehozásának, megvalósításának, folyamatos ellenőrzésének és fejlesztésének követelményeit. A rendszer célja, hogy olyan módszeres és jól szervezett megközelítést kínáljon, amely megvédi az adott szervezet bizalmas információit, biztosítja az üzleti adatok (titkok) sértetlenségét és javítja az informatikai rendszerek rendelkezésre állását. A rendszer folyamatszempontú, alapja pedig az úgynevezett PDCA modell⁶¹, amely az összes lényeges biztonsági szempontot támogatja a strukturált megvalósítás folyamán. A modell

⁵⁷ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, továbbiakban: GDPR)

⁵⁸ GDPR 32. cikk (1) bekezdés

⁵⁹ CIA-elv: bizalmasság (Confidentiality; egy adott információt csak az arra jogosultak tudhatnak meg), sértetlenség (Integrity; egy adott információt vagy rendszert csak az arra jogosultak változtathat meg) és rendelkezésre állás (Availability; egy adott rendszernek milyen megbízhatósággal kell ellátnia a feladatát) követelménye.

⁶⁰ Az ISO 27001 információbiztonsági szabványt a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) együttesen teszi közzé.

⁶¹ Plan-Do-Check-Act (PDCA) modell egy ismétlődő, négylépéses menedzsment módszer, amelyet a termékek és folyamatok kontrolljára és folyamatos fejlesztésére használnak. A modell elemei: Plan - tervezés, Do – cselekvés, Check – ellenőrzés, Act – beavatkozás.

segítségével megállapíthatóak és elemezhetőek egy szervezet potenciális kockázata, valamint meghatározhatók a szükséges tevékenységek és intézkedések. A modell célja a kockázatok folyamatos felügyelete, a mértékük optimalizálása és folyamatosan szemmel tarthatósága a lényeges biztonsági célok függvényében.

A 2004-ben létrehozott **Európai Unió Kiberbiztonsági Ügynökség (ENISA)**⁶² célja, hogy a tudásmegosztás és a figyelemfelkeltés révén erősítse az összekapcsolt gazdaságba vetett bizalmat és fokozza az uniós infrastruktúra ellenálló-képességét, segítve Európa társadalmának és polgárainak digitális biztonságát. Az ENISA hatékony támogatást nyújt a kiberbiztonsági szakemberek számára, hogy azok megfeleljenek a korunk kihívásainak, valamint hozzájussanak az alapvető a kiberbiztonsági információkhoz és ismeretekhez.

Az ENISA számos ajánlást bocsátott ki például az IPAR 4.0 és az ipari tárgyak internete („IIoT”) biztonsági intézkedéseivel és biztonságával⁶³, valamint a tárgyak internetének (IoT) biztonságával kapcsolatban, és alapvető biztonsági ajánlásokat fogalmaz meg az IoT-ökoszisztémák biztonságára.⁶⁴ Külön iránymutatást adott ki a tárgyak internete ellátási láncának biztosítása érdekében segítve az IoT-gyártókat, fejlesztőket, integrátorokat, valamint valamennyi érdekelt felet abban, hogy megfelelő, egyenszilárdságú biztonsági döntéseket hozzanak az IoT-technológiák kiépítése, telepítése, illetve értékelése során.⁶⁵

Az ENISA szerint egyik különösen fontos terület a mesterséges intelligenciához kapcsolódó ellátási lánc és hangsúlyozza, az EU biztonságos mesterséges intelligenciával kapcsolatos ökoszisztémájának a kiberbiztonságot és az adatvédelmet kell előtérbe helyeznie.⁶⁶ Külön ajánlás készült a gépi tanulás algoritmusával kapcsolatban, kiemelve az alapvető funkciókat és a kritikus szakaszokat, valamint részletesen bemutatva a gépi tanulási rendszereket célzó fenyegetéseket. Ilyen, az ENISA által azonosított fenyegetések közé tartozik például az adatmérgezés, az ellenséges támadás és az adatszivárgás.⁶⁷

Az Európai Adatvédelmi Testület (EDPB) független európai szerv, amely hozzájárul az adatvédelmi szabályok következetes alkalmazásához az Európai Unió teljes területén, valamint előmozdítja az uniós adatvédelmi hatóságok közötti együttműködést. Az EDPB célja, az Európai Unióban következetesen alkalmazzák az általános adatvédelmi rendeletet és az uniós

⁶² The European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/about-enisa/about/hu>

⁶³ <https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>

⁶⁴ <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iiot-1>

⁶⁵ <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>

⁶⁶ <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>

⁶⁷ <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>

adatvédelmi jogszabályok feltételeinek tisztázása érdekében általános iránymutatásokat fogad el biztosítva ezáltal az érdekelt felek jogainak és kötelezettségeinek következetes értelmezését⁶⁸. Megemlítendő az az iránymutatás, amely a beépített és alapértelmezett adatvédelem követelményével kapcsolatban nyújt általános eligazítást. A beépített és alapértelmezett adatvédelem mérettől és az adatkezelés összetettségének mértékétől függetlenül minden adatkezelő számára kötelező, az iránymutatás pedig – a fő beépített és alapértelmezett elemek, valamint gyakorlati példák felsorolásával – útmutatást is tartalmaz arra vonatkozóan, hogy miként lehet hatékonyan megfelelni ezen kötelezettségnek.⁶⁹

Az EDPB, illetve az elődje⁷⁰ számtalan olyan iránymutatást bocsátott ki, amely az új, innovatív technológiák alkalmazásához kapcsolódik, például az IoT eszközök,⁷¹ a Virtual Voice Assistants⁷², az információs és kommunikációs technológiák munkahelyi használata⁷³, a kooperatív intelligens közlekedési rendszerek (C-ITS)⁷⁴ és a kapcsolódó járművek⁷⁵, valamint a drónok⁷⁶ témájában. Ezen iránymutatásokban és véleményekben foglalt jó gyakorlatok alkalmazása jelentősen csökkentheti a szervezetek információbiztonsági kockázatát. A blokklánc tekintetében azonban az EDPB mind a mai napig nem adott ki átfogó iránymutatást, ezen a téren a Gibraltar Regulatory Authority (GRA)⁷⁷, a francia adatvédelmi hatóság (Commission Nationale Informatique & Libertés, CNIL)⁷⁸ dokumentumaira, illetve az Európai Parlament számára készült tanulmányra⁷⁹ támaszkodhatunk.

Németországban a **Federal Office for Information Security (BSi)** adott ki útmutatót⁸⁰ a blokklánc biztonságával kapcsolatban, amely nemcsak bemutatja az új technológiát, hanem tárgyalja a technológiával kapcsolatos biztonsági kérdéseket és támadási formákat.

⁶⁸ https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_hu

⁶⁹ https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf

⁷⁰ 29. cikk szerinti adatvédelmi munkacsoport (WP29)

⁷¹ 29. cikk szerinti adatvédelmi munkacsoport. 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16.

⁷² EDPB Guidelines 02/2021 on Virtual Voice Assistants, version 1.0. Adopted on 2021. március 9.

⁷³ 29. cikk szerinti adatvédelmi munkacsoport: 2/2017. számú vélemény a munkahelyi adatkezelésről (wp249)

⁷⁴ 29. cikk szerinti adatvédelmi munkacsoport: 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről (wp252)

⁷⁵ EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, version 2.0. Adopted on 2021. március 29.

⁷⁶ Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (wp231)

⁷⁷ Gibraltar Regulatory Authority (GRA) - GN16 Blockchain, 2020. február 20, <https://www.gra.gi/data-protection/guidance>

⁷⁸ Commission Nationale Informatique & Libertés (CNIL) - BLOCKCHAIN Solutions for a responsible use of the blockchain in the context of personal data, 2018. https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf

⁷⁹ Dr Michèle Finck - Blockchain and the General Data Protection Regulation, European Parliamentary Research Service (EPRS) Scientific Foresight Unit (STOA), 2019.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

⁸⁰ Towards Secure Blockchains - Concepts, Requirements, Assessments, Federal office for information Security (BSi), Last updated March 2019,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf?__blob=publicationFile&v=3

Az **Amerikai Egyesült Államokban** a NIST⁸¹ és a CISA⁸² tett közzé számtalan iránymutatást (jó gyakorlatokat) például zsarolóvírus témában, ezeket is érdemes figyelemmel követni. Szintén ajánlott az Egyesült Államok⁸³, Ausztrália (ACSC)⁸⁴ és az Egyesült Királyság (NCSC-UK)⁸⁵ kiberbiztonsági hatóságainak közös kiadványainak⁸⁶ ismerete.

Adatbiztonság, informatikai biztonság, információbiztonság és kiberbiztonság

A köznyelvben gyakran keverednek olyan fogalmak, mint az adatbiztonság, az információbiztonság, illetve a kiberbiztonság.

Az adatbiztonság⁸⁷ az adatok műszaki, szervezési, technikai védelmét a középpontjába állító megközelítés; nem biztonsági, hanem védelmi kategória, nem egy elérendő cél, hanem az adatalany védelmének egy eszköze. Az **informatikai biztonság** „az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.”⁸⁸

Az információbiztonság⁸⁹ az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága (Confidentiality, „C”), sértetlensége (Integrity, „I”) és rendelkezésre állása (Availability, „A”, együttesen CIA-elv), valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

⁸¹ National Institute of Standards and Technology

⁸² The Cybersecurity and Infrastructure Security Agency (CISA)

⁸³ The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA)

⁸⁴ Australian Cyber Security Centre (ACSC)

⁸⁵ The United Kingdom's National Cyber Security Centre (NCSC-UK)

⁸⁶ Például 2021 Trends Show Increased Globalized Threat of Ransomware, February 9, 2022, [https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A 2021 Trends Show Increased Globalized Threat of Ransomware 508.pdf](https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A%2021%20Trends%20Show%20Increased%20Globalized%20Threat%20of%20Ransomware%20508.pdf)

⁸⁷ Törley Gábor. Adatbiztonság a közigazgatásban. Egyetemi jegyzet. Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, Budapest, 2013. p. 11.

⁸⁸ Közigazgatási Informatikai Bizottság 25. számú Ajánlása. Magyar Informatikai Biztonsági Ajánlások (MIBA). 2008. www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf [2015.03.20.] p. 23.

⁸⁹ Muha Lajos; Krasznay Csaba. Az elektronikus információs rendszerek biztonságának menedzselése. p. 13. Nemzeti Közszolgálati Egyetem 2018. <https://nke.repo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9se%3FB3.pdf?sequence=5&isAllowed=y>

A kiberbiztonság⁹⁰ a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibernetet megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Az információbiztonsággal kapcsolatos problémák és fenyegetések

A gyakorlatban – az élelmiszer szektorban működő vállalkozások esetében is – az információbiztonság olyan komplex terület, amely három részterületből tevődik össze, a biztonsági szakembereknek pedig mindhárom területet adottságait figyelembe kell venniük. Célszerű az Ibtv.⁹¹ és a végrehajtására kiadott BM rendelet⁹² rendelkezéseit figyelembe venni (akkor is, ha az adott szervezet nem tartozik ezen jogszabályok hatálya alá), illetve hasznos segítség lehet a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet⁹³ 2021-ben kiadott Kézikönyve⁹⁴. Ezen források szektorsemleges normái az egységes fogalomrendszere segíti az élelmiszerellátó lánc tagjai közötti kommunikációt, illetve kisebb az esélye annak, hogy a szereplők ugyanazon kifejezés használata során eltérő tartalomra gondolnak.

A fizikai védelem a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem. **A logikai védelem** az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem, **az adminisztratív védelem** pedig a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések (pl. a beléptetésre vagy a kamerarendszer működtetésére vonatkozó előírások stb.), továbbá a védelemre vonatkozó oktatás.

⁹⁰ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.) 1.§ (1) bekezdés 26. pont

⁹¹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

⁹² 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó köve-telményekről (továbbiakban: BM rendelet)

⁹³ Kézikönyv a 41/2015. BM rendelet alkalmazásához. Nemzeti Kibervédelmi Intézet. <https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kezikonyv-a-41-2015-bm-rendelet-alkalmazasahoz/>

⁹⁴ Nemzeti Kibervédelmi Intézet. Felhasználói kézikönyv a 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez. 2021. december. <https://nki.gov.hu/wp-content/uploads/2021/12/Felhasznaloi-kezikonyv-vedelmi-intezkedesekhez-v1.0.pdf>

Egy multinacionális élelmiszerüzletlánc például kamerákkal és élőerős őrzéssel védi az üzleteit, a saját fejlesztésű vállalatirányítási rendszerét a legmodernebb kiberbiztonsági eszközökkel védi, illetve annak érdekében, hogy a munkavállalói betartsák az információbiztonsággal kapcsolatos szabályokat, szabályzatokat, illetve protokollokat léptet életbe.

A három védelmi terület csak együttesen teremthet biztonságot, hiszen hiába van a legtökéletesebb kibervédelme egy rendszernek, ha fizikailag nem védik például a személyesen, fizikai jelenléttel végrehajtott támadások ellen, illetve ha a védelmi folyamatokat nem írják le olyan protokollokban, amelyek nemcsak léteznek, de a végrehajtásuk és a végrehajtás folyamatos ellenőrzése is biztosított.

Az ENISA szerint szervezeteknek nem azon kell gondolniuk, hogy érheti-e őket zsarolóvírustámadás, hanem arra, hogy mikor fog ez bekövetkezni, ajánlásaival pedig segít felkészülni a támadásra. Ilyen javaslat például a szervezeteknek, hogy

- rendelkezzenek jó és ellenőrzött biztonsági mentéssel az összes üzleti szempontból kritikus fájlról és személyes adatról, ezt tartsák naprakészen és a hálózattól elszigetelve;
- alkalmazza a biztonsági mentés 3-2-1 szabályát, azaz minden adat esetében legyen 3 másolat, 2 különböző adathordozó, 1 másolat külső helyszínen;
- a személyes adatokat a GDPR rendelkezéseinek megfelelően titkosítva tárolják és használjanak kockázatalapú megközelítést az ellenőrzések folyamán;
- futtassanak olyan biztonsági szoftvert a végponti eszközökön, amely képes a legtöbb zsarolóvírust felismerni;
- a biztonságtudatosság naprakész legyen és alkalmazzák a legjobb iparági gyakorlatokat (pl. a hálózati szegmentáció, a naprakész javítások, a rendszeres biztonsági mentések, valamint a megfelelő személyazonosság-, hitelesítő és hozzáférés-kezelés, rendszergazdai jogosultságok kiosztásának korlátozása, legkisebb kiváltság elvének alkalmazása⁹⁵ stb.)
- rendszeresen végezzenek kockázatértékelést.

Az IPAR 4.0 összekapcsolt rendszereinek világában az információbiztonság területén az egyik legnagyobb figyelmet a kiberbiztonság és a kiberbiztonság megfelelő szintjéhez kapcsolódó intézkedések kapják. Az ENISA rendszeresen nyújt részletes tájékoztatást a kiberfenyegetések helyzetéről, melyek azonosítják az elsődleges fenyegetéseket, valamint a fenyegetések, a

⁹⁵ egy felhasználói fióknak vagy folyamatnak csak azokat a jogosultságokat adjuk meg, amelyek elengedhetetlenek a tervezett funkció végrehajtásához

fenyegető szereplők és a támadási technikák tekintetében megfigyelt főbb tendenciákat. Ezen kívül ismertetik a lehetséges ellenintézkedéseket is, kiemelve azok – mindhárom védelmi területet érintő – komplexitását.

Az ellátási láncokat fenyegető veszélyeket az ENISA külön jelentésben⁹⁶ részletesen elemezte azért, mert az ellátási láncok elleni támadások száma és súlyossága nő, és ez egyre nagyobb kockázatot jelent a szervezetek számára. Az ENISA hangsúlyozza, mivel ezen támadások felét a fejlett perzisztenciájú fenyegetések (APT⁹⁷) szereplőinek tulajdonítják és az összetettségük, valamint erőforrásaik jelentősen meghaladják a gyakoribb, nem célzott támadásokat, ezért egyre nagyobb szükség van új, a beszállítókat is bevonó védelmi módszerekre.

Az élelmiszerellátó lánc tagjait érintő fenyegetések

Bárhol is helyezkedik el – a farmtól az asztalig – egy adott láncban belül egy szervezet, az információbiztonságra kiemelt figyelmet kell fordítania akkor is, ha egyébként úgy véli, ő a kevésbé fenyegetett szereplők közé tartozik. Azonban ma, az összekapcsolt rendszerek világában kevés olyan vállalkozás van, amely sziget-üzemmódban működik és semmilyen módon sincs kapcsolatban más vállalkozásokkal és egyéb szervezetekkel, például felügyeleti hatóságokkal. Éppen ezért a „hagyományos” információbiztonság már csak nagyon ritkán elegendő, mivel egy-egy szervezet

- számtalan egyéb szervezettel áll úgy kapcsolatban, hogy ez fel sem tűnik neki (például a felhőszolgáltatók, az irodai és a termelésben-szolgáltatásban rendszeresített alkalmazások szolgáltatói, a könyvelő szoftver támogatója, a gépjárműflotta követésére igénybe vett cég, az adóhivatal stb.);
- a munkavállalók nemcsak a szervezet üzleti partnereivel teremthetnek kapcsolatot a kibertérben, hanem rosszindulatú szereplőkkel is például adathalász vagy zsarolóvírussal operáló támadók e-mailjében megadott linkre kattintva;
- a meghatározó pozícióban lévő munkavállalók (például kutatással-fejlesztéssel foglalkozók, felsővezetők) számtalan ártó szándékú, az információbiztonságot negatívan érintő megkeresésnek lehetnek kitéve a versenytársak agresszív érdeklődése miatt, valamint

⁹⁶ <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

⁹⁷ advanced persistent threat

- az új technológiák (pl. felhőszolgáltatások, nagy adat technológia, mesterséges intelligencia, blokklánc stb.) is számtalan olyan veszélyt hordozhatnak, amelyet kezelni szükséges.

Az új típusú kockázatok új típusú megközelítést igényelnek, a megoldásban pedig komplex biztonsági szemlélet szükséges. Az ENISA felmérése alapján⁹⁸ 2022-ben a legfontosabb azonosított veszélyek (kockázatok):

1. Zsaroló vírusos támadások („ransomware”), amelyek olyan típusú támadások, amelyben a támadók átveszik az ellenőrzést a célpontjuk eszközei felett és váltságdíjat követelnek az eszköz rendelkezésre állásának visszaállításáért cserébe, céljuk pedig a pénzügyi haszonszerzés.⁹⁹

2. Rosszindulatú szoftver/kód („malware”) olyan átfogó kifejezés, amelyet minden olyan szoftver vagy firmware¹⁰⁰ leírására használnak, amelynek célja olyan jogosulatlan folyamat végrehajtása, amely káros hatással van a rendszer bizalmasságára, integritására vagy rendelkezésre állására. Ilyen rosszindulatú kódtípusok például a vírusok, a férgek, a trójai falovak vagy más kódalapú eszközök, amelyek megfertőzik a megcélzott rendszert.

3. Pszichológiai manipuláción alapuló (Social engineering típusú) fenyegetések olyan tevékenységek, amelyek emberi hibát vagy emberi viselkedést próbálnak kihasználni azzal a céllal, hogy hozzáférjenek információkhoz vagy szolgáltatásokhoz. A social engineering a manipuláció különböző formáit használja arra, hogy az áldozatokat hibákra vagy érzékeny/titkos információk átadására készítse, például dokumentumokat, fájlokat vagy e-maileket nyissanak meg, weboldalakat látogassanak meg, vagy jogosulatlan személyeknek adjanak hozzáférést rendszerekhez vagy szolgáltatásokhoz. És bár ezek a megoldások visszaélhetnek a technológiával, minden esetben az emberi tényezőre támaszkodnak sikerük érdekében. Ilyen tevékenység például az adathalászat, spear-phishing¹⁰¹, whaling¹⁰², smishing¹⁰³, vishing¹⁰⁴, üzleti e-mail kompromittálás (BEC)¹⁰⁵, csalás és hamisítás.

⁹⁸ ENISA Threat Landscape 2022. October 2022. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

⁹⁹ Az ENISA részletesen elemezte a zsarolóvírusos támadásokat ebben a kiadványában: ENISA Threat Landscape for Ransomware Attacks. July 29, 2022. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>

¹⁰⁰ az elektronikai rendszerekben és a számítástechnika területén azok a rögzített, többnyire kis méretű programok és/vagy adatstruktúrák, melyek különböző elektronikai eszközök vezérlését végzik el.

¹⁰¹ célzott kísérlet arra, hogy érzékeny információkat, például számlaadatokat vagy pénzügyi információkat lopjanak el egy adott áldozattól, gyakran rosszindulatú okokból

¹⁰² felsővezetőnek célzott adathalász-támadás, legitim e-mailnek álcázva

¹⁰³ SmS adathalászat

¹⁰⁴ hang alapú adathalászat

¹⁰⁵ a kiberbűnözés olyan fajtája, amely során a csaló e-maileket használva rávesz valakit arra, hogy pénzt küldjön vagy bizalmas céges adatokat osszon meg

4. **Az adatok elleni fenyegetések** az adatforrásokat célozzák meg azzal a céllal, hogy jogosulatlan hozzáférést szerezzenek és nyilvánosságra hozzák, manipulálva az adatokat, illetve beavatkozzanak a rendszerek viselkedésébe. Ezek a fenyegetések számos más fenyegetések alapját is képezhetik, például zsarolóvírusos támadásnak. Technikailag az adatok elleni fenyegetések főként adatvédelmi incidensek¹⁰⁶ és adatszivárgások¹⁰⁷.

5. A rendelkezésre állás elleni fenyegetések közül a **szolgáltatásmegtagadás** során az elérhetőség a támadás célpontja, azaz az az állapot, amikor egy rendszer vagy szolgáltatás felhasználói nem tudnak hozzáférni a számukra szükséges adatokhoz, szolgáltatásokhoz vagy egyéb erőforrásokhoz. Ez a szolgáltatás és erőforrásainak kimerítésével vagy a hálózati infrastruktúra összetevőinek túlterhelésével érhető el (pl. a DDoS támadás¹⁰⁸).

6. A rendelkezésre állás elleni fenyegetések közül az **internetes fenyegetések** azt használják ki, hogy sok ember számára az internet-hozzáférés alapvető szükségletté vált a munkavégzéshez, a tanuláshoz, a szabad véleménynyilvánításhoz, a politikai szabadsághoz, illetve a szociális kapcsolatokhoz (pl. a BGP¹⁰⁹).

7. **Dezinformáció – félretájékoztatás** kampányokat a közösségi médiaplatformok és az online média használata ösztönzi, a téves és a szándékosan meghamisított információk közötti különbségek mögött pedig különböző motívumok húzódnak meg.

8. Az **ellátási láncot érintő támadások** a szervezetek és beszállítóik közötti kapcsolatot veszi célba. Egy támadás akkor tekinthető ellátási lánc komponenssel rendelkezőnek, ha legalább két támadás kombinációjából áll. Ahhoz, hogy egy támadás ellátási láncot érintő támadásnak minősüljön, a szállítónak és a vevőnek is célpontnak kell lennie, a támadók pedig megpróbálják kihasználni az ilyen támadások széles körű hatását és potenciális áldozati bázisát.

Milyen támadásokra kell felkészülniük az élelmiszer lánc tagjainak?

Az ENISA legfontosabb megállapításai 2022-re vonatkozóan:

¹⁰⁶ A GDPR alapján (4. cikk 12. pont) az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményez.

¹⁰⁷ adatszivárgás olyan esemény, amely érzékeny, bizalmas vagy védett adatok nem szándékos közlését okozhatja, például hibás konfigurációk, sebezhetőségek vagy emberi hibák miatt.

¹⁰⁸ a hálózati szolgáltatások megzavarásával támadják a webhelyeket és a kiszolgálókat

¹⁰⁹ egy autonóm rendszerek (AS) közötti forgalomirányító protokoll, mely a különböző AS-ek hálózati adminisztrátorai által meghatározott útvonalak, hálózati politikák és szabályrendszerek alapján hozza meg az útvonalválasztási döntéseket.

- A geopolitika jelentős hatással van a kiberbiztonsági fenyegetésekre. Az orosz-ukrán konfliktus jelentősen átformálta a fenyegetettségi környezetet, például jelentősen növekedett a hekker, illetve a dezinformációs tevékenység.
- A támadók növelik képességeiket, például nulladik napos exploitokat¹¹⁰ használnak fel operatív és stratégiai céljaik eléréséhez. A tapasztalatok alapján minél inkább növelik a szervezetek védekezésük és kiberbiztonsági programjaik szintjét, annál inkább növelik az ellenfelek költségeit, és ez arra készíti a támadókat, hogy nulladik napos exploitokat fejlesszenek ki és/vagy vásároljanak.
- A hacker as-a-service¹¹¹ üzleti modell egyre jobban terjed.
- A kiberbűnözéssel foglalkozó csoportok egyre nagyobb képességet mutatnak az ellátási láncot érintő támadások és a felügyelt szolgáltatók (MSP) elleni támadások terén.
- A zsarolóvírusok és az elérhetőség elleni támadások a legnépszerűbbek, és jelentős növekedés tapasztalható a rendelkezésre állás elleni támadások, különösen a DDoS-támadások terén. Ennek oka az ENISA szerint – elsősorban – az orosz-ukrán háború.
- Az adathalászat újra népszerű, a támadások kifinomultsága nőtt, a mesterséges intelligencia használatának tömeges elterjedése pedig új távlatokat nyit.
- A social engineering fenyegetések új csalijai az ukrán-orosz konfliktusra összpontosítanak, hasonlóan ahhoz, mint ami a COVID-helyzet során történt.
- A rosszindulatú szoftverekkel kapcsolatos támadások száma a COVID-19 világjárvány alatt csökkent, de most újra emelkedik.
- A zsarolási technikák tovább fejlődnek a kiszivárogtató oldalak használatával.
- A DDoS támadások egyre nagyobbak és összetettebbek, a mobilhálózatok és a tárgyak internete felé mozdulnak el.
- Újszerű, hibrid fenyegetésekre kell számítani.
- Az adatok kompromittálódása évről évre nő, miközben az adatok szerepe egyre fontosabb az ellátó láncokban is, köszönhetően az összegyűjtött adatok mennyiségének és az adatelemzés fontosságának.
- A gépi tanulási (ML) modellek egyre inkább támadások célpontjává válnak, a mesterséges intelligencia által támogatott dezinformáció és deep fake¹¹² technológia pedig komoly zavarokat okozhat a közösség interakciójában.

¹¹⁰ A nulladik napi támadás olyan biztonsági fenyegetés, amely valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, amelyet még nem publikáltak, a szoftver fejlesztője nem tud róla, vagy nem érhető még el biztonsági javítás. Nulladik napi exploitnak nevezik azt a kódot, amit a sérülékenység kihasználására használnak a támadók.

¹¹¹ a hackerképességek kereskedelmi hasznosítása, amelyben a hacker vállalkozóként dolgozik

¹¹² olyan szintetikus médiák, amelyekben egy meglévő képen vagy videón egy személyt valaki más képére cserélnek.

A vállalkozásoknak ismerniük kell lenniük a potenciálisan fenyegető szereplőket (például államilag támogatott támadók, hacktivisták¹¹³, bérhekkerek stb.), a szereplők motivációit és célpontjait, illetve az ezekkel kapcsolatos tendenciákat annak érdekében, hogy megfelelő védekezési és kockázatsökkentési stratégiákat alakíthassanak ki. Valószínűleg más kockázatokkal kell számolnia egy ökogazdaságnak és mással egy nagy multinacionális élelmiszerkereskedelmi láncnak, azonban – éppen az összekapcsolt rendszereknek, valamint a komplex élelmiszerellátó láncoknak köszönhetően – ma már egy kisméretű gazdaság információbiztonsági felkészültsége (illetve annak hiánya) is okozhatja egy nagy multinacionális cég sérülékenységét.

Az ENISA fenyegetési listáját a zsaroló vírusok vezetik, nincs ez másként az Unión kívül sem. A globalizációs hatások, illetve a kibertér jellegzetességei miatt az ellátó láncok tagjainak célszerű az **Egyesült Államok, Ausztrália és az Egyesült Királyság kiberbiztonsági hatóságainak** jelzéseit is figyelni a zsarolóvírusos támadásokkal kapcsolatban, melyek – mint kiberbűnözői magatartás – a következő viselkedési formákat és trendeket figyelték meg¹¹⁴:

- A hálózatokhoz hozzáférés megszerzése adathalászattal, lopott Remote Desktop Protocols (RDP) hitelesítő adatokkal vagy nyers erővel, valamint a sebezhetőségek kihasználása.

Bérelhető kiberbűnözési szolgáltatások használata. A zsarolóvírusok piaca egyre "professzionálisabbá" válik, és a zsarolóvírusok bűnözői üzleti modellje honosodott meg. A ransomware-as-a-service (RaaS)¹¹⁵ szolgáltatás fokozott használata mellett a zsarolóvírusokkal fenyegető szereplők független szolgáltatásokat alkalmaznak a kifizetések megtárgyalására, a kifizetések teljesítése során az áldozatok segítésére, valamint a támadók és más kiberbűnözők közötti fizetési viták eldöntésére. Az NCSC-UK¹¹⁶ megfigyelte, hogy egyes zsarolóvírussal fenyegető szereplők a váltságdíj kifizetésének és a titkosított rendszerek vagy adatok helyreállításának felgyorsítása érdekében 24/7 segélyközpont szolgáltatásait ajánlották fel áldozataiknak.

A tájékoztatót kiadó kiberbiztonsági hatóságok meglátása szerint, amennyiben a zsarolóvírus-bűncselekmények elkövetői számára a zsarolóvírus-bűncselekmények

¹¹³ a hacktívizmus olyan számítógép-alapú technikák alkalmazása, mint a hackelés, mint a polgári engedetlenség egy formája egy politikai napirend vagy társadalmi változás előmozdítása érdekében

¹¹⁴ 2021 Trends Show Increased Globalized Threat of Ransomware. February 9, 2022. https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf

¹¹⁵ olyan üzleti modell, amelynek keretében a rosszindulatú szoftverek fejlesztői a zsarolóprogramokat és azok vezérlő infrastruktúráját más kiberbűnözőknek adják bérbe.

¹¹⁶ The United Kingdom's National Cyber Security Centre (NCSC-UK)

üzleti modellje továbbra is nyereséges pénzügyileg, akkor a zsarolóvírus-incidensek egyre gyakoribbá válnak, mivel minden egyes váltságdíjfizetés megerősíti a bűnözői üzleti modell életképességét és pénzügyi vonzerejét. Az alkalmazott bűnügyi üzleti modell emellett gyakran megnehezíti a felelősségre vonást, mivel fejlesztők, társvállalatok és szabadúszók bonyolult hálózatai léteznek, és emiatt gyakran nehéz egyértelműen azonosítani a zsarolóvírusok mögött álló szereplőket. A GDPR hatálya alatt működő szervezetek ráadásul hajlamosabbak fizetni annak érdekében, hogy az őket ért támadások ne jussanak az illetékes adatvédelmi felügyeleti hatóságok tudomására, mert ebben az esetben nemcsak a zsarolókat kell kifizetniük, de a hatóság által rájuk kiszabott bírság is jelentős lehet.

- **Az áldozatokkal kapcsolatos információk megosztása.** Az eurázsiai zsarolóvíruscsoportok megosztották egymással az áldozatokkal kapcsolatos információkat, így diverzifikálva a célszervezeteket fenyegető veszélyt, például a BlackMatter zsarolóvíruscsoport a leállításának bejelentése után a meglévő áldozatait a Lockbit 2.0 néven ismert csoport tulajdonában lévő infrastruktúrára helyezte át.
- **Elmozdulás a "nagyvadak"¹¹⁷ vadászatától (USA).** 2021 első felében a zsarolóvírus-fenyegető szereplők "nagyvad" szervezeteket vettek célba (például a Colonial Pipeline Company, a JBS Foods és a Kaseya Limited). A zsarolóvírussal foglalkozó csoportok működését azonban 2021 közepén az amerikai hatóságok megzavarták, ezt követően az egyes zsarolóvírussal támadók a lebukási esély csökkentése érdekében a "nagyvadak" helyett a közepes méretű áldozatokra koncentráltak.
- **A zsarolási módszerek diverzifikálódása.** Az áldozatok hálózatainak titkosítása után a zsarolóvírussal fenyegető szereplők egyre gyakrabban alkalmaztak "hármasszarolást". Ennek során az áldozatot azzal fenyegetik, hogy (1) nyilvánosan nyilvánosságra hozzák az ellopott érzékeny információkat, (2) megszakítják az áldozat internet-hozzáférését és/vagy (3) tájékoztatják az áldozat üzleti partnereit, részvényeseit vagy beszállítóit az incidensről. Az ACSC továbbra is találkozott olyan "kettős zsarolási" esetekkel, amelyekben a fenyegető szereplő a titkosítás és az adatlopás kombinációját használta arra, hogy az áldozatokat váltságdíj fizetésre kényszerítse.

A zsarolóvírusos támadásoknál a szervezeteknek számítaniuk kell arra, hogy a váltságdíj kifizetése csak egy része a támadás költségeinek, az egyéb költségek (pl. állásidő, az emberek

¹¹⁷ A bűnelkövetők által nagy értékűnek vélt és/vagy kritikus szolgáltatásokat nyújtó szervezetek

ideje, az eszközkölségek, a hálózati költségek, az elvesztett lehetőségek stb.) sokszorosára növelhetik az elszenvedett kár mértékét.

A JBS Foods zsarolóvírusos támadása

2021. május 30-án a brazil székhelyű JBS S.A. húsfeldolgozó vállalatot¹¹⁸ (továbbiakban JBS Foods) olyan kibertámadás érte, amely működésképtelenné tette marha- és sertés vágóhidjait, illetve a támadás hatása kiterjedt az Egyesült Államokban, Kanadában és Ausztráliában található létesítményeire is.¹¹⁹ A multinacionális vállalat méretét jelzi, hogy világszerte több, mint 150 ezer alkalmazottal rendelkezik és csak Ausztráliában 47 létesítménye van, köztük vágóhidak, takarmányüzemek és húsfeldolgozó üzemek. A támadás nem érintette a tartalék szervereket és a vállalat közölte, hogy nincs tudomása arról, hogy vevőinek, beszállítóinak vagy alkalmazottjainak az adatai sérültek volna. A vállalat a biztonsági mentési rendszerek segítségével állította vissza az üzemei működését.

Az üzemek leállása példa arra, hogy a modern húsfeldolgozó üzemek mind élelmiszerbiztonsági, mind pedig munkavédelmi okokból nagymértékben automatizáltak, és a számítógépek a termelési folyamat számos szakaszában gyűjtenek adatokat, valamint a megrendelések, a számlázás, a szállítás és más funkciók is mind elektronikusok.

Allan Liska, a Recorded Future kiberbiztonsági cég zsarolóvírus-szakértője szerint ez a támadás volt az eddigi legnagyobb élelmiszeripari gyártó elleni támadás. Elmondása szerint azonban az esetet megelőző 12 hónapban legalább negyven élelmiszeripari vállalatot vettek célba hackerek, köztük a Molson Coors sörgyárat és az E & J Gallo Winery-t.¹²⁰¹²¹ Liska szerint az élelmiszeripari vállalatok "körülbelül ugyanolyan biztonsági szinten vannak, mint a gyártás és a szállítás. Ami azt jelenti, hogy nem túl magas". Egy másik szakértő, Trey Malone, a Michigani Állami Egyetem mezőgazdasági tanszékének adjunktusa szerint a JBS a második legnagyobb marha-, sertés- és csirkehús-előállító az Egyesült Államokban, és ha akár csak egy napra is

¹¹⁸ A JBS S.A. brazil székhelyű húsfeldolgozó vállalat, amely a világ húsellátásának körülbelül egyötödét biztosítja, és az eladási adatok alapján a világ legnagyobb marha-, csirke- és sertéshús-előállítója.

¹¹⁹ Bryan Menegus. World's largest meat supplier grinds to a halt after cyberattack. The Verge. Jun 1, 2021, 9:42 PM GMT+2. <https://www.theverge.com/2021/6/1/22463621/jbs-cyberattack-russia-largest-meat-supplier>

¹²⁰ Az E & J Gallo Pincészet az Egyesült Államok legnagyobb családi tulajdonú pincészete, a kaliforniai borok legnagyobb exportőre.

¹²¹ Rod McGuirk and Dee-Ann Durbin. Meatpacker JBS says systems 'coming back online' after REvil cyberattack. Chicago Tribune ssociated Press. Jun 02, 2021 at 4:45 pm. <https://www.chicagotribune.com/business/ct-biz-jbs-cyberattack-ransomware-meat-20210602-lv5tguj6sbbto6azzq3jzer4-story.html>

leállna, az Amerikai Egyesült Államok elveszítené marhahús-feldolgozó kapacitásának közel negyedét, ami 20 ezer marha feldolgozásának.¹²²

A támadás felhívta a figyelmet az Amerikai Egyesült Államok húsfeldolgozó iparának koncentrációjának mértékére és a termelés csökkenésével kapcsolatos kiszolgáltatottságra abban az esetben, amennyiben a négy nagy húsipari termelő egyike csökkentené termelését. Az incidenst az FBI vizsgálta, a CISA technikai támogatást nyújtott a JBS Foods-nak, az USA Mezőgazdasági Minisztériuma (USDA¹²³) több nagy amerikai húsfeldolgozót figyelmeztetett a helyzetre, a Fehér Ház pedig értékelte az ország húsellátására gyakorolt esetleges hatásokat.

A gyorsan megmozduló hatóságok is alátámasztják, miszerint a JBS Foods-típusú vállalatok kritikus szerepet játszanak az élelmiszerellátó láncban, és a támadók valószínűleg úgy gondolják, hogy ez növeli az esélyüket a gyors kifizetésre. Sőt az is, hogy az Amerikai Egyesült Államokban az elektromos, nukleáris és banki rendszereken kívül nincsenek kiberbiztonsági követelmények a vállalatokra. David White, az Axio kiberkockázat-kezelő¹²⁴ vállalat elnöke szerint egy jól átgondolt szabályozás segítene, különösen a nem megfelelő vagy kiforratlan kiberbiztonsági programokkal rendelkező vállalatok esetében. A szabályoknak azonban ágazatspecifikusnak kellene lenniük, figyelembe véve a kiesések nemzetgazdasági kockázatait. Azonban a szabályozásoknak negatív hatása is lehet, ugyanis egyes vállalatok arra úgy tekinthetnek, mint a kockázatkezeléssel kapcsolatban maximum teljesítendő követelményre, nem pedig a kiindulópontra, azaz „a szabályozás segíthet, de nem csodaszer”.¹²⁵

Bár sokan kritizálták ezért, JBS Foods 11 millió dollárnak megfelelő értékű váltságdíjat fizetett Bitcoinban a hekkereknek. Andre Nogueira, a JBS Foods amerikai részlegének vezérigazgatója elmondta, a váltságdíjat azért fizették ki, hogy megvédjék a JBS Foods húszüemeit a további zavaroktól, és korlátozzák a JBS Foods-tól függő éttermekre, élelmiszerboltokra és farmerekre gyakorolt lehetséges hatást. Azt is hozzátette, hogy a kifizetésre azután került sor, hogy a JBS Foods üzemek többsége újra működőképes volt.¹²⁶

¹²² McGuirk, Rod; Durbin, Dee-Ann. Meatpacker JBS says systems ‘coming back online’ after REvil cyberattack. Chicago Tribune ssociated Press. Jun 02, 2021 at 4:45 pm. <https://www.chicagotribune.com/business/ct-biz-jbs-cyberattack-ransomware-meat-20210602-lv5tguj6sbbyto6azzqi3jzer4-story.html>

¹²³ USA Mezőgazdasági Minisztériuma, alapította: Abraham Lincoln, alapítva: 1862. május 15-én. <https://www.usda.gov/>

¹²⁴ olyan kockázatkezelés, amely információs és kommunikációs rendszerek használatából fakadó bármely kockázatot kezel, amely veszélyezteti az adatszolgáltatás titkosságát, rendelkezésre állását vagy sértetlenségét.

¹²⁵ McGuirk, Rod; Durbin, Dee-Ann. Meatpacker JBS says systems ‘coming back online’ after REvil cyberattack. Chicago Tribune ssociated Press. Jun 02, 2021 at 4:45 pm. <https://www.chicagotribune.com/business/ct-biz-jbs-cyberattack-ransomware-meat-20210602-lv5tguj6sbbyto6azzqi3jzer4-story.html>

¹²⁶ Bunge, Jacob. JBS Paid \$11 Million to Resolve Ransomware Attack. The Wall Street Journal. Updated June 9, 2021 8:27 pm ET. <https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781>

A Fehér Ház sajtóreferense bejelentette, hogy a kibertámadást valószínűleg egy orosz szervezet hajtotta végre¹²⁷, a feltételezések szerint a REvil csoport. A probléma feljutott a legmagasabb szintre és az USA elnöke, Joe Biden és Vlagyimir Putyin orosz elnök 2021. július 9-i telefonbeszélgetése után Joe Biden amerikai elnök sajtótájékoztatóján kijelentette, hogy "Világossá tettem neki, hogy az Egyesült Államok elvárja, ha egy zsarolóvírus művelet az ő területéről érkezik, még akkor is, ha azt nem az állam szponzorálja, elvárjuk, hogy cselekedjenek, ha elég információt adunk nekik ahhoz, hogy cselekedjenek, hogy ki az."¹²⁸ 2021. július 13-án a REvil weboldalai és egyéb infrastruktúrája eltűnt az internetről.¹²⁹

Intézkedések incidensek esetén

A kibertérből érkező támadások elleni válaszingtézkedések, valamint a védelem és ellenállóképesség kialakítása és folyamatos fejlesztése mindig az adott szervezet feladata, azonban nemzetközi, illetve nemzeti, valamint szektorspecifikus (pl. üzleti, kormányzati, katonai stb.) szinten a megfelelő védelmi képességek kialakítása céljából alakultak reagáló csapatok (CERT¹³⁰-ek, CSIRT¹³¹-ek) is.

A szervezetek segítségül hívhatják az EDBP iránymutatását¹³², amely részletesen bemutatja az adatvédelmi incidenseket és elemzi azokat az azonnali intézkedések kárelhárítás és kárenyhítés szempontjából. Az ilyen típusú incidensek súlyát jelzi, hogy az iránymutatás első hét esete a zsarolóvírusos támadásokkal kapcsolatos és részletesen (de nem kizárólagosan) felsorolja azokat az intézkedéseket, amelyeket a szervezetek tehetnek annak érdekében, hogy elkerüljék, illetve csökkentsék a hatását az ilyen típusú támadásoknak, például:

¹²⁷ Harris, Bryan; Politi, James; Smyth, Jamie; Foy, Henry. "Russian criminal gang probably hacked meat supplier JBS, says White House". Financial Times. 2 June 2021. <https://www.ft.com/content/00eca8fc-4278-4c98-ace3-5967fe3bbd11>

¹²⁸ Miller, Zeke; Tucker, Eric. "Biden tells Putin Russia must crack down on cybercriminals". AP NEWS. July 9, 2021. <https://apnews.com/article/joe-biden-europe-technology-government-and-politics-russia-df7ef73f02bcba61ad6e628aa95a9f84>

¹²⁹ Fung, Brian; Cohen, Zachary; Sands, Geneva Sands. Ransomware gang that hit meat supplier mysteriously vanishes from the internet. CNN Business. Updated 10:26 AM EDT, Wed July 14, 2021. <https://edition.cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html>

¹³⁰ Computer Emergency Response Team (Számítógép Vészhelyzet Kezelő Csoportok) olyan szervezetek (USA), mely a kiberbiztonság területén különböző szolgáltatásokat nyújtanak megfelelő időben és minőségben

¹³¹ Computer Security Incident Response Team (Számítógép-biztonsági Incidenskezelő Csoport), a CERT európai megfelelője

¹³² EDPB Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Adopted on 14 December 2021, Version 2.0, 2.5. és 3.4.

- a firmware, az operációs rendszer és az alkalmazászoftverek naprakészen tartása a szervereken, az ügyfélgépeken, az aktív hálózati komponenseken és az ugyanazon a LAN¹³³-on lévő bármely más gépen (beleértve a Wi-Fi¹³⁴ eszközöket is).
- megfelelő informatikai biztonsági intézkedések alkalmazása, azok hatékonyságának biztosítása és rendszeres frissítése amennyiben a körülmények változnak, ideértve a részletes naplók vezetését arról, hogy mely javításokat milyen időbélyeggel végezték.
- az adatrendszerek és hálózatok szegmentálása vagy elszigetelése annak érdekében, hogy elkerülhető legyen a rosszindulatú szoftverek terjedése a szervezeten belül, valamint a külső rendszerekben.
- naprakész, biztonságos és tesztelt biztonsági mentési eljárások megléte, a közép- és hosszú távú biztonsági mentéshez használt adathordozók operatív adattárolástól elkülönítve, harmadik felek számára még sikeres támadás esetén is elérhetetlenül tárolása (pl. napi inkrementális biztonsági mentés¹³⁵ és heti teljes biztonsági mentés).
- rendszeres felülvizsgálat és tesztelés annak biztosítására, hogy a biztonsági mentések segítségével vissza lehessen állítani minden olyan adatot, amelynek integritását vagy rendelkezésre állását befolyásolták.
- megfelelő, naprakész, hatékony és integrált, a rosszindulatú programok elleni szoftver megléte/beszerzése.
- megfelelő, naprakész, hatékony és integrált tűzfal és behatolásérzékelő, valamint megelőző rendszer megléte/beszerzése. A hálózati forgalom átirányítása a tűzfalon keresztül, még távoli munkavégzés (home office) vagy mobil munkavégzés esetén is (pl. VPN-kapcsolatok használatával a szervezeti biztonsági mechanizmusokhoz az internethez való hozzáféréskor).
- a munkavállalók oktatása az informatikai támadások felismerésének és megelőzésének módszereiről, valamint megfelelő eszközöket kell biztosítani annak megállapítására, hogy az e-mailek és az egyéb kommunikációs eszközökkel kapott üzenetek hitelesek és megbízhatóak-e. Az alkalmazottakat ki kell képezni arra, hogy felismerjék, ha egy ilyen támadás történik, hogyan lehet a végpontot kivonni a hálózathoz és kötelesek azt azonnal jelenteni a biztonsági vezetőnek.

¹³³ Local Area Network: olyan számítógépes hálózat, amely egy épületen belül, vagy egymáshoz közel elhelyezkedő épületekben, épüle cso portokban teszi lehetővé az informatikai eszközök kommunikációját

¹³⁴ Wirele ss Fidelity: vezeték nélküli kommunikációs technológia, amely lehetővé teszi a készülékek (pl. számítógépek, táblagépek, okostelefonok stb.) vezeték nélküli csatlakozását az internethez és annak használatát.

¹³⁵ A mentési folyamat teljes mentéssel kezdődik, utána mindig az utolsó mentés óta történt változásokat mentjük. A teljes visszaállításhoz az utolsó teljes mentésre és az összes inkrementális mentésre szükség van.

- a rosszindulatú kód típusának azonosításának szükségessége annak érdekében, hogy láthatóak legyenek a támadás következményei és képes legyen a szervezet megtalálni a megfelelő intézkedéseket a kockázatok csökkentésére. Amennyiben a zsarolóvírus-támadás sikeres volt és nem áll rendelkezésre biztonsági mentés, az adatok visszaszerzéséhez olyan rendelkezésre álló eszközök alkalmazását javasolja az EDPB, mint például a "no more ransom" (nomoreransom.org) projekt által kínált eszközök. Abban az esetben azonban, ha biztonságos biztonsági mentés áll rendelkezésre, az adatok visszaállítása arról ajánlott.
- az összes naplófájl továbbítása vagy replikálása¹³⁶ egy központi naplószerverre (esetleg a naplóbejegyzések aláírásával vagy kriptográfiai időbélyegzésével).
- erős titkosítás és többfaktoros hitelesítés, különösen az informatikai rendszerekhez való adminisztrátori hozzáférés esetében, valamint megfelelő kulcs- és jelszókezelés.
- számítógépes biztonsági incidensekre reagáló csoport (CSIRT) vagy számítógépes eseménykezelő központ (CERT) létrehozása a szervezeten belül, vagy csatlakozás egy kollektív CSIRT/CERT-hez. A szervezetnek készítenie kell incidensreagálási tervet, katasztrófa-visszaállítási tervet és üzletmenet-folytonossági tervet, valamint gondoskodnia kell ezek teszteléséről is.
- az ellenintézkedések értékelése során a meglévő kockázatelemzést felül kell vizsgálni és a megállapítások alapján frissíteni kell.
- a legkorszerűbb titkosítás és kulcskezelés, különösen jelszavak, érzékeny vagy pénzügyi adatok kezelése esetén.
- a rendszer naprakészen tartása (szoftver és firmware).
- erős hitelesítési módszerek, például kétfaktoros hitelesítés és hitelesítési szerverek használata, kiegészítve naprakész jelszópolitikával.
- erős felhasználói jogosultság- és hozzáférés-szabályozás.
- megfelelő, naprakész, hatékony és integrált tűzfal, behatolásjelző és egyéb peremvédelmi rendszerek használata.
- rendszeres informatikai biztonsági auditok és sebezhetőségi értékelések (behatolásvizsgálat).¹³⁷

¹³⁶ az információk megosztását a redundáns erőforrások, például a szoftver- vagy hardverkomponensek közötti konzisztencia biztosítása érdekében, a megbízhatóság, a hibatűrés vagy a hozzáférhetőség javítása érdekében.

¹³⁷ EDPB Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. Adopted on 14 December 2021. Version 2.0, 2.5. és 3.4.

Az ellátó láncok információbiztonságával kapcsolatos problémák és fenyegetések

A ENISA definíciója alapján¹³⁸ ellátási lánc a végső megoldás vagy termék létrehozásában és szállításában részt vevő folyamatok, emberek, szervezetek és forgalmazók ökoszisztémáját jelenti. A kiberbiztonságban az ellátási lánc az erőforrások (hardver és szoftver), a tárolás (felhő vagy helyi), a terjesztési mechanizmusok (webes alkalmazások, online áruházak) és az irányítási szoftverek széles körét foglalja magában.

Az ellátási láncnak négy kulcsfontosságú eleme van, a beszállító (olyan szervezet, amely terméket vagy szolgáltatást szállít egy másik szervezetnek), a beszállító eszközei (a szállító által a termék vagy szolgáltatás előállításához használt értékes elemek), a vevő (az a szervezet, amely a szállító által előállított terméket vagy szolgáltatást fogyasztja) és a vevő eszközei (a célvállalat tulajdonában lévő értékes elemek).

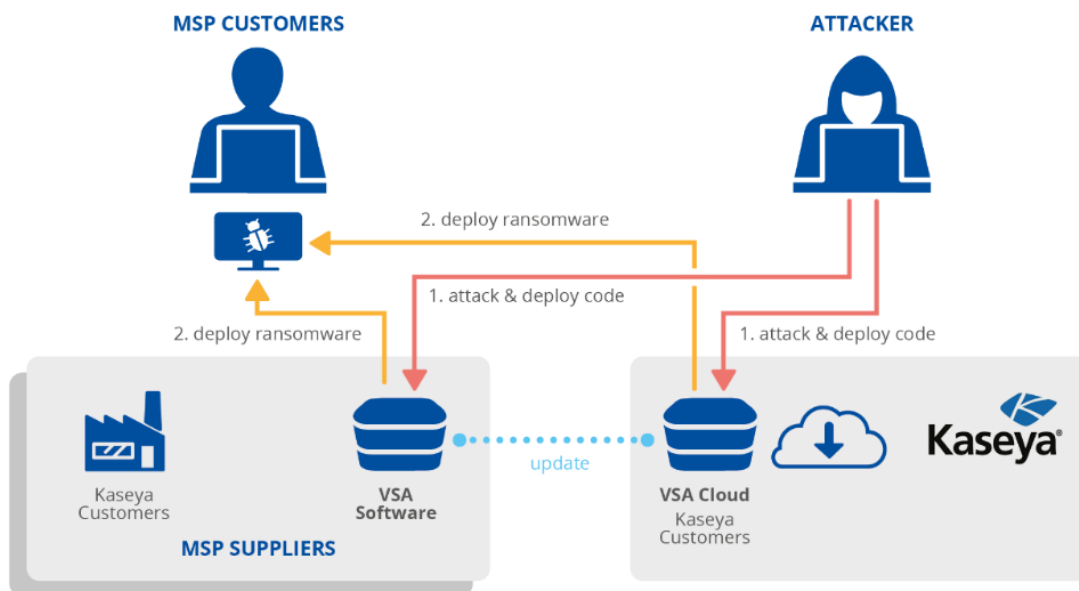
Az ellátási lánc szereplői lehetnek egyének, egyének csoportjai vagy szervezetek, az eszközök pedig lehetnek emberek, szoftverek, dokumentumok, pénzeszközök, hardverek vagy egyéb eszközök. Az is fontos, hogy az élelmiszerellátó láncokban nemcsak az élelmiszer útjával kapcsolatos láncokat kell figyelembe venni a lehetséges támadások szempontjából, hanem az egyéb, az élelmiszer előállításában közvetlenül részt nem vevő beszállítókat is. Ilyen szállítók lehetnek például a termelési, vállalatirányítási és irodai alkalmazás szoftverek szállítói (fejlesztői, üzemeltetői, támogatói), de akár a felhőszolgáltató is.

Az ellátási láncban ugyanaz a szereplő egyszerre lehet vevő és szállító is, tekintettel a láncok hosszára és bonyolultságára, valamint ezek az ellátási láncok akár rövid idő alatt is jelentősen megváltozhatnak a lánc tagjaiban történt módosulások miatt (pl. világjárvány vagy háború miatt kiesnek bizonyos szállítók és vevők, nemzetközi egyezmények megszűnése, vagy szankciók/embargók miatt egyes lánctagokat le kell cserélni stb.)

Az ellátási lánc támadása abban különbözik a hagyományos támadásoktól, hogy legalább két támadás kombinációja, mely esetben az első támadás egy szállító ellen irányul, amelyet aztán a célpont megtámadására használnak fel, hogy hozzáférjenek annak eszközeihez. A célpont lehet a végső vevő vagy a vevő egy másik beszállítója. Ezért ahhoz, hogy egy támadás ellátási lánc elleni támadásnak minősüljön, a szállítónak és a vevőnek is célpontnak kell lennie. A támadások akár hónapokig is eltarthatnak, mire sikert érnek el és sok esetben hosszú ideig

¹³⁸ ENISA Threat Landscape for Supply Chain Attacks. July 29, 2021. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

észrevétlenek maradnak. A Kaseya ellátási lánc támadása során a támadók kódot telepítettek az MSP-szállítók¹³⁹ VSA-példányaira¹⁴⁰, és rosszindulatú szoftvereket és zsarolóprogramokat telepítettek ügyfeleikhez.



1.sz. ábra: A Kaseya ellátási lánc támadásának diagramja.¹⁴¹

Az élelmiszer ellátási lánc („fármtól az asztalig”) tagjának megtámadása esetén külön kockázat az élelmiszerek és az élelmiszereket elfogyasztó, vagy éppen a támadás miatt azt elfogyasztani nem tudó emberek élete és egészsége.

Az ellátási láncok kompromittálására használt támadási technikák

Az ENISA számos, az ellátási láncok kompromittálására használt támadási technikát ismertet oly módon, hogy nem azt taglalja, hogy a támadók „mit” használtak a támadáshoz, hanem azt, hogy „hogyan történt” a támadás (az ENISA taxonómiája szempontjából érdektelen, hogy az online talált jelszó kiszivárgott, alapértelmezett jelszó volt-e, vagy feketepiacon adták el).

A leggyakrabban alkalmazott támadási technikák, amelyekre fel kell készülnie az ellátó láncok tagjának (egy támadás során a támadók több technikát is alkalmazhatnak):

- rosszindulatú szoftverek fertőzése, pl. kémprogramok, amelyeket a munkavállalók hitelesítő adatainak ellopására használnak;

¹³⁹ A menedzselt szolgáltató (MSP) olyan harmadik félként működő vállalat, amely távolról kezeli az ügyfél informatikai infrastruktúráját és végfelhasználói rendszereit.

¹⁴⁰ A Kaseya VSA (rendszer, IT menedzsment megoldás) segítségével távolról felügyelheti és kezelheti a hálózaton belüli és kívüli végpontokat, erőteljes IT-automatizálással skálázhat, javíthatja az IT-biztonságot és növelheti az IT-hatékonyságot.

¹⁴¹ ENISA Threat Landscape for Supply Chain Attacks. July 2021. p. 19. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

- social engineering, pl. adathalászat, hamis alkalmazások, Wi-Fi megszemélyesítés, a beszállító meggyőzése, hogy tegyen valamit;
- brute-force támadás¹⁴², pl. jelszó, webes bejelentkezés kitalálása;
- szoftver sebezhetőség kihasználása pl. SQL-kódbeszórás¹⁴³ vagy puffer túlcsordulás kihasználása¹⁴⁴ egy alkalmazásban;
- konfigurációs sebezhetőség kihasználása pl. egy konfigurációs probléma kihasználása;
- fizikai támadás vagy módosítás, pl. hardver módosítása, fizikai behatolás;
- nyílt forráskódú kutatás (OSINT¹⁴⁵), pl. online keresés hitelesítő adatok, API¹⁴⁶-kulcsok¹⁴⁷, felhasználónevek után;
- hamisítás, pl. USB utánzása rosszindulatú céllal.

Szállítói eszközök elleni támadások az ellátási láncban

A ENISA taxonómiájában a támadók által megcélzott beszállítói eszközök arra utalnak, hogy "mi" volt a beszállító elleni támadás célpontja, ami lehetővé tette a további támadás végrehajtását. A célba vett eszköz(ök) általában közvetlen kapcsolatban áll(nak) a végső célponttal, és az érintett eszközök listájának elemzésével általában meg lehet érteni a támadó végső szándékait. Az is gyakran előfordul, hogy a szállítók nem rendelkeznek a szükséges ismeretekkel vagy szakértelemmel ahhoz, hogy megállapítsák, mely eszközöket veszélyeztették a támadók. Milyen szállítói eszközöket céloznak meg leggyakrabban a támadók?

- Már meglévő szoftverek, pl. a szállító által használt szoftverek, webserverek, alkalmazások, adatbázisok, felügyeleti rendszerek, felhőalkalmazások, firmware;
- szoftverkönyvtárak, pl. harmadik féltől származó könyvtárak, harmadik féltől telepített szoftvercsomagok stb.;
- kód, pl. forráskód vagy a szállító által fejlesztett szoftver;
- konfigurációk, pl. jelszavak, API-kulcsok, tűzfalszabályok, URL-ek¹⁴⁸;

¹⁴² olyan jelszófeltörő módszer, ami az összes lehetséges variáció végigpróbálásával dolgozik

¹⁴³ az az eljárás, mikor egy olyan memóriatartományra, amely normál esetben adatot tartalmaz, illetőleg adatbevitel számára van fenntartva, valamely futtató környezet által futtatható kódot helyezünk el.

¹⁴⁴ olyan rendellenesség, amikor a program, miközben adatokat ír a pufferbe, túllépi a puffer határát, és felülírja a szomszédos memóriahelyeket.

¹⁴⁵ Az OSINT (Open Source Intelligence, nyílt forrású hírszerzés): olyan folyamat, amelynek célja a nyilvános forrásokból történő információgyűjtés.

¹⁴⁶ Application Programming Interface, alkalmazásprogramozási felület

¹⁴⁷ Az API-kulcs egy egyedi kód, amelyet egy API a hívó alkalmazás vagy felhasználó azonosításához használ.

¹⁴⁸ webcím (Uniform Resource Locator; egységes erőforrás-helymeghatározó rövidítése), az interneten megtalálható bizonyos erőforrások (például szövegek, képek) szabványosított címe

- adatok, pl. a szállítóra vonatkozó információk, érzékelőkből származó adatok, tanúsítványok, az ügyfeleknek vagy maguknak a szállítóknak, illetve a szállítók munkavállalóinak személyes adatai;
- folyamatok, pl. frissítések, biztonsági mentések vagy érvényesítési folyamatok, tanúsítványok aláírási folyamatai;
- hardver, pl. a szállító által gyártott hardver, chipek, USB-k;
- emberek, pl. az adatokhoz, infrastruktúrához vagy más személyekhez hozzáféréssel rendelkező célszemélyek.

A vevő kompromittálására használt támadási technikák

A ENISA taxonómiájában ezek azok a támadási technikák, amelyeket a támadók a vevőnek a beszállítóján keresztül történő kompromittálására használnak. Ebben az esetben azt azonosítjuk, hogy "hogyan" támadták meg a vevőt, és nem azt, hogy "mivel". Ilyen támadási technika például az, amikor a vevő a szállítótól frissíti a szoftverét, és a frissítéssel együtt rosszindulatú programot is kap. Ebben az esetben a támadás egyszerre vonatkozik a "megbízható kapcsolatra" és a "rosszindulatú programmal való fertőzésre". Előfordulhat, hogy a vevő nem ismeri azt a támadók alkalmazta technikát, amellyel a szállítón keresztül hozzáfértek az eszközeihez, de rendelkezik a szükséges eszközökkel annak azonosítására, hogy az alkalmazott technika nem a saját peremterületén belül történt. Az ENISA szerint leggyakoribb vevő kompromittálására alkalmazott támadási technikák:

- a megbízható kapcsolat, pl. egy tanúsítványban, automatikus frissítésben, automatikus biztonsági mentésben megbízás;
- Drive-by Compromise¹⁴⁹, pl. rosszindulatú szkriptek egy weboldalon abból a célból, hogy megfertőzzék a felhasználókat rosszindulatú kódokkal;
- adathalászat, pl. az üzenetek úgy néznek ki, mintha a szállító küldte volna, hamis frissítési értesítések;
- rosszindulatú szoftverek fertőzése, pl. távoli hozzáférésű trójai (RAT)¹⁵⁰, hátsó ajtó, zsarolóprogram;
- fizikai támadás vagy módosítás, pl. hardver módosítása, fizikai behatolás;
- hamisítás, pl. hamisított USB-készítés, alaplap módosítása, a szállító, illetve a szállító alkalmazottja személyazonosságának megszemélyesítése.

¹⁴⁹ A támadó egy legitim weboldalt kompromittál, ahova valamilyen rosszindulatú kódot tölt fel

¹⁵⁰ A távoli hozzáférésű trójaiak (RAT) használatával a hackerek megkerülhetik az eszközök (pl. mobiltelefon) biztonsági infrastruktúráját, lehetővé téve a kiberbűnözők számára, hogy közvetlenül a fertőzött eszközökről végezzenek tranzakciókat.

A vevő eszközeit ért támadások

Ebben az esetben a vevő eszközei a támadók fő és végső célpontjai (a legtöbb ellátóláncot érintő támadás végső célja a vevő eszközei). Az ilyen támadások esetén előfordulhat, hogy bizonyos eszközöket a támadókat közvetlenül célba vesznek, míg másokat véletlenül érintenek. A tipikus ellátási lánc támadások általában egynél több ügyfelet érintenek. Az ENISA szerint a leggyakrabban érintett eszközök a vevőnél:

- adatok, pl. fizetési adatok, videófelvevételek, dokumentumok, e-mailek, értékesítési és pénzügyi adatok, szellemi tulajdon;
- személyes adatok, pl. ügyfél- és üzleti partner adatok, munkavállalói nyilvántartások;
- szoftverek, pl. hozzáférés a vevő termékének forráskódjához, a vevő szoftverének módosítása;
- folyamatok, pl. a belső működési folyamatok és konfigurációk dokumentációja, új rosszindulatú folyamatok beillesztése, kapcsolási rajzok stb. dokumentumai;
- a sávszélességet pl. elosztott szolgáltatásmegtagadásra (DDoS), SPAM¹⁵¹ küldésére vagy mások tömeges megfertőzésére használják.
- pénzügyek, pl. kriptoeszközök ellopása, bankszámlák eltérítése, pénzáttalások;
- emberek, pl. a pozíciójuk vagy tudásuk miatt célzottan támadott személyek.

A különböző támadási formák ismerete azért fontos, mert egy szervezet még akkor is sebezhető lehet egy ellátási lánc elleni támadással szemben, ha egyébként jó védelmi rendszerekkel rendelkezik. Előfordulhat például az, hogy egy vállalkozásnak a saját védelme kiváló, ezért a támadók új utat keresnek a beszivárgáshoz, például a szállítóján keresztül, ezáltal célpontot (áldozatot) gyártva az eredetileg nem célpont szállítóból. Az esetek többségében ráadásul ugyanazon szállítón keresztül számos vevő elérhető az ellátási lánc természetének köszönhetően, így az ilyen típusú támadások potenciális hatása óriási lehet. Többek között ezért is egyre gyakoribbak az ilyen támadások, mivel a támadóknak lehetőséget biztosítanak egyrészt arra, hogy potenciálisan növeljék a hírnevüket, másrészt arra is, hogy jelentősen nagyobb pénzügyi nyereségre tegyenek szert.

Az ellátási láncot érintő támadások további jellemzője az, hogy a kezelésük rendkívül összetett, valamint a támadások mérséklése és kezelése sokkal nagyobb erőfeszítést igényel, mint egy átlagos támadás. Már maga az, hogy legalább két szervezetet érint egy támadás, ez bonyolítja az incidens kezelését, illetve a történést felderítését és elemzését. Az a tény, hogy

¹⁵¹ a fogadók által nem kért, elektronikusan, például e-mailen keresztül tömegesen küldött hirdetés, felhívás vagy lánclevél.

a szállító-vevő kapcsolat többszintű, folyamatosan fejlődik és bővül, és mind a szállítók, mind a vevők folyamatosan frissítik-fejlesztik a rendszereiket, szükségessé teszi az ellátási lánc folyamatos biztonságának biztosítását, valamint az aktív kockázatértékelést és -kezelést.

Ebben az esetben is igaz, hogy egy lánc olyan erős, mint amilyen erős a leggyengébb láncszeme, így az élelmiszer ellátó láncokban is a sebezhetőség mértéke attól függ, mennyire sérülékenyek a szereplők. A kockázatokat tovább növelhetik olyan tényezők, mint például:

- a lánc tagjai körében össze nem hangolt fejlesztések;
- az interoperabilitás hiánya, elavult hardverek és szoftverek;
- különböző korú, gyártmányú és platformú eszközök komplex rendszerbe összekapcsolása;
- különböző felhőszolgáltatók, platformok és szabványok használata;
- eltérő jogszabályi környezethez, illetve szabványokhoz igazodás kényszere;
- eltérő szervezeti, információbiztonsági és adatvédelmi kultúra;
- különböző szándék a fejlesztések tekintetében;
- pénzügyi problémák a finanszírozásban, illetve az olcsóbb, helyettesítő termékek beszerzése a láncban domináns szervezet igényeinek kielégítése érdekében (kényszerű megfelelés).

Természetesen ezek a kockázatok együttműködés keretében csökkenthetők, ám éppen a Walmart blokklánc projektje bizonyította be, a fejlődés gátja, de legalábbis lassítója lehet az ellátólánc szereplőinek ellenállása, illetve eltérő finanszírozási képessége.

Az ellátási lánc elleni támadások sikerességét elősegíti a globális piacok összekapcsolódása. Ha több vevő ugyanattól a szállítótól függ, akkor a szállítót ért támadás következményei felerősödnek, ami nagyszabású nemzeti vagy akár határokon átnyúló, globális hatást eredményezhet. Ráadásul egyes termékek (például a szoftverek és a futtatható kódok) esetében a végfelhasználó számára átláthatatlan vagy akár teljesen rejtett is lehet a szállítói lánc létezése.

A már megtörtént eseteknek köszönhetően a szervezetek egyre inkább tudatában vannak annak, hogy fel kell mérniük a szállítóik kiberbiztonsági állapotát és az ebből az állapotból eredő kockázatokat, azaz kísérletet kell tenniük arra, hogy megállapítsák, mely szervezet a leggyengébb láncszeme az ellátóláncnak.

Mit tehetnek a vevők az ellátó lánc kiberbiztonsági kockázatainak kezelése érdekében? Az ENISA ajánlása alapján – többek között –

- meg kell határozniuk a kockázatokat a különböző típusú szállítóik és az igénybe vett szolgáltatások tekintetében (pl. kritikus szoftverfüggőségek, közösen használt rendszerek stb.);
- az ellátási lánc kockázatait saját üzletmenet-folytonossági hatásvizsgálataik és követelményeik szerint kell értékelniük;
- a bevált gyakorlatok alapján intézkedéseket kell meghatározniuk a kockázatok kezelésére;
- folyamatosan nyomon kell követniük az ellátási lánc kockázatait és veszélyeit és
- az alkalmazottakban is tudatosítaniuk kell a kockázatokat, illetve fel kell készíteni őket ezeknek a kockázatok kezelésére.

A szállítókkal való kapcsolat kezelése érdekében a vevőknek:

- a termék vagy szolgáltatás teljes életciklusa során felügyelniük kell a beszállítóikat;
- osztályozniuk kell a szállítókkal megosztott vagy számukra hozzáférhető eszközöket és információkat, és meg kell határozniuk a hozzáférésükre és kezelésükre vonatkozó eljárásokat (ehhez segítséget nyújthat a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet már említett Kézikönyve¹⁵²);
- meg kell határozniuk a szállítók kötelezettségeit a szervezet eszközeinek védelmével kapcsolatban és olyan területeken is, mint például az információ megosztása, az ellenőrzési jogok, az üzletmenet folytonosságára, a személyzet átvilágítására és az incidensek kezelésére vonatkozó felelősségi körök, az értesítési kötelezettségek és eljárások;
- meg kell határozniuk a beszerzett termékek és szolgáltatások biztonsági követelményeit;
- mindezen kötelezettségeket és követelményeket írásos szerződésbe kell foglalni;
- folyamatosan figyelemmel kell kísérniük a szolgáltatások teljesítményét, például rutinszerű biztonsági ellenőrzéseket kell végezniük a megállapodásokban foglalt kiberbiztonsági követelmények betartása érdekében;
- biztosíték megkövetelése a téren, hogy a szállítók és szolgáltatók biztosította termékek nem tartalmaznak tudatosan rejtett funkciókat vagy hátsó ajtókat;

¹⁵² Nemzeti Kibervédelmi Intézet: Felhasználói kézikönyv A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez 2021. december, <https://nki.gov.hu/wp-content/uploads/2021/12/Felhasznaloi-kezikonyv-vedelmi-intezkedesekhez-v1.0.pdf>

- meg kell határozniuk, hogyan kezelik a fejlesztések, illetve a digitális transzformáció, valamint a technológiai fejlesztések generálta változásokat.

Az ENISA nem említi az iránymutatásában, de mindenképpen meg kell jegyezni, amennyiben ezek a rendszerek személyes adatokat tartalmaznak, a GDPR számtalan követelményt ír elő ezen rendszerek biztonságos üzemeltetése, illetve a szerződő felek kapcsolata tekintetében. Ilyen például az a kötelezettség, hogy az adatkezelésben érintett szereplőknek mindig képesnek kell lenniük elszámolni azzal, hogy mi történt a személyes adatokkal. Az írásban megkötött szerződések esetében számtalan kikötés van azok kötelező tartalma tekintetében, különösen az adatfeldolgozásra vonatkozó megállapodások esetében. A kötelezettségek megszegése esetében pedig az illetékes adatvédelmi hatóságok súlyos büntetéseket szabhatnak ki.

A szállítóknak

- biztosítaniuk kell, hogy a termékek és szolgáltatások tervezésének, fejlesztésének, gyártásának és szállításának infrastruktúrája a jó kiberbiztonsági gyakorlatokat kövesse;
- az általánosan elfogadott biztonsági gyakorlatokkal összhangban lévő biztonságos tervezési-gyártási folyamatot kell rendszeresíteniük;
- megfelelőségi nyilatkozatokat ajánlhatnak fel a vevőknek az ismert szabványokhoz (pl. ISO/IEC 27001), illetve csatlakozhatnak tanúsítványokhoz;
- rendszeresen ellenőrizniük kell a saját információbiztonsági megfelelőségüket;
- vizsgálniuk kell a belső és külső források által jelentett biztonsági réseket, illetve ezeket a problémákat kezelniük is kell;
- ki kell dolgozniuk olyan tájékoztatási eljárást, amely alkalmazásával szükség esetén hatékonyan tudják a vevőiket tájékoztatni;
- az együttműködésre vonatkozó megállapodásokban foglaltakat be kell tartaniuk, különös tekintettel a biztonsági és az adatvédelmi incidensekkel kapcsolatos értesítési és együttműködési kötelezettségekre.

Az ENISA figyelmeztet arra is, vannak olyan kockázatok, amelyeket nem lehet mérsékelni a jó gyakorlatokkal, például a hardverkomponensekben rejlő rejtett funkciókat és dokumentálatlan hozzáférési lehetőségeket nem lehet kimerítően azonosítani a legelterjedtebb tanúsítványokkal vagy szabványos behatolásvizsgálatokkal, illetve a nulladik napi sebezhetőségek is nagy kihívást jelentenek. Előfordulhatnak olyan támadások is, amelyek túlmutatnak a klasszikus értelemben vett támadásokon, például azok, amelyeket fejlett képességekkel rendelkező állami

szereplők támogathatják azt. Az ilyen esetekben szükség lehet az illetékes hatóságok, illetve magas szintű politikai szereplők segítségére is ezen támadások kockázatainak mérsékléséhez.

Összefoglalás

Az információbiztonság és a digitalizáció területén számos kihívással kell megküzdeniük az élelmiszerellátó láncok szereplőinek, és nemcsak a saját tevékenységükből eredő kockázatokat kell kezelniük, hanem mindazon ellátó lánc tagjainak kockázatait is, amelynek részesei. Ezért nemcsak az élelmiszerlánc kockázatait kell ismerniük, hanem például az általuk, illetve a lánc tagjai által közösen használt szoftverek fejlesztőinek, üzemeltetőinek és támogatóinak a kockázatait is.

A tapasztalatok azt mutatják, mivel az információbiztonság terén megfelelően felkészült szervezetek elleni közvetlen támadások költségei nőnek, a támadók inkább az ellátási láncot támadják meg, motivációjukat pedig erősítheti az, hogy ezzel potenciálisan komolyabb hatást tudnak elérni, a nemzeti szintről kilépve a nemzetközi szintérre.

Az élelmiszerellátó láncok esetében elsődleges szempont az élelmiszerek biztonságának, illetve az ellátás folyamatosságának biztosítása, ezt pedig jelentősen veszélyeztetheti a „farmtól az asztalig” láncban, illetve az összekapcsolt rendszerekben használt szoftvereket, illetve ezen szoftverek szállítói láncát érintő támadások. Ezek a támadások azonban nemcsak a szoftverek ökoszisztémájába vetett bizalmat rengethetik meg, hanem az élelmiszerbiztonságba vetett bizalmat is. Ráadásul az ENISA statisztikái alapján 2021-ben a beszállítók ellen alkalmazott támadási vektorok 66%-a még mindig ismeretlen volt, és az átláthatóság, az elszámoltathatóság, valamint a kivizsgálási képesség hiánya komoly kockázatot jelent az ellátási láncba vetett bizalomra.

Az információbiztonsági szakembereknek azonban nemcsak a jelent kell ismerniük, hanem a jövőre is gondolniuk kell. Az ENISA szakemberei kísérletet tettek arra, hogy megjósolják, milyen fenyegetésekkel kell számolniuk a szervezeteknek 2030-ban¹⁵³, és az alábbi főbb fenyegetéseket prognosztizálták:

1. ellátási lánc kompromittálódása szoftverfüggőségek miatt;
2. fejlett dezinformációs kampányok;
3. digitális megfigyelési önkényuralom térnyerése, illetve a privát szféra elvesztése;

¹⁵³ ENISA Foresight Cybersecurity Threats for 2030. March 29, 2023. <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

4. emberi hiba és elavult öröklött rendszerek a kiber-fizikai ökoszisztémákban¹⁵⁴;
5. célzott támadások az intelligens (smart) eszközökből származó adatok felhasználásával;
6. a világűrbe telepített infrastruktúra és eszközök vizsgálatának, valamint ellenőrzésének hiánya;
7. fejlett hibrid fenyegetések térhódítása;
8. szakképzettség hiánya;
9. a határokon átnyúló IKT-szolgáltatások¹⁵⁵, mint egyetlen hibapontok;
10. a mesterséges intelligenciával való visszaélés.

Az ENISA előrejelzése szerint a fenyegetettségek között mindenképpen dobogós lesz az ellátási láncok kompromittálódása az általuk használt szoftverek miatt, de az élelmiszerellátó láncok információbiztonsági szakembereinek kiemelt figyelmet kell fordítaniuk az emberi hibákra, a szakképzettség hiányából eredő problémákra, az elavult, öröklött rendszerekből eredő gondokra, az összekapcsolt (intelligens) rendszerekre és nem utolsósorban a mesterséges intelligencia nem megfelelő alkalmazására is.

Mindezek alapján a jövő élelmiszerellátó lánc tagjainak kiemelt kockázatként kell kezelniük nemcsak a saját, de a szállítóik információbiztonsági megfelelőségét is, különösen az általuk igénybe vett felhőszolgáltatók és menedzselt szolgáltatók esetében. Éppen ezért ezeknek a szervezeteknek be kell vezetni azt az eljárásrendet is, hogy ne csak a saját maguk, hanem a szállítóik megfelelőségét is ellenőrizzék, erre pedig ki kell alakítaniuk a speciális audit folyamataikat, illetve azt, hogy milyen tanúsítványokat követeljenek meg kritikus üzleti partnereiktől a folyamatos és biztonságos működésük érdekében.

A JBS Foods esete megmutatta, hogy a megnövekedett kölcsönös függőségek és az egyre komplexebb folyamatok miatt egy információbiztonságot érintő (zsarolóvírusos) támadás milyen messzemenő következményekkel járhat nemcsak nemzeti, de országhatárokon átnyúló szinten is. A következmények pedig nemcsak az érintett felek nagy száma miatt lehet súlyos, de akár élelmiszerbiztonsági, nemzetbiztonsági vagy geopolitikai következményekkel kapcsolatos aggodalmakra is okot adhat.

¹⁵⁴ Kiber-fizikai rendszerek hardverbe ágyazott szoftverekből, például érzékelőkből, processzorokból és kommunikációs technológiákból állnak, és képesek önállóan információt cserélni, műveleteket indítani és egymást önállóan irányítani. European Parliament. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy. Industry 4.0. IP/A/ITRE/2015-02. February 2016. PE 570.007. p. 22. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

¹⁵⁵ „Az IKT fogalma: az Információs és Kommunikációs Technológiák olyan eszközök, technológiák, szervezési tevékenységek, innovatív folyamatok összessége, amelyek az információ- és a kommunikációközlést, feldolgozást, áramlást, tárolást, kódolást elősegítik, gyorsabbá, könnyebbé, és hatékonyabbá teszik.” forrás: Lengyel dr. Molnár Tünde és Dr. Kis-Tóth Lajos: IKT innováció. Eger, 2015 http://okt.ektf.hu/data/szlahorek/file/kezek/05_ikt_02_27/221ikt_fogalma.html

Irodalomjegyzék

Hassouna A, Bekhitc A. E, Jambrakd A. R, Regensteine J. M, Chematf F, Mortong J. D, Gudjónsdóttirh M, Carpenai M, Prietoi M. A, Varelanj P, Arshadk R. N, Aadill R. M, Bhatm Z, Ueland Ø. **The Fourth Industrial Revolution in the Food Industry— Part II: Emerging Food Trends.** Critical Reviews In Food Science and Nutrition. 2022. DOI:10.1080/10408398.2022.2106472.

Babu L, Ganesh (2021) **Recent Scope for AI in the Food Production Industry Leading to the Fourth Industrial Revolution.** Webology, 18 (2). pp. 1066-1080. DOI: 10.14704/WEB/V18I2/WEB18375.

Case Study: **How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric**, HYPERLEDGER Blockchain Technologies for Business, utolsó letöltés: 2021. https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdfhttps://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf, utolsó letöltés: 2021. február 26.

Casino F, Kanakaris V, Dasaklis T. K, Moschuris S, Rachaniotis N. P. **Modeling food supply chain traceability based on blockchain technology**, 2019. <https://doi.org/10.1016/j.ifacol.2019.11.620>

Commission Nationale Informatique & Libertés (CNIL). **BLOCKCHAIN** 2018. https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf

Defending Against Critical Threats, CISCO Secure, <https://blogs.cisco.com/security/defending-against-critical-threats-analyzing-key-trends-part-1>

Digital Business Strategies in Blockchain Ecosystems - Transformational Design and Future of Global Business, szerk: Hacioglu U, Springer Nature Switzerland AG 2020

EDPB - 4/2019. számú **iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről.** 2.0.v. 2020. október 20. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf

EDPB Guidelines 01/2021 on **Examples regarding Personal Data Breach Notification**. Adopted on 14 December 2021. Version 2.0. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

ENISA **Artificial Intelligence Cybersecurity Challenges**. Szerk.: Malatras A, Dede G. DOI 10.2824/238222 December 15, 2020. <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>

ENISA **Good Practices for Security of IoT** - Secure Software Development Lifecycle. 2019. DOI: 10.2824/742784 <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>

ENISA **Good practices for security of Smart Cars**. 2019. DOI 10.2824/17802 <https://www.enisa.europa.eu/publications/smart-cars>

ENISA **Securing Machine Learning Algorithms**. Szerk.: Malatras A, Agrafiotis I, Adamczyk M. DOI: 10.2824/874249 2021. <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>

ENISA **Supply Chain Integrity**. 2015. https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport

ENISA **Threat Landscape For Ransomware Attacks**. Szerk.: I. Lella, E. Tsekmezoglou, R. Naydenov, A. Malatras, S. Garcia, V. Valeros, A. Goma 2022. DOI: 10.2824/456263 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>

ENISA **Threat Landscape for Supply Chain Attacks**. Szerk.: I. Lella, M. Theocharidou, E. Tsekmezoglou, A. Malatras, S. Garcia, V. Valeros 2021. DOI: 10.2824/168593 <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

ENISA **Threat Landscape**, Szerk.: I. Lella, E. Tsekmezoglou, R. S. Naydenov, C. Ciobanu, A. Malatras, M. Theocharidou 2022. ISBN: 978-92-9204-588-3, DOI: 10.2824/764318 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Federal Office for Information Security: **Towards Secure Blockchains Concepts, Requirements, Assessments**, 2019, Federal Office for Information Security (BSI) 53175 Bonn, Germany, utolsó letöltés: 2021. február 26. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf?__blob=publicationFile&v=3https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf?__blob=publicationFile&v=3

Finck, Dr Michèle - **Blockchain and the General Data Protection Regulation**, European Parliamentary Research Service (EPRS) Scientific Foresight Unit (STOA), 2019. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

Gibraltar Regulatory Authority (GRA) - **GN16 Blockchain**, 2020. <https://www.gra.gi/data-protection/guidance>

Hassoun A, Aït-Kaddour A, Adnan M. Abu A. M, Mahfouz, Bhojraj N, Baderg R. F, Barbah F. J, Biancolillo A, Cropotova J, Galanakis C. M, Jambrak A. R, Lorenzo J. M, Måge I, Ozogulq F, Regenstein J. **The Fourth Industrial Revolution in the Food Industry — Part I: Industry 4.0 Technologies**. Critical Reviews In Food Science and Nutrition. 2022. DOI:10.1080/10408398.2022.2110033.

Canelón J, Huerta E, Incera J, Ryan T: **A Cybersecurity Control Framework for Blockchain Ecosystems**, The International Journal of Digital Accounting Research Vol. 19, 2019, pp. 103-144 ISSN: 2340-5058

Bambara J. J, Allen P. R: **Blockchain - A Practical Guide to Developing Business, Law, and Technology Solutions**, McGraw-Hill Education 2018, ISBN: 978-1-26-011587-1

Lezoche M, Hernandez, J. E, Alemany, M. M. E, Panetto, H, Kacprzyk, J. **Agri-food 4.0: A Survey of the Supply Chains and Technologies for the Future Agriculture**. Computers in Industry. 2020. <https://doi.org/10.1016/j.compind.2020.103187>

Malatras Dr. A, Skouloudi C, Koukounas A. **Industry 4.0 - Cybersecurity Challenges and Recommendations**. ENISA 2019. DOI: 10.2824/143986
<https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>

Mattioli R, Malatras A, Hunter E. N, Biasibetti Penso M. G, Bertram D, Neubert I. **Foresight Cybersecurity Threats for 2030**. ENISA 2023. DOI: 10.2824/117542
<https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

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

Skouloudi C, Malatras A, Naydenov R, Dede G. **Guidelines for Securing the Internet of Things**. ENISA 2020. DOI: 10.2824/314452

<https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>

Smit J, Kreutzer S, Moeller C, Carlberg M.: **Economic And Scientific Policy. Industry 4.0**. Analytical Study. European Parliament. Directorate General for Internal Policies Policy Department A. IP/A/ITRE/2015-02. February 2016. PE 570.007.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU\(2016\)570007_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

The State of Ransomware 2021, Sophos Whitepaper. 2021, <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

Xiaolin Xu, Rahman F, Shakya B, Vassilev A, Forte D, Tehranipoo M.: **Electronics Supply Chain Integrity Enabled by Blockchain**, Author manuscript; available in PMC 2020 Feb 28., Published in final edited form as: ACM Transact Des Autom Electron Syst. 2019; 24(3): 10.1145/3315571. doi: 10.1145/3315571

Jogszabályok:

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

2003. évi C. törvény az elektronikus hírközlésről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR)

Javaslat az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok **(a mesterséges intelligenciáról szóló jogszabály)** megállapításáról és egyes uniós jogalkotási aktusok módosításáról, Brüsszel, 2021.4.21., COM(2021) 206 final, 2021/0106(COD), <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>