8. fejezet

Az ellátási láncok támadása, azaz mi történik, ha már a nyomtatott áramkör sem megbízható?

Koczka Ferenc

Bevezetés

Az 1994-ben még könyvkereskedelemmel foglalkozó webshopból a világ egyik legnagyobb vállalatává fejlődött amerikai vállalat, az Amazon 2015-ben már a videostreaming-piacon igyekezett stabilizálni a helyzetét. Olyan szoftverre volt ehhez szükség, amely lehetővé teszi nagy méretű videofile-ok tömörítését és gyors konverzióját úgy, hogy azok különböző platformokon is lejátszhatók legyenek. Akkoriban egy alig ismert startup, az Elemental Technologies (ET) már kifejlesztett erre egy kiváló referenciákkal rendelkező megoldást. A szoftvert nemcsak a Központi Hírszerző Ügynökség (CIA) alkalmazta, hanem kritikus alkalmazásokban, például a Nemzetközi Űrállomással való kapcsolattartásban is használták. Az Amazon számára kézenfekvő megoldás volt a startup felvásárlása, így a jól ismert recept szerint meg is kezdte a cég beolvasztását. A termékre nemcsak az Amazon Prime Video szolgáltatás továbbfejlesztését alapozták, ugyanez a technológia került be a CIA számára épített különleges biztonsági követelményeket támasztó felhőbe is. Ez – a korábbiakkal ellentétben – megkövetelte az alkalmazott elemek szigorú auditját; a részletes átvizsgálási folyamat során kiderült, hogy a startup Supermicro gyártmányú szervereinek alaplapjai egy, az eredeti dokumentációban nem szereplő, rendkívül kis méretű chipet is tartalmaznak.[1] Mivel a chipet ismeretlen helyen, valószínűsíthetően a gyártást követően építették be, az incidenst jelentették az amerikai hatóságoknak. Hamarosan világossá vált, hogy a népszerű szervergyártó így módosított kiszolgálói számos más kormányzati szervezet informatikai rendszerében is megtalálhatók,

[1] Bodnár Zsolt: Rizsszemnyi mikrochipekkel hajthatta végre Kína a legnagyobb USA elleni támadást. *Qubit.hu,* 2018. október 5.

https://doi.org/10.36250/01079_08

https://orcid.org/0000-0002-7541-6495

többek közt a Védelmi Minisztérium adatközpontjában és az Amerikai Haditengerészet hadihajóinak fedélzeti hálózatában is.

Az érintett szerverek nagy száma miatt az eset kivizsgálása évekig tartott. Amerikai elemzők megállapítása szerint a chip az operációs rendszer magját módosította úgy, hogy lehetővé tette annak későbbi megváltoztatását, hátsó ajtót nyitott[2] az érintett szerverekben, amely lehetővé tette a gépek azonosítását és további kódok lefuttatását. A chipeket kínai alvállalkozók gyáraiban ültethették be azokba az alaplapokba, amelyeket összeszerelésre szállítottak oda.[3] Mivel a Supermicro az egyik legnagyobb szervergyártó, gépei a világ számos hálózatában működnek, így világszerte lehetnek olyan gépek, amelyek ezzel a módosítással sérülékennyé váltak.

Különböző források eltérően nyilatkoztak az esetről, és több cég nem ismerte el az érintettségét. Ilyen reakció 2015-ben az informatikai incidensek 20%-ában fordult elő.[4] Ügyfelei és reputációja megőrzése érdekében ugyanis számos szervezet igyekszik megakadályozni, hogy incidensei napvilágra kerüljenek. Az Apple például annak ellenére, hogy állítása szerint nem talált érintett Supermicro gépet a hálózatában, közel 7000 ilyen gyártmányú szervert cserélt le. Híradások szerint legalább 30 amerikai nagyvállalat volt érintett az esetben, ugyanakkor a hatásokról alig áll rendelkezésre hiteles információ. Az érintettek teljes köre és az idegen áramkör beültetését végző cég is ismeretlen maradt, egyes források az utóbbi létezését is igyekeznek cáfolni.

Az eset egyike volt azoknak, amelyek új fejezetet nyitottak az incidensek történetében, mivel a támadás a korábbiaktól eltérően nem valamilyen szoftverhiba kihasználásán alapult. A kompromittált alaplapok felfedezésének valószínűsége eléggé csekély, hiszen csak egy olyan vizsgálat deríthetett fényt a chip jelenlétére, amelyet a legtöbb szervezet soha nem végez el. Az a lehetőség, hogy akár kritikus infrastruktúrák működtetésében szerepet játszó kiszolgálók adattartalma tartósan lehallgatható, azok adatai módosíthatók, működésük megváltoztatható,

[2] A hátsó ajtó *(backdoor)* elnevezésű (szoftver-) komponens ahhoz nyújt lehetőséget, hogy egy rendszerhez annak üzemeltetője által nem ismert és nem szándékozott hozzáférést biztosítson. A *backdoorok* telepítését a támadók a rendszer sikeres feltörése után végzik, ezzel biztosítják, hogy ahhoz az eredeti biztonsági hiba elhárítása után hozzáférjenek. Mivel erre rengeteg megoldás létezik, és az üzemeltetők nem feltétlenül ismerik ezeket, ezért egy rendszer kompromittálódása esetén a legtöbbször arra kényszerülnek, hogy tiszta forrásból teljes egészében újratelepítsék azt.

[3] Jordan Robertson – Michael Riley: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek,* 2018. október 4.

[4] Javvad Malik: *Ethics, Security and Getting the Job Done.* AlienVault, 2015. november.

adott esetben akár el is pusztítható, bármely kormányzat számára elfogadhatatlan kockázatot jelent. A Supermicro története egy olyan, kifejezetten nehezen felderíthető támadómódszer tömeges elterjedésének lehetőségére világított rá, amelytől a biztonsági szakemberek talán leginkább tartanak: a célzott APT-támadások[5] sikeres kivitelezésére kritikus információs infrastruktúrákban.

Visszatekintve a Supermicro-ügyre ma már elmondható, hogy az egyáltalán nem volt egyedi. Az olvasó számára minden bizonnyal ismert a Huawei esete, amikor az Egyesült Államok mellett többek közt Svédország, Nagy-Britannia és Lengyelország is megtiltotta, hogy stratégiai rendszereit a gyártó eszközeiből építsék fel. Bár ebben az ügyben sem került napvilágra egyértelmű bizonyíték, számos ország szűkítette az informatikai eszközeinek beszállítói körét, előnyben részesítve így a saját politikai vagy katonai közössége által megbízhatókat. Több EU-tagállam ezért leginkább az európai és amerikai gyártmányú termékkör alkalmazását részesíti előnyben.

Az informatikai rendszerek valódi támadóit annak ellenére rendkívül nehéz teljes bizonyossággal azonosítani, hogy a motivációelemzéstől a forenzikus vizsgálatokig számos módszer alkalmazható annak eldöntésére, hogy egy magányos támadó akciójával, egy csoport által kivitelezett kibertámadással vagy éppen katonai célú kiberművelettel, esetleg annak előkészítésével állunk szemben. Általános vélemény, hogy az említett támadásokat elsősorban nemzetállamok által finanszírozott csoportok képesek megvalósítani, és ezek célja elsősorban gazdasági, politikai vagy katonai előny megszerzése. A katonai műveletekben egyre nagyobb szerep jut a kibertérnek, mivel az információ megszerzése, az ellenség döntéseinek befolyásolása és erőforrásainak pusztítása ebben is eredményes lehet. Ennek következtében az elmúlt évtizedben felértékelődött az a képesség, amely a szemben álló fél informatikai rendszereinek lehallgatását, befolyásolását vagy működésének megzavarását a kibertérben teszi lehetővé.

A kritikus infrastruktúrák működőképessége valamennyi ország működőképességének fenntartásához elengedhetetlen. A magyar politikai vezetés számára már a 2010-es években is világossá vált a kibertér stratégiai szerepe. A kibertérbe helyezett funkciók bizalmasságának, rendelkezésre állásának és sértetlenségének fenntartása és fejlesztésének szükségessége a Magyarország

[5] APT: *Advanced Persistent Threat.* A támadás célja egy rendszer feltörése és a folyamatos, rejtett hozzáférés hosszú időn át történő fenntartása. Az APT-támadások célja rendszerint kormányzati, pénzügyi, gazdasági és katonai szervezetek rendszereiben tárolt adatok szivárogtatása.

Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat szövegében is megjelenik:

> „31. Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét."

> „32. Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."

Nem ismert a Supermicro-gépekre alapozott támadás kivitelezőinek indítéka. Lehetséges, hogy az informatikai rendszereken nyitott hátsó ajtók tömegét csak alkalomszerűen megvalósított támadásokra akarták felhasználni. Elképzelhető, hogy a terv további elemei csak a szerverek üzembe állítása után alakultak ki. Ha feltételezzük, hogy ismert lehetett számukra a gyártó vásárlói köre, esetleg be tudtak avatkozni a szállítási folyamatokba, akkor elképzelhető, hogy egy célzott támadást ilyen „messziről" indítottak. Tekintettel a valószínűsíthető megbízói körre azonban számolni kell a kritikus infrastruktúrák működését biztosító szűkebb terület, az *ellátási lánc* támadásával, vagy akár az ellátási láncon keresztül megvalósított további műveletek előkészítésével.

Az ellátási lánc

Az ellátási lánc *(supply chain)* meghatározására több különböző forrást is találhatunk. A hazai szakirodalom egyik elfogadott meghatározása szerint az „ellátási láncok […] egy adott fogyasztói igény kielégítésére szerveződő, egymással lineáris és vertikális kapcsolatban lévő vállalatokból állnak".[6] Az egyes szakterületek specifikus meghatározásokat adnak, és esetükben hiba lenne a hagyományos értelemben vett termékekre és szolgáltatásokra szorítkozni. A NIST-

[6] Chikán Attila: *Vállalatgazdaságtan*. Budapest, Aula, 2004.

800-161 az információs és kommunikációs technológiák (ICT)[7] ellátási láncát a beszerzők, integrátorok és beszállítók közötti erőforrások, folyamatok összekapcsolt halmazaként definiálja, amely az ICT-termékek és -szolgáltatások tervezésétől a fejlesztésén, beszerzésén, gyártásán át a végfelhasználóhoz jutásáig tart.[8] Az Amerikai Védelmi Minisztérium az ellátási lánc három meghatározását is alkalmazza, amelyek elsősorban a fegyverrendszerekhez kapcsolódnak. Ezek: a mikroelektronikai berendezések beszerzésére szolgáló globális lánc, a beszerzési ellátási lánc, valamint a fenntartási ellátási lánc.[9] Ezeket a termékek előállításában, kezelésében, elosztásában és feldolgozásában részt vevő szervezetek és folyamatok rendszereként definiálják, amelynek célja a termékek, az információ, a tudás és a financiális források biztosítása az előállító és a fogyasztó között.

A meghatározások értelmében az *ellátási lánc támadása* olyan művelet, amelynek célja az ellátási lánc működési folyamataiba történő beavatkozás azért, hogy a támadó elérje a szándékának megfelelő hatást.

Nemzetbiztonsági szempontból az ellátási lánc szerepe leginkább a gazdasági, közmű-, ipari, pénzügyi, kormányzati és közigazgatási, távközlési, média-, valamint a katonai szervezetek folyamataiban kiemelkedő, de szinte bármilyen szervezet működésében alapvető. Mind alkalmaz eszközöket, igénybe vesz szolgáltatásokat, amelyek nélkül nem lenne képes teljeskörűen ellátni feladatát. A működéshez szükséges összetevőket szintén az ellátási lánc elemeinek tekintjük, amelyek kiesése nemcsak az adott szervezetben okoz zavart, hanem a ráépülő továbbiak működésében is.

Az ellátási láncra történő első szakirodalmi utalások a rendszerelmélet kialakulásával az 1940-es évekre tehetők. Addig a gyártók határozták meg a termelés körülményeit, és jórészt a kereskedelmet is. A fogyasztó felértékelődése a 70-es évek Amerikájában kezdődött meg, kialakult a termékek összehasonlíthatósága és az árverseny. A kereskedők szerepe kulcsfontosságúvá vált, csökkentek a haszonkulcsok, kiemelt szerepet kaptak a vevői elégedettséget növelő szolgáltatások, mint például a gyorsaság, a garancia vagy éppen a termék visszaválthatósága. Kialakult a gyártók és a kereskedők kölcsönös függősége, a korábbi,

[7] Az ICT ebben az értelmezésében magában foglalja az információ összegyűjtésére, tárolására, továbbítására, lekérdezésére és feldolgozására használt valamennyi technológia minden kategóriáját (például mikroelektronika, nyomtatott áramkörök, szoftverek, informatikai rendszerek, feldolgozók, kommunikációs hálózatok).

[8] NIST Computer Security Center: Definitions.

[9] DoD Defense Science Board: DSB Task Force Report on Cyber Supply Chain, 2017.

push rendszerű elosztórendszereket a *pull* váltotta fel, azaz csak azok a termékek kerültek a kereskedelembe, amelyekre létezett vásárlói igény.

Az elmúlt évtizedekben az informatikai fejlődés a gazdasági rendszerek szervezésében is jelentős változásokat hozott.[10] A nagy gyártók és beszállítók az igények gyors kielégítése érdekében eleinte óriási, csak költségesen fenntartható raktárkészletekkel dolgoztak. Ezeket tette szükségtelenné a gyors kommunikációs csatornákra alapozott új logisztikai módszer, a gyártók számára jelentős költségmegtakarítást eredményező *just in time* (JIT). A JIT a raktározási feladatok csökkentését célozta úgy, hogy a beszállítók a szükséges elemeket csak a felhasználáshoz közeli időpontban szállították. A JIT azonban kényes kockázati elem, akár egyetlen komponens, szélső esetben még egy csavar késedelmes beszállítása is a teljes termelési folyamat elakadását okozhatja. Bár a gyártók igyekeznek szerződésekkel védeni magukat, számos olyan helyzet alakulhat ki, amely ily módon nem kezelhető. A helyzetet tovább rontja, hogy a beszállítók működése szinte minden esetben további beszállítóra alapozott. A nagy gyártók igyekeznek minimalizálni ilyen irányú kitettségüket, ezért a minőségbiztosítás érdekében beszállítóiktól is megkövetelik működésük szabályzását, folyamataik dokumentálását és termékeik azonosíthatóságát, nyomon követhetőségét.[11]

A JIT gyengesége a váratlan katasztrófák, előre nem látható akadályok esetén mutatkozik meg igazán. A kockázatkezelés kialakítása során annak módszertana következtében kevéssé veszik figyelembe a ritkán bekövetkező, ugyanakkor nagy hatású eseményeket. Tűzesetek, hóviharok, földrengés, sztrájk és különféle terrorcselekmények ezért hirtelen nagy hatással lehetnek egy ország kulcsfontosságú területeire. A 9/11-es terrortámadásokat követően, amelyek egyik fő célpontja a New-York-i Világkereskedelmi Központ volt, súlyos zavarok keletkeztek az ellátási láncban.[12] Szinte azonnal leállt a teljes légi közlekedés, korlátozták a határok forgalmát, de a belföldi áruszállításban

[10] Sarah Hippold: 5 Trends From the Gartner Hype Cycle for Supply Chain Strategy. *Gartner,* 2020. október 2.

[11] A gyártók számos különböző szabvány szerinti minősítést követelhetnek meg. Magyarországon jellemzően az ISO 9001 szabványcsalád az elvárt követelmény, de egyes iparágak további elvárásokat is támaszthatnak, például az autóiparban a QS-9000 tartalmazza az ágazatspecifikus többletkövetelményeket.

[12] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Tanulmánygyűjtemény.* Budapest, Nemzeti Közszolgálati Egyetem, 2016.

is nagy veszteségek forrása volt az a körülmény, hogy a hatóságok a gyanús kereskedelmi konténerek tartalmát is átvizsgálták. 2021-ben az Ever Given konténerszállító hajó egy manőverezési hiba következtében elzárta a Szuezi-csatornát, és így a világkereskedelem 12%-át bonyolító útvonalat tett hetekre használhatatlanná, amivel nemcsak a beszállítási folyamatokat akasztotta meg, hanem világgazdasági szinten érzékelhető zavart okozott. A Covid–19 hatása az ellátási láncban közismert; több autógyár is felfüggesztette gyártási folyamatait az ellátási láncban keletkezett zavarok következtében. Az ilyen típusú eseményekre nehéz költségarányosan felkészülni úgy, hogy minden negatív következmény kizárható legyen, így inkább a kialakult helyzet megfelelő kezelésére érdemes erőforrásokat biztosítani.

A fejlődés nem állt meg a JIT szintjén, az Ipar 4.0 – amelyet negyedik ipari forradalomként is szokás említeni – alapkoncepciója a gyártók és beszállítóik rendszereinek, akár magát a (rész)termékek előállítását végző gépeknek az adatszintű összekapcsolása. Ellentétben a JIT logisztikájával, amely alapvetően emberek munkájára épül, az Ipar 4.0 esetében a gépek közti kommunikációra kerül a hangsúly. E koncepció Achilles-sarka az időzítés, amely még inkább magában hordozza a könnyű célponttá válás lehetőségét egy ellenséges támadás megtervezése vagy kivitelezése során.

A pénzügyi rendszerek működése szintén az ellátási láncra épül. A kereskedelem ma már nem működhetne a banki rendszerek támogatása nélkül,[13] és azok sérülése a gazdasági rendszer működésére nézve is katasztrofális következményekkel járna. A fejlett gazdasági rendszerrel rendelkező társadalmak visszaszorították a készpénzforgalmat, aminek következtében a banki rendszerek üzemzavara esetén nemcsak a gazdasági szféra működése bénulna meg, hanem a lakosság is csak korlátozottan lenne képes akár egyszerű vásárlásokat is lebonyolítani. A pénzügyi rendszer kitettsége már 2007-ben, az Észtország ellen irányuló kiberműveletben[14] is nyilvánvalóvá vált. A szektor kiemelt szerepét mutatja, hogy a készpénzellátás, a bank- és hitelintézeti biztonság és a pénzügyi eszközök kereskedelmi, fizetési, klíring- és elszámolási infrastruktúrái és rendszerei a nemzeti létfontosságú rendszerelemek pénzügyi ágazatának kiemelt elemei. A pénzügyi rendszer zavaraiból származó károk mértéke mérhető volt azokban az országokban, ahol politikai okokból az internet lekapcsolása mellett

[13] Juhász Péter – Száz János – Misik Sándor: Ellátási láncok versenyképessége és finanszírozása – gondolatok az optimumról. *Közgazdasági Szemle,* 64. (2019), 1. 53–71.

[14] Andreas Schmidt: The Estonian Cyberattacks. *Researchgate.net,* 2013. január.

döntöttek. Esetükben 2015-ben az ebből eredő veszteség elérte a 2,4 milliárd dollárt.[15] Ez világossá teszi a pénzügyi rendszerek kiemelt védelmét: egy sikeresen végrehajtott kiberművelet az érintett ország teljes gazdaságán végiggyűrűzne, és amellett, hogy óriási károkat okozna, annak reputációját is jelentősen meggyengítené.[16]

A kormányzatok alapvető érdeke az ellátási láncok működőképességének fenntartása, ezért legfontosabb elemeit kritikus infrastruktúraként azonosítják, így rájuk szabott jogszabályok határozzák meg a működésüket. Ezen túl további szervezetek foglalkoznak a működés szervezésével. 1996-ban több iparág összefogásával alakult meg a Supply Chain Council (SCC), amely kidolgozta az ellátásilánc-menedzsment ipari szabványának tekintett Supply Chain Operations Reference Modelt (SCOR). A téma fontosságát jól szemlélteti, hogy a NIST az amerikai szövetségi ügynökségek számára külön készített kockázatkezelési gyakorlati információkat tartalmazó ajánlást.[17]

Az ellátási lánc támadása tehát kézenfekvő lehetőség egy ország vagy szervezet funkcióinak megzavarásához. Ez nem feltétlenül kötődik a kibertérhez, számos olyan incidens ismert, ahol egyáltalán nem kaptak szerepet elektronikai eszközök. A 2010-es évek gondolatkísérlete, a Digitális Mohács[18] több olyan elképzelt lehetőséget ír le, amely kisebb-nagyobb előkészületet igénylő szabotázsakcióval zavarokat idézhet elő a kritikus infrastruktúrákban, miközben azok egy része egyáltalán nem igényel informatikai tudást. Mivel könyvünk elsősorban a kibertérrel kapcsolatos problémákra koncentrál, a kérdést elsősorban ebből a szemszögből vizsgáljuk.

[15] Darrell M. West: *Internet Shutdowns Cost Countries $2.4 Billion Last Year*. Center for Technology Innovations at Brookings, 2016.

[16] Steven S. DeBusk: *What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack*. Fort Leavenworth, School of Advanced Military Studies United States Army Command and General Staff College (First Term AY 02-03), 2003.

[17] Jon Boyens et al.: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* National Institute of Standards and Technology, 2015.

[18] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56.

Az ellátási láncok támadásainak elemzése

Az ellátási láncokra irányuló incidensek elemzéséhez érdemes megvizsgálni az azok ellen indított eddigi támadásokat, és a konkrét esetek alapján levonni azokat a következtetéseket, amelyek betartásával a működésük biztosítható. Felkutatásuk nem egyszerű, mivel szinte mindegyikük tartalmaz nem publikálható elemeket. Megállapításainkat ezért csak közvetetten, az Amerikai Védelmi Minisztérium (DoD) által elkészített keretrendszer és az abban közzétett 41 konkrét eset katalógusa alapján tesszük meg.[19]

Célok

A MITRE 2017-es *technical reportja*[20] az ellátási lánc támadását *(supply chain attack)* a következőképp határozza meg: szándékos rosszindulatú cselekmény, amelynek célja az információs és kommunikációs technológia *(hardver, szoftver, firmware)* sebezhetőségének létrehozása és végső soron kihasználása az ellátási lánc bármely pontján azzal az elsődleges céllal, hogy megfigyeljen vagy megzavarjon egy műveletet a kibertér erőforrásainak felhasználásával.

A támadó elsődleges szándéka tehát az ellátási lánc működésének megzavarására, a rendszerben tárolt információ megszerzésére, módosítására vagy elpusztítására irányulhat, de általánosságban a CIA-elvek megsértése is lehet cél. Ugyanakkor egy sikeres támadás megnyitja a lehetőségét, hogy egy támadó annak működését a későbbiekben is a saját érdekeinek megfelelően befolyásolja. Ebben az esetben az ellátási lánc támadása valószínűsíthetően egy magasabb taktikai cél eléréséhez szükséges eszköz.

Az ellátási lánc kifinomult támadása az elmúlt évtizedben volt jellemző. A 2010-es évekig még alig fordult elő, hogy az ellátási lánc támadása egy ország gazdaságában jelentősebb problémát okozott volna. Két eset igazán közismert; a 2007-es észt–orosz konfliktus során Észtország gazdasági működése néhány napra gyakorlatilag megbénult. A különlegesen kifinomult Stuxnet pedig 2010-ben akadályozta meg az atomfegyver kifejlesztését, évekkel kitolva

[19] Melinda Reed – John F. Miller – Paul Popick: *Supply Chain Attack Patterns: Framework and Catalog.* Office of the Assistant Secretary of Defense for Research and Engineering, 2014.

[20] William J. Heinbockel – Ellen R. Laderman – Gloria J. Serrao: *Supply Chain Attacks and Resiliency Mitigations, Guidance for System Security Engineers.* MITRE, 2017. október.

az iráni atomprogram végrehajtását.[21] A kibertámadások száma és természete azóta jelentős változáson ment keresztül. Bár a magyar kibervédelmi szakemberek többsége egyetért abban, hogy Magyarország fenyegetettsége ma nem számottevő, ez inkább a célzott támadásokra vonatkozik. Nincsenek közismert célzott, magyar létfontosságú rendszerekre irányuló kibertámadások. A nem célzott támadások tekintetében a magyar informatikai rendszerek fenyegetettsége már nem ilyen alacsony, mivel az egyes rendszerek sérülékenységeit kihasználó automaták, amelyek a megtámadott eszközöket a hálózati címek szkennelésével végzik, a megtévesztő levelek mellékleteiként terjedő kriptovírusok által okozott károk a magyar kibertérre ugyanúgy kiterjednek, mint más országokéra. A véletlenre bízott támadások által okozott kár a legtöbb esetben lényegesen kisebb, mint a célzott támadásoké, de az ellenkezőjére is voltak már példák.

Támadási típusok

Az ellátási lánc támadásának operatív célja a konkrét esetek katalógusának elemzése alapján három területre irányul, és mindhárom esetében elérhető a bizalmasság, a sértetlenség és a rendelkezésre állás sérülése.

Egy rosszindulatú hardverelem elhelyezésére részben jó példa a Supermicro esete. Ilyen incidens nem csak a rendszer kialakításának fázisában fordulhat elő, a teljes életciklus alatt további belépési pontok vannak egy meglevő hardverelem kicserélésére vagy módosítására. A hardverelemek manipulálásával végzett támadás a prototípus kialakításától a sorozatgyártáson és a karbantartási folyamatokon keresztül bármikor, szélső esetben akár a rendszer kivezetése után is kivitelezhető. A hardverelemek nemcsak funkcionalitásban, hanem rendelkezésre állásban is jelenthetnek kockázatot. Az Amerikai Légierő már 2012-ben szembesült azzal, hogy a jellemzően külföldről származó, katonai minősítésű elektronikai részegységek nem képesek teljesíteni a velük szemben támasztott követelményeket, egyes esetekben pedig akár újnak látszó, de valójában csak felújított elemek kerülnek a beszállítói láncba. A kezdeti teszteken még jól teljesítő elemek élettartama sokkal rövidebb az elvártnál, ami a légierő gépei esetében katasztrofális következménnyel járhat.[22]

[21] Cserháti András: A Stuxnet vírus és az iráni atomprogram. *Nukleon,* 4. (2011), 1. 1–7.

[22] Flying Fraudulently – How a Weak Supply Chain Became the Usaf's Worst Enemy. *Airforce Technology,* 2012. szeptember 24.

A szoftverelemek cseréje egy információs rendszerrel szemben végrehajtott kiberműveletben kézenfekvő eszköznek tűnik. Sikeres támadás során a számítógépen tárolt szoftverkomponensek módosítása már egyszerű feladat lehet a támadó számára. De nem csak a hagyományos szoftverelemek lehetnek érintettek, a Supermicro esetében a hardverelemekhez közvetlenül kapcsolódó *firmware* is kulcsszerepet játszott a támadó céljának elérésében. A Stuxnet esetében a kritikus elemekben (PLC-kben) is kicserélt/módosított szoftver működött, ez okozta a dúsítók közel 20%-ának megsemmisülését.

Annak ellenére, hogy a szoftverelemek cseréje könnyebben kivitelezhetőnek tűnik, a 41 publikált esetben azonos számban fordult elő szoftverfejlesztők és hardverfejlesztők ellen irányult támadás.

Szintén jellemző támadási típus egy rendszerrel kapcsolatos *adat jogtalan felhasználása* vagy *rosszindulatú módosítása*. Ebbe a típusba nem csak olyan esetek tartoznak, amelyek közvetlenül a kifejlesztett rendszerre vonatkoznak, mert a rendszer megtervezésében és kifejlesztésében részt vevő teljes környezet is támadható. Amennyiben egy kifejlesztendő rendszer kezdeti fázisában felállított követelményrendszert egy támadó képes módosítani, annak funkciói a saját érdekei mentén működhetnek majd a kifejlesztett rendszerben. Ugyanez történhet egy rendszer biztonsági elemzésével, *hardeningdokumentációjával* kapcsolatban is. Módosíthatók lehetnek a rendszer fejlesztői és felhasználói dokumentációi.

Nem túl gyakori, de korántsem példa nélküli lehetőség a fejlesztőeszközök módosítása. Efféle támadás esetén a támadó a fejlesztők által alkalmazott szoftverkörnyezetet módosítja azért, hogy például egy manipulált fordítóprogram a lefordított programkódokban a programozó tudta nélkül káros kódot helyezhessen el. Egy ilyen típusú támadás 2015-ben vált ismertté, amikor az Apple XCode nevű fejlesztőeszközét módosították, majd Kínában az Apple forrásain kívül terjeszteni kezdték. Az ezzel készült alkalmazások egy XCodeGhost nevű kártékony kódot tartalmaztak, átmentek az Apple ellenőrzési eljárásán, és bejutottak az App Store-ba is, így végül hozzávetőleg 500 millió felhasználó vált érintetté.[23]

Támadási pontok

A fenti támadási típusok azonban nemcsak az ellátási láncok közvetlen környezetében, hanem azon kívül is alkalmazhatók, így a védekezés során érdemes

[23] Lin Yang – Quan Yu: *Dynamically Enabled Cyber Defense.* H. n., World Scientific, 2021. 26–28.

azonosítani a lehetséges támadási pontokat is. A MITRE tanulmányában dokumentált 41 eset 81 támadási pontot azonosít, és bemutatja, hogy ezek nem csak egyetlen pontra irányulnak.

Egy rendszer támadása akkor a leghatékonyabb, ha az életciklusának minél korábbi pontján történik meg. Egy *elemzési fázisban* levő rendszer megismerése információt nyújt az azzal szemben támasztott funkcionális követelményrendszerről, a rendszer céljai mellett az azon kívül eső területeket is definiálja. Már ez a fázis is információt nyújthat a műszaki környezetről. Az elmúlt évben a távmunka térnyerésével sok szervezet alakított ki távoli hozzáférést, a rövid határidők miatt nem mindig szem előtt tartva az információbiztonsági követelményeket. Ez a tény is közrejátszhat a jogosulatlan hozzáférések kockázatának megemelkedésében. Ebben a fázisban 3, *a kockázatok elemzésének és csökkentésének fázisában* már 12 támadás volt érintett.

A mérnöki tervezés és gyártmányfejlesztés a leginkább veszélyeztetett fázis, ebben regisztrálták a legtöbb incidenst, a MITRE kutatásában 28-at. Ebben a szakaszban a támadó célja, hogy kifejlessze és konfigurálja a támadó eszközeit, bejuttassa, és aktiválja azokat a célkörnyezetben. A célpontok közt nemcsak a fő-, hanem az alvállalkozói rendszerek is szerepelnek, a kifinomultabb módszerek a szoftver- és hardverfejlesztőkre irányulnak akár úgy, hogy a köztük folyó információáramlásba ékelődnek be.

A gyártás és telepítés során végzett támadás pontos technikai információkat szolgáltat a támadó számára a már működő rendszerről, erre alapozva további támadóeszközök fejleszthetők ki, és juttathatók tovább. Egy tesztfázisban levő rendszer védelmére sok esetben még kevesebb energiát fordítanak, ami nagyban megkönnyítheti a támadó kódok elrejtését. Ez a fázis 24 támadásban volt érintett.

A működés és támogatás szakaszában működő rendszerek már védett környezetben, a *hardeningeljárásokat* már elvégezve működnek, így azok eredményes kompromittálása már nehezebb feladat. Annak ellenére, hogy ez a fázis az életciklus várhatóan leghosszabb szakasza, a katalógusban csak 22 esetben fordult elő. A SolarWinds rendszerében ezt a szakaszt támadták úgy, hogy a támadó kódot szoftverfrissítéssel juttatták be különböző rendszerekbe. Az akció az ellátási láncon keresztül történő támadás tiszta esete volt, ami világossá teszi a beszállítói informatikai rendszerek kockázatának hatását a rájuk épülő rendszerekre.

A támadók

A kibertámadások megbízóinak, illetve kivitelezőinek rendszerezésére számos forrás tett kísérletet. Ezek az aktorok eltérő motivációkkal és eltérő eszközrendszerrel rendelkeznek, profiljaik ismeretében meghatározhatók motivációik, az általuk alkalmazott technológiák, és kidolgozhatók a megelőzési és védelmi módszerek. A támadók kategóriákba sorolására számos forrást találhatunk,[24] a Hackmageddon[25] adatai alapján korreláció fedezhető fel a támadó csoportba tartozása és a támadás célja közt.

A motivációk azonosításával szintén több forrás foglalkozik, az azonosítás alapjai az ismertté vált incidensek elemzése és az azokból alkotott statisztikák lehetnek. Az informatikai incidensek bejelentési kötelezettsége az Amerikai Egyesült Államokban 2004-re nyúlik vissza, ma már ezek bárki számára elérhetők és tanulmányozhatók. A Hackmageddon havi rendszerességgel készít statisztikákat. Az elmúlt évek motivációit és azok változását mutatja be az 1. táblázat, amelyben a kiberkémkedés és a kiberhadviselés arányának csökkenése mellett a kiberbűnözés egyre magasabb arányban jelenik meg. Az ilyen típusú statisztikák adatai és a tényleges állapot közt valószínűsíthetők eltérések, aminek leggyakoribb oka az esetek egy részének felderítetlensége és a nyilvánosság tájékoztatásának ellenérdekeltsége.

1. táblázat: A kiberbűnözés motivációinak változásai, 2018–2020

Év	Kiberbűnözés	Kiberkémkedés	Hacktivizmus	Kiberhadviselés	Ismeretlen
2018	81,82%	12,86%	2,84%	2,47%	n. a.
2019	83,96%	11,21%	3,05%	1,55%	0,17%
2020	85,17%	9,94%	2,34%	1,83%	0,64%

Forrás: www.hackmageddon.com

Az ellátási láncok támadására itt csak közvetett statisztikák állnak rendelkezésre. A tendenciát azonban jól érzékelteti az Identity Theft Resource Center (ITRC) 2021. első negyedéves adata, amelyben 137 szervezet 27 különböző

[24] Lásd például Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 171.; az Intel pedig publikálta a kiberbűnözés motivációinak személyközpontú referenciatáblázatát, lásd Tim[othy] Casey: Understanding Cyberthreat Motivations to Improve Defense. *Intel White Paper,* 2015. február 16. 8. (Függelék.)

[25] Lásd: www.hackmageddon.com.

beszállítójával kapcsolatban jelzett a kibertérből származó támadást – ez az előző időszak esetszámánál 42%-kal magasabb volt. Bár a MITRE 2017-es jelentésében a kifinomult eljárásokat alkalmazó támadásokat nemzetállamoknak tulajdonítja,[26] felmerül a kérdés, hogy mely szereplők milyen célok érdekében hajtanak végre kifejezetten az ellátási láncokra irányuló támadásokat.

Katonai célú kiberműveletek

A katonai szervezetek és stratégiák a történelem során folyamatos változáson mentek keresztül, hajtómotorjukat a technikai és logikai fejlődés jelentette. A kezdetleges fegyverektől a modern légierőig számos példa igazolta, hogy a modern technikai eszközök nélkülözhetetlenek a katonai műveletek támogatásában, ugyanakkor a harcászati műveletek eredményessége nem csak ettől függ. A saját ellátási lánc fenntartása és az ellenség ellátási láncainak támadása kiemelt szereppel bír a modern hadviselésben, bár maga a módszer egyáltalán nem új. A modern hadviselés viszont már nem jár minden esetben együtt a konfliktus nyílt vállalásával, a jelen háborúi már nem feltétlenül a harcmezőn dőlnek el. Az elmúlt évtizedekben nagyobb szerepet kapott az elrettentés, az USA 2003-ban az iraki háborúban demonstrálta információs fölényének elsöprő hatását. A fejlett országok által vívott hagyományos háborúkat felváltotta a hibrid háború, amely már nem csak katonai szereplők közt zajlik, abban a civil szféra és helyettesítő szervezetek is részt vesznek. Az ellátási lánc támadása reális cél, mert annak fenyegetettsége már önmagában elég lehet ahhoz, hogy a hatalom aktuális gyakorlójával szembeni bizalmat megingassa, és elérje a civil lakosság szembefordulását a hatalommal.[27]

Az ellátási lánc támadásának a hírszerzésben betöltött szerepét aligha kell részletesen bemutatni, az ellenség ellátási folyamatairól, annak tartalmáról, az alkalmazott eszközökről, az utánpótlás útvonaláról, idejéről és tartalmáról szerzett információk képet adhatnak az ellenséges haderők mozgásáról, és kikövetkeztethetők a lehetséges jövőbeni lépések. Ezek ismerete lerövidíti a katonai vezetés döntési ciklusát, és hathatós támogatást nyújt az információs fölény elérésében és megtartásában.

[26] Heinbockel–Laderman–Serrao (2017): i. m. 1–5.

[27] Bodoróczki János: A modern hadviselés logisztikája – a katonai logisztika jövője. *Hadtudomány,* 30. (2020), 2. 98–108.

Az utánpótlási logisztika információinak megszerzése mellett annak lehetőség szerinti befolyásolása, valamint az ellátási lánc működésének meghiúsítása a fejlettebb technikával rendelkező haderőket is vesztes helyzetbe hozhatja. A befolyásolás célja általában a megtévesztés, és ezt kihasználva olyan helyzet kialakítása, amelyben adott szereplő akaratát a szemben álló félre kényszerítheti. Az ellátási lánc támadása, pusztítása már a hadviselés történetének korai szakaszában is fontos stratégiai elem volt, a hadianyag- és az élelmiszer-utánpótlás elvágása számtalanszor bizonyult ütőképes lépésnek. Az ellátási lánc zavaraira a modern logisztika is érzékeny. A modern, hálózati kommunikációra alapozott rendszerek esetében ezek a zavarok a hagyományos támadóeszközök igénybevétele nélkül is előállíthatók.

A hadviselésben a számítógép-hálózatokra alapozott információs műveleti tevékenységek alkalmazása először 1998-ban, az Egyesült Államokban jelent meg, ekkor adták ki JP 3-13 jelzéssel az első összhaderőnemi információs műveleti doktrínát.[28] Az anyag az információs műveleteket támadó és védelmi kategóriákba sorolja, a hangsúlyt a saját információk és információs rendszerek megvédésére helyezi úgy, hogy közben a szemben álló fél információinak megszerzésére és a rendszereinek támadására törekszik. A doktrína megjelenését követően további országok is felismerték a kibertér jelentőségét a műveleti tevékenységekben, így hamarosan Kína és Oroszország is megkezdte ez irányú képességeinek kifejlesztését.[29]

Háború, lövések nélkül

A Supermicro esetéhez hasonló támadás kivitelezésére magányos támadóknak, terroristáknak vagy hackercsoportoknak jelen tudásunk szerint nem volt még lehetőségük. A negyedik generációs hadviselésben ugyan szinte bármely csoport képes lehet érdekeinek érvényesítésére, akár még nemzetállamokkal szemben is úgy, hogy támadásai célpontjául kritikus infrastruktúrákat jelöl ki,[30] erre jelenleg kevés példa van. Ha meg is tudnának egy alaplapra ültethető chipet tervezni, annak gyártása már nehezen lenne titokban tartható, nem beszélve

[28] Joint Publication 3-13, Information Operations. 2012.

[29] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 170.

[30] Deák Veronika (szerk.).: *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 161.

az alaplapok gyártási folyamatába való beavatkozásról vagy a minőségellenőrzés kijátszásáról. Egy ilyen feladat megvalósítására csak olyan szervezet képes, amelynek kapcsolatai minden részterületen érvényesülni tudnak, és ez leginkább az államhatalom esetében áll fenn. De mi motiválja a kibertámadások kivitelezésére alkalmas Supermicro-szerű incidensek kitervelőit ilyen költséges és nagy szervezési feladatot igénylő módszer alkalmazására azért, hogy tartósan rejtett hozzáférést biztosítsanak maguk számára, annak ellenére, hogy idővel szinte biztosan fény derül az incidensre? A történelem során az államok mindig is igyekeztek egymás titkait kifürkészni, és eközben soha nem válogattak különösebben a módszerekben. Nincs ez másképp a modern informatika világában sem, de az ehhez szükséges erőforrások ma szinte kizárólag az államok által támogatott csoportok számára állnak rendelkezésre. Így többségében három általános cél valószínűsíthető: az információszerzés, a befolyásolás és a pusztítás képességének elérése. A titkosszolgálatokhoz köthető incidensek jórészt az első két területet célozzák, míg a pusztítás inkább a nemzetbiztonsági vagy katonai akciók során jelenik meg.

Míg a hadviselés korai szakaszában a fizikai pusztítás volt az elsődleges cél, később az elrettentés is hatékony fegyvernek bizonyult. Az erőfölény nyilvánvalóvá tétele már önmagában képes biztosítani a domináns fél akaratának érvényesülését, ugyanakkor képet ad az azt biztosító környezetről. Az elrettentés a kibertérben is kiválóan alkalmazható eszközzé vált, mivel az informatikai berendezések működésének zavarait a társadalom egy része jól érzékeli, miközben annak lehetséges következményeitől a társadalom egészének tartania kell. Az ellátási láncban keletkezett zavarok hatása a létfontosságú rendszerelemek esetén ennél is továbbmegy, nemcsak az adott szolgáltatás eshet ki, hanem az arra épülő továbbiakban is problémát okozhat. Ez magyarázatot ad arra, hogy egy támadó számára miért nem feltétlenül jelent problémát, ha támadó célú kiberképessége ismertté válik az ellenfél számára. A nyilvánosság előtt természetes az ilyen irányú tevékenység tagadása, de a napvilágra kerülő incidensek minden szereplő számára nyilvánvalóvá teszik a támadó erejét és azt a tényt, hogy ellenséges hírszerzők az informatikai rendszerében szinte bárhol jelen lehetnek. Az APT-támadásokhoz kötődő befolyásolási képesség réme pedig a kibertér legerősebb országait is visszatartja egy kiberkonfliktus nyílt kezdeményezésétől.

A legnagyobb kárt talán az elektromos hálózat sikeres támadásával lehetne előidézni bármely országban; ez szinte a teljes ellátási láncban kifejtené a hatását. Elektromos áram nélkül szinte semmilyen terület nem tudja ellátni feladatát, és más kritikus infrastruktúrákkal szemben a kiesése teljes összeomlást váltana

ki. Az elektromos hálózat elemei ráadásul akár több évtizeddel ezelőtt épültek, régi, elavult technológiát használhatnak, ezért leváltásuk nem triviális feladat, és támadhatóságuk is egyszerűbb. Érdekes, de ez a probléma ráadásul épp a fejlett országokat érinti, hiszen a teljes ország elektromos rendszerének folyamatos korszerűsítése lehetetlen, így szükségszerűen megtalálhatók benne régi, elavult elemek. A hálózat kitettségét szinte minden nemzetállam érzékeli. Az Amerikai Egyesült Államok kitettségét a villamosenergia-rendszer elleni támadásoknak jól jellemzi, hogy Donald Trump egy 2020-as *executive orderben* az ezzel kapcsolatos kockázatok csökkentését írta elő. A rendeletben, amelynek létrejöttét minden bizonnyal titkosszolgálati információkra alapozták, Trump így fogalmaz:

> „[…] megállapítom, hogy a külföldi ellenfelek egyre inkább sebezhető pontokat hoznak létre és használnak ki az Egyesült Államok nagyfeszültségűvillamosenergia-rendszerében, amely biztosítja a nemzeti védelmünket, a létfontosságú vészhelyzeti szolgáltatásokat, a kritikus infrastruktúrát, a gazdaságot és a [mindennapi] életünkhöz szükséges villamos energiát. A nagyfeszültségűvillamosenergia-rendszer célpontja azoknak, akik rosszindulatú cselekményeket akarnak elkövetni az Egyesült Államok és az Egyesült Államok népe ellen, beleértve a rosszindulatú kibertevékenységeket is, mivel a nagyfeszültségűvillamosenergia-rendszerünk elleni sikeres támadás jelentős kockázatot jelentene gazdaságunkra […]”

Az elnök az energiaellátó rendszer fő gyengeségét a nem megbízható forrásból származó rendszerkomponensekkel azonosítja:

> „Megállapítom továbbá, hogy a külföldi ellenfelek tulajdonában lévő, általuk ellenőrzött, illetve joghatóságuk vagy irányításuk alá tartozó személyek által tervezett, fejlesztett, gyártott vagy szállított, az Egyesült Államokban lévő nagyfeszültségű elektromos berendezések korlátlan beszerzése vagy használata növeli a külföldi ellenfelek képességét, hogy potenciálisan katasztrofális következményekkel járó sebezhetőségeket hozzanak létre és használjanak ki a nagyfeszültségű elektromos berendezésekben. Ezért megállapítom, hogy a nagyfeszültségű elektromos berendezések korlátlan külföldi szállítása szokatlan és rendkívüli fenyegetést jelent az Egyesült Államok nemzetbiztonságára.”

A rendelet tiltásokat vezet be az energiaellátó rendszer komponenseinek elemeire:

> „[a tiltás] olyan elektromos hálózati berendezéseket érint, amelyeket olyan személyek terveztek, fejlesztettek, gyártottak vagy szállítottak, amelyek külföldi ellenfél tulajdonában vannak, annak ellenőrzése alatt állnak, annak joghatósága vagy irányítása alá tartoznak […] az Egyesült Államokban lévő nagyfeszültségűvillamosenergia-rendszer tervezése, integritása, gyártása, előállítása, termelése, elosztása, telepítése, üzemeltetése vagy karbantartása elleni szabotázs vagy felforgatás indokolatlan kockázatát hordozza magában.”

Egy 2021-ben megjelent utasítás ennél is tovább megy,[31] és megköveteli a kereskedelmi minisztertől a félvezetőgyártással, a védelmi minisztertől a kritikus ásványi anyagokkal kapcsolatos rizikófaktorok, az egészségügyi minisztertől a gyógyszerek és hatóanyagaik kockázatainak azonosítását és kezelésükre vonatkozó ajánlásokat. A rendelet az energiaügyi, a közlekedési és a mezőgazdasági minisztérium mellett a kereskedelmi és belbiztonsági tárca vezetőit utasítja, hogy

> „[…] a megfelelő ügynökségek vezetőivel konzultálva jelentést nyújtsanak be az információs és kommunikációs technológiai (IKT) ipari bázis kritikus ágazatainak és alágazatainak ellátási láncáról (a kereskedelmi miniszter és a belbiztonsági miniszter által meghatározottak szerint), beleértve az IKT-szoftverek, az adatok és a kapcsolódó szolgáltatások fejlesztésének ipari bázisát."[32]

Az elnöki utasítások tartalmát valószínűsíthetően titkosszolgálati információkra alapozták, és akár korábbi példákra is támaszkodhattak. A támadás nem lenne példa nélküli: Ukrajna elektromosenergia-ellátási hálózatával szemben már hajtottak végre sikeres kibertámadást, amely a feltételezések szerint egy BlackEnergy nevű trójaira volt visszavezethető.[33]

A támadás eszközeinek vizsgálata önmagában is könyvet alkothatna. Szakemberek körében sokszor említett gyenge pont az Internet of Things (IoT) és az olcsó távol-keleti berendezések beépítése kritikus informatikai rendszerekbe. Az IoT-eszközökkel szembeni leggyakoribb kritika a futtatott szoftver ellenőrizhetetlensége és a minimális számítási kapacitásból adódó kriptográfiai eljárások alkalmazhatóságának hiánya. Ezek az eszközök ugyanis rendszerint nem rendelkeznek elég erőforrással ahhoz, hogy erős titkosítási algoritmusokat hajthassanak végre, így védelmük nehézségekbe ütközhet. Az ellenőrizetlen olcsó berendezések üzleti alkalmazása erősen ellenjavallt, mivel nem tudható, hogy azokba a gyártó milyen rejtett funkciókat épített be. Mivel Kína berendezkedése lehetőséget nyújt arra, hogy az állami vezetés bármikor előírja, hogy egy gyártó az érdekeinek megfelelően módosítsa a termék funkcionalitását, ezeket az üzleti szempontból kritikus területeken nem célszerű használni.

Ugyanakkor az ellenőrzési eljárásokat sikeresen teljesítő eszközökben is lehetnek hibák, amelyek jelentős értéket képviselnek, és mivel nem közismertek,

[31] White House: *Executive order EO14017: America's Supply Chains. Executive Office of the President on 03/01/2021.*

[32] White House: *Executive Order on Securing the United States Bulk-Power System* (2020. május).

[33] Robert Lipovsky: Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. *WeLiveSecurity.com*, 2014. szeptember 22.

piaci értékük van, amellyel kereskednek is. A sérülékenységek vásárlói a magas ár következtében általában kormányzati szereplők.[34]

Terrorszervezetek, vallási csoportok

A terrorcselekmények célja rendszerint a lakosság megfélemlítése, a kormányzat rákényszerítése valamilyen intézkedésre vagy egy ország politikai, alkotmányos vagy gazdasági destabilizálása. A legtöbb esetben ezért védtelen civileket támadnak, mivel ennek kivitelezése a legegyszerűbb, és nem is kötődik különösebben a kibertérhez. Bár a terrorszervezetek számára ideális lehetőség lehetne egy szervezet informatikai infrastruktúrájának támadása, eddig elenyésző számban fordultak elő olyan esetek, amikor terrortámadás okozta informatikai üzemzavarral érték volna el az említett célok valamelyikét. Eszközként azonban ez a kör alkalmazza a kibertér szolgáltatásait. Az Európai Unió 2018-as állásfoglalása az alábbi szerint fogalmazza meg a terroristacsoportok és a kibertér kapcsolatát:[35]

> „Mivel számos terrorista csoport és szervezet toborzásra, radikalizálásra és a terrorista propaganda terjesztésére szolgáló olcsó eszközként használja a kiberteret; mivel terrorista csoportok, nem állami szereplők és nemzetközi bűnszövetkezetek arra használják a kiberműveleteket, hogy a névtelenség leple alatt szerezzenek pénzforrásokat, hírszerzési információkat gyűjtsenek és kiberterror-kampányok indításához kiberfegyvereket fejlesszenek ki, kritikus infrastruktúrákat romboljanak szét, tegyenek tönkre vagy semmisítsenek meg, pénzügyi rendszereket támadjanak meg és egyéb illegális tevékenységeket folytassanak, amelyek kihatással járnak az európai polgárok biztonságára nézve."

A magyar kibevédelmi szakemberek szinte egyöntetű véleménye, hogy Magyarország a jelenlegi politikai helyzetben nem célpontja az ellátási láncra irányuló cselekményeknek. Ahogyan a már említett Digitális Mohács szerzői is utalnak rá, feltehetően ennek köszönhető, hogy bár az elektromos távvezetékek, optikai kábelek támadása aránylag sikeresen végrehajtható lenne, mégsem történnek ilyen incidensek. Az egyszerű szolgáltatáskiesések valószínűleg nem segítenék

[34] A közismert Chrome böngésző esetében egy távoli kódfuttatást lehetővé tevő sérülékenység demonstrálása e sorok írásakor 500 000 dollárt ér a Zerodiumnál, lásd: https://zerodium.com/program.html.

[35] Európai Parlament: Az Európai Parlament 2018. június 12-i állásfoglalása a kibervédelemről (2018/2004(INI)). 2018. június 12.

az elkövetőket eléggé a céljaik elérésében, a civil szféra számára okozott kényelmetlenség miatt esetleg épp az elvárttal ellenkező hatást érnének el: a közvélemény ellenük fordulna. Természetesen elképzelhető, hogy előbb-utóbb terroristák által végrehajtott kibertámadás is bekövetkezik, de ahhoz ezeknek a csoportoknak olyan szakmai hátteret kell felépíteniük, amelyhez szükséges anyagi háttér jelenleg valószínűsíthetően nem áll rendelkezésükre.

Rosszindulatú hackerek

Az ellátási láncban a fentiektől eltérő célú kibertámadások is okoztak zavarokat. Az anyagi haszonszerzés érdekében készített támadó szoftverek meghiúsítják az informatikai rendszerek működését. Az elmúlt évek legjellemzőbb eszközei a kriptovírusok különböző változatai voltak, amelyek sikeresen okoztak zavarokat a gazdasági szereplők informatikai rendszereiben. A NotPetya *ransomware*-rel elkövetett támadás által okozott károk hosszan sorolhatók, nem ritkák az olyan üzemzavarok sem, mint a csernobili atomerőmű ipari telephelye automatikus ellenőrző rendszerének ideiglenes leállása. A 2017-ben indított WannaCry legalább 150 országban hozzávetőleg 300 000 számítógép adatait tette elérhetetlenné, és az egészségügyi ellátási láncban is súlyos zavarokat okozott. A legtöbb fertőzést Oroszországban regisztrálták, ahol a legnagyobb vállalatok mellett a Sberbank és különböző minisztériumok számítógépei is áldozatul estek. Más európai országok is nagy károkat szenvedtek, több esetben kórházak is működésképtelenné váltak, így az egészségügyi ellátásban keletkezett zavarok következtében halálesetek is történtek. A *ransomware*-támadások előtt nem voltak ismertek ilyen súlyos következményekkel járó esetek.

Érdekes tény, hogy a WannaCry működése azokon a kiberfegyvereken alapult, amelyeket az NSA fejlesztett ki, és tartalékolt egy esetleges kiberművelet végrehajtásához. Az NSA eljárási rendjében levő hiba következtében a szoftverek a támadókhoz kerültek, majd később a dark neten is megvásárolhatók voltak.

Az ellátási lánc támadása a rosszindulatú hackerek számára a legtöbb esetben anyagi haszonszerzésről szól, valódi céljuk nem az ellátási lánc működésének megzavarása, azt csupán fenyegetésként használják anyagi céljaik eléréséhez. Kiváló lehetőség számukra, hiszen ezzel könnyen rá tudják kényszeríteni áldozataikat arra, hogy fizessenek nekik.

Ellentevékenységek

Az ellátási láncok alkotóelemeinek kifejlesztése és felépítése több ország szervezeteinek összetett hálózatán át történik. Számos elem komplexitása olyan nagy, hogy az hagyományos módszerekkel vagy eszközökkel nem ellenőrizhető. A helyzet kezelését tovább nehezíti, hogy a különféle ellenőrzéseket a rendszerek minden egyes változása esetén újra és újra el kellene végezni. Mivel ennek végrehajtása nagyon költséges lenne, nem zárhatók ki a hibák, a védekezés módszertanában így hangsúlyos szerep jut a kockázatkezelésnek, az ajánlások, jó gyakorlatok és szabványok alkalmazásának. Mivel mindig lesznek olyan pontok, amelyeket egy művelet során ki lehet majd használni, az ellátási lánc ellen indított műveletek időnként sikeresek lesznek, ezt nem lehet elkerülni. A védelem célja ezért a kiemelt fontosságú elemek költségarányos, ugyanakkor minél magasabb szintű védelme, felkészülés a lehetséges kockázatokra és azok szakszerű kezelésére.[36]

A kockázatkezelés elterjedt módszertanában egy esemény kockázatát a bekövetkezés valószínűségének és az okozott kár nagyságának együttesével határozzák meg. Így a gyakran bekövetkező, de kis kárértékű esemény kezelésére hozzávetőleg ugyanakkora erőforrást kell biztosítani. A nagy kárt okozó események azonban rendszerint csak nagy költségű megoldásokkal előzhetők meg, és anyagi források hiányában vagy a költségarányos védelem következtében elmarad a megfelelő eljárások bevezetése.

A termelőkből, alvállalkozókból, szállítókból, kereskedőkből és fogyasztókból álló ellátási láncban a rendszeresen előforduló zavarok kivédésére fordítanak kiemelt figyelmet. A láncok rendszerint hierarchikus szervezésűek, csúcsukon a megrendelő áll. Az elsődleges beszállítók csomópontokat alkotnak, amelyekhez további elemek, az alvállalkozók kapcsolódnak. A csomópontoknak megfelelően integrálódni kell a felettük elhelyezkedő elembe. A struktúrában akár egyetlen láncszem a teljes folyamatra nézve kritikus lehet, mivel a láncok működését ugyanakkor olyan globális beszállítók is befolyásolják, amelyek kiesése katasztrofális hatású, és a keletkező hullámhatás a teljes rendszeren végighalad.

Az ellátási láncok életciklusának tervszerű kialakítása az egyik leghatékonyabb módszer a működési biztonság szintjének emelésére. Ez következetesen összehangolt tevékenységet igényel, amelynek biztosítania kell az életciklus

[36] Supply Chain Attacks, Cybersecurity & Regulations: What to Expect in 2021. *Quointelligence,* 2021. január 27.

minden pontján az átláthatóságot és az ellenőrizhetőséget. Mivel a mai rendszerek fejlesztése már nem egy helyen történik, ezt nehéz teljes egészében elérni.[37] Az Egyesült Államokban az ICT-rendszerek hibáiból eredő kár már 2003-ban meghaladta a 60 milliárd dollárt,[38] így az ezekre épülő szolgáltatások védelmére az ország kockázatkezelési gyakorlati programokat kínál. Az alkalmazhatóság és az érvényesség érdekében ezek a programok célszerűen a korábbi precedenseken alapulnak, és azokat időről időre aktualizálni kell. Az életciklus folyamatainak standardizálására gyakran mintákba foglaló keretrendszerek kidolgozása és közzététele a megoldás.

A MITRE tanulmányában bemutatott, az ellátási lánc támadását célzó esetek elemzésével készült el a *potenciális ellenintézkedések katalógusa,* amely 20 csoportba sorolva foglalja össze az ellátási láncokhoz kapcsolódó intézkedéseket. Ezek részben más ajánlások testreszabott adaptációi, részben kifejezetten ellátásilánc-specifikusak (Reed, Miller és Popick alapján). A katalógus az alábbi védelmi pontok mentén javasolja az ellentevékenységek felépítését.

A *szoftverek biztonságos konfigurációkezelése* a fejlesztési rendszer általános felügyeletét, a hozzáférések ellenőrzését, a rendszer és a termék sértetlenségének, integritásának ellenőrzését, a konfigurációkezelés kritériumainak meghatározását és alkalmazását emeli ki.

A *kritikus komponensek manipulálásának megelőzésére* számos, az adott komponensre kialakított eljárást kell biztosítani. Ebben a legegyszerűbb, de esetenként hatékony módszer a szemrevételezés, amely során pusztán külső nyomok alapján szűrhető ki a manipuláció. Általános szabály a *névtelenség biztosítása,* azaz, amennyiben lehetséges, a potenciális támadók elől el kell fedni a végfelhasználó kilétét. A rendszer komponenseinek *anonim vásárlása* a rendszer kialakításának korai fázisában segít megelőzni a kompromittált változatok bejuttatását. Az egyedi konfigurációk alkalmazásakor az anonimitás már nehezebben biztosítható, így érdemes mérlegelni ennek elkerülését. A *megbízható szállítás* különösen kritikus pont, mert ennek során a biztonsági eljárásokat nem védett környezetben kell érvényesíteni. A jogosulatlan hozzáférés, az adattartalom megismerése, a hamisítás, a csere vagy a módosítás elkerülését fizikai és logikai mechanizmusokon keresztül lehet biztosítani a fejlesztési, az üzembehelyezési

[37] Christopher J. Alberts – Audrey J. Dorofee: *A Framework for Categorizing Key Drivers of Risk*. Carnegie Mellon, 2009.

[38] Michael Newman: Software Errors Cost U.S. Economy $59.5 Billion Annually. *National Institute of Standards and Technology (NIST News Release),* 2002. június 28.

és az üzemeltetési fázisban is. Az ellátási lánc elemeinek javítása, a cserealkatrészek szállítása során célszerű hologramokat, optikai vagy RFID-azonosítókat és egyedi vagy speciális csomagolást alkalmazni. Különös figyelmet érdemes szánni a szoftverkomponensek megváltoztatásának elkerülésére, amelyre szintén számos módszer ismert, de biztonságuk csak az eljárási rend maradéktalan betartásával garantálható. Az *elektromágneses vagy termikus elemzés* lehetőséget nyújt a hardverelemek módosításának detektálására. Valószínűleg egy ilyen vizsgálat mutatta ki a Supermicro alaplapjának módosítását. Az *ellátási lánc átláthatósága* a felhasználó számára biztosítja az abban rejlő kockázatok azonosítását és azok kezelését. *A teljes ellátási láncban vizsgálni kell a komponensek származását,* lehetőség szerint ugyanarra a komponensre *több beszállítóval* is ki kell alakítani a kapcsolatot, és *értékelni kell a kritikus elemek beszállítóinak megbízhatóságát*.

A *biztonságra összpontosító programozási nyelvek alkalmazása* már a tervezési fázisban meghatározható. Ebbe a kategóriába nem csak maguk a programozási nyelvek értendők, idetartoznak a különböző programkönyvtárak, harmadik féltől származó szoftverelemek, futtató környezetek is. A biztonságra nem eléggé összpontosító fejlesztőeszközre az Adobe által 1996-ban kifejlesztett Flash az egyik legismertebb példa, amelyet elsősorban webböngészőkben futó alkalmazások fejlesztésére terveztek. A Flash technológiája szinte teljes élete során biztonsági hibáktól szenvedett, és teljesen ellehetetlenült, miután a legtöbb böngésző letiltotta annak működését.

A *biztonságközpontú tervezési és kódolási szabványok* beépítése és rendszeres felülvizsgálata nemcsak a rendszer rendelkezésre állásának garanciáját teremtheti meg, hanem biztosítja adattárolásának és kommunikációjának bizalmasságát is. Egy rendszer megtervezésekor nem csak annak funkcióira, hanem az üzemelési környezet meghatározására is ki kell térni. Az olyan kritikus rendszerek működését, amelyektől rendkívül magas szintű rendelkezésre állást követelnek meg, nem lehet egyetlen szerverrel megoldani, ehhez több, szétszórtan elhelyezkedő, elosztott működésű kiszolgálóra van szükség. Ennek megvalósítását sokan üzemeltetési feladatnak tekintik, valójában egy ilyen rendszert akkor lehet létrehozni, ha ezt a kritériumot már a tervezési fázisban beépítették. A biztonságos adattárolás legtöbbször kriptográfiai eljárások alkalmazásával valósul meg, de ezek sem örökéletűek, így már a tervezési fázisban érdemes kidolgozni a későbbi cseréjük eljárását.[39] A *hálózati forgalom korlátozásának*

[39] Mary Cindy Ah Kioon – Zhao Shun Wang – Shubra Deb Das: Security Analysis of MD5 algorithm in Password Storage. *ResearchGate, Proceedings of the 2nd International Symposium on*

szabályait a rendszerben megvalósított kommunikációs folyamatok alapján már a tervezési folyamat során dokumentálni kell, és a telepítési és tesztelési fázisban alkalmazni kell.

Red Team és Bug Bounty programok. Sajnos az informatikai rendszerek támadására alkalmazott módszerek mindig is túl változatosak voltak ahhoz, hogy azokat részletesen nyomon lehessen követni. A sérülékenységek technikai tartalmának vizsgálata, azok nyomon követése, a támadó kódok elemzése és az ellentevékenység kidolgozása egy szűk szakmai réteg feladata, amely idővel mindig meghaladja a legjobb szakemberek képességeit is. A sérülékenységek hatalmas száma szinte lehetetlenné teszi a teljes körű védettség kialakítását. A CVE-adatbázis[40] e sorok írásakor 156 019 rekordot tartalmaz, amelyek az egyes szoftvereket, rendszerkomponenseket érintő sérülékenységekről részletes leírást tartalmaznak. A támadók mindig újabb és újabb módszereket találnak majd arra, hogy a rendszerekbe behatoljanak, és ezt valószínűleg nem tudjuk megakadályozni. Az informatikai rendszerek üzemeltetői rendszerint sémák mentén végzik a feladataikat. Frissítéseket és új szoftvereket telepítenek, elvégzik az adatvagyon mentését. A legtöbbjük nem rendelkezik napi ismeretekkel a különböző sérülékenységekről, pusztán az eljárásrendet követve végzi el a feladatát. Egy rendszer biztonságos működtetésében sokat segít, ha az üzemeltetők ismerik azokat a módszereket és eszköztárakat, amelyeket a támadók is használnak, hiszen a legtöbb esetben nem önálló fejlesztést végeznek, csupán meglevő eszközöket alkalmaznak. A sérülékenységek felderítésére érdemes erre a célra fejlesztett célszoftvert használni,[41] és legalább a külvilág számára elérhető gépek esetén elvégezni a *hardeningbeállításokat.*[42] A különböző időszaki jelentések képet adnak az elkövetkező időszak fenyegetettségeinek változásairól, ami alapul szolgálhat a jövőbeni felkészüléshez. A *Red Team* alkalmazása egy fajta megoldást jelenthet a problémák kezelésére. Ez a csoport az ellátási láncot alkotó rendszerre, az annak működését biztosító személyzetre, valamint a felhasználóira irányuló behatolásvizsgálatokat végez, amelyekkel feltárhatók a sérülékenységek, és begyakorolhatók a veszélyhelyzeti eljárások.[43] A *Bug*

Computer, Communication, Control and Automation, 2013.

[40] Lásd: https://cve.mitre.org

[41] Ilyen szoftver a Nessus, amelynek a korlátozott számú számítógép ellenőrzésére szolgáló tesztverziója ingyenesen letölthető: www.tenable.com.

[42] A *hardeningeljárás* a biztonsági beállítások lehetőség szerinti legszigorúbb szintjét jelenti.

[43] Egy Red Team program nem feltétlenül valamiféle bonyolult műszaki megoldás, számos cég teszteli például a munkatársait megtévesztő vagy káros mellékletet tartalmazó levelekkel úgy, hogy

Bounty programok bizonyos keretek közt bárki számára lehetőséget adnak biztonsági hibák felderítésére, és annak jelzése esetén jutalmazzák annak jelzését.

Tartalék eszközök rendelkezésre állása. A tervezés alapvető fontosságú az ellentevékenység végrehajtásában, ez biztosítja az egyes eljárások meghatározását és az ahhoz szükséges erőforrások rendelkezésre állását. A lehetséges zavarok előzetes számbavétele, a kiesésük vagy zavaruk esetében keletkező kár felmérése, a kezelésben részt vevők szerepköreinek definiálása, a szervezet vészhelyzeti működésének meghatározása tudja biztosítani a megfelelő kezelést. A pótalkatrészek JIT-rendszerű rendelkezésre állása lerövidíti az adott komponens által okozott szolgáltatás kiesésének idejét, a bevizsgált raktárkészlet csökkenti a kompromittált komponens beépítését. A katasztrófatervek kidolgozása, azok megismertetése és gyakorlása, valamint az ahhoz szükséges tartalék eszközök rendelkezésre állása helyettesítheti az ellátási lánc kieső elemeit. Tipikus eszközök a szünetmentes tápegységek, az aggregátorok, a tartalék internetkapcsolatok és szerverek, a számítógépek, a hálózati elemek. Az ellátási lánc működőképességének biztosítására további hatékony védelmet nyújt a kritikus pontokon kialakított redundancia. Ez a tartalékokkal szemben a működő rendszerelemek olyan többszörözését jelenti, amelyben a kulcsfeladatok kezelését esetenként akár földrajzilag is elválasztott rendszerelemekre bízzák. A teljes rendszer így képes elviselni összetevői egy részének kiesését. A tartalékok kezelésének megléte, rendszeres frissítése, betartása és annak ellenőrzése szintén alapvető az ellátási láncot támogató informatikai rendszerek működtetése során.

A felhasználók informatikai képzését nem lehet elég alkalommal hangsúlyozni. A kibertámadások még mindig leginkább e-mail-mellékletek vagy megtévesztő weboldalakról letöltött alkalmazások útján válnak aktívvá a kliensszámítógépeken. Az incidens gyakran ilyen jellegű felhasználói hibával indul, és bár egy részük teljesen nyilvánvalóan hamis, adott helyzetben még az üzemeltetők is becsaphatók.[44] A kulcsfelhasználók és üzemeltetők megbízhatóságának sérülése fokozott veszélyforrás, mivel ők a magasabb jogosultsági szintjük következtében a rendszer komponenseinek szélesebb köréhez férnek hozzá, így az általuk szándékosan vagy véletlenül okozott kár mértéke sokkal jelentősebb lehet. A védelmi feladatok ellátásában a felelősség többrétű, és sok esetben

amennyiben a munkatárs arra nem az elvárt módon reagál, oktatási programban kell részt vennie.

[44] Ha például egy munkatárs gyakran fogad csomagküldeményeket, valószínűleg nehezebben tűnik fel számára, ha egy *ransomware*-t tartalmazó levél a megszokott csomagküldő nevében érkezik.

a szakmai vélemények is eltérnek arról, hogy egy incidens bekövetkezésekor végső soron kinek kell a morális felelősséget viselnie.[45]

A célzott támadásokkal szemben már sokkal nehezebb a hatékony védekezés kialakítása. Az átláthatóság érdekében a szervezetek közzéteszik tevékenységüket, referenciáikat, az adott terület vezetőjének, munkatársainak elérhetőségeit, így a nyílt forrású felderítés (*open source intelligence* – OSINT) alkalmazásával nagy mennyiségű információt nyújtanak egy ilyen támadás megalapozásához.

A *szoftverfrissítés biztonsága* a SolarWinds esete óta közismert kockázati tényező a módosított rendszerkomponensek célba juttatására.[46] A nagyvállalatok informatikai szabályzatai a rendelkezésre állás biztosításáért gyakran tiltják a frissítések azonnali telepítését, azok előzetes ellenőrzését írják elő. A magas biztonsági szintet elváró szervezetek egy köre a dobozos szoftverek auditálását is megköveteli, vagy a Common Criteria valamely szintje szerinti megfelelőséget vár el.[47] A *zero-day* sérülékenységek hatásának elkerülése szinte lehetetlen. Ezek alapján kimondható, hogy csak kevés informatikai rendszer képes arra, hogy a teljes életciklusa során incidensmentes legyen. Szabályzati szinten az üzletfolytonossági terv határozza meg az üzemzavar esetén végrehajtandó ellentevékenységek körét. A hatékony adminisztratív védelem kidolgozásának egyik nehézsége az összetett események kezelése és azok másodrendű hatásainak elemzése.

Összefoglalás

Az ellátási láncban keletkezett zavarok minden ország esetében jelentős problémát okoznak, amit számos kormány felismert, és erőforrásokat fordít annak védelmére. Valószínű, hogy a láncok komplexitása tovább növekszik, az internetes lefedettség egyre nagyobb területek számára jelent majd alig érzékelhető támadási lehetőséget. Az 5G hálózatokra alapozott fejlesztési tervek, az önvezető járművek, okosvárosok, okosotthonok kényelme egyre értékesebb támadási pontot nyújt, és egyre inkább növeli a társadalom kitettségét az infrastruktúra és az arra épülő ellátási lánc sérülékenységeinek. A fenyegetettség mértéke

[45] Vélemény: A sírás határán – a WannaCry-probléma. *Hwsw.hu,* 2017. május 16.

[46] FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. *Fireeye.com,* 2020. december 13.

[47] A Common Criteria informatikai biztonsági keretrendszere különféle védelmi profilok mentén garantálja egy szoftver vagy eszköz biztonságos működését.

a társadalom számára alig érezhető, miközben egyes források az ellátási lánc elemei közé már olyan termékeket is besorolnak, mint a Microsoft Office szolgáltatásai. A hadviselés kiterjed a kibertérre is, miközben a kiberképességek fejlesztésére a legnagyobb hangsúlyt fektető országok, Nagy Britannia, Izrael, Kína, Oroszország és az Egyesült Államok saját rendszerei is sérülékenyek. Az ellátási láncok ellen indított kiberműveletek száma bár rendkívül alacsony, egy sikeres támadás közvetett és közvetlen hatásai súlyos kockázati tényezőket jelentenek. Az olyan rendkívüli események, mint a Covid–19, amelynek kezelése során az informatikai rendszerek rutinszerű működését az alkalmi megoldások kényszere váltotta fel, a jövőben is kiváló alkalmat nyújt majd érzékeny célpontok felkutatására és megtámadására, miközben a „láthatatlan ellenség" elleni védekezés fontossága is felértékelődik.

Irodalomjegyzék

Ah Kioon, Mary Cindy – Zhaoshun Wang – Shubra Deb Das: Security Analysis of MD5 algorithm in Password Storage. *ResearchGate, Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation,* 2013.

Alberts, Christopher J. – Audrey J. Dorofee: *A Framework for Categorizing Key Drivers of Risk.* Carnegie Mellon, 2009. Online: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2009_005_001_15104.pdf

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Tanulmánygyűjtemény.* Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673. Online: http://real.mtak.hu/id/eprint/94339

Bodoróczki János: A modern hadviselés logisztikája – a katonai logisztika jövője. *Hadtudomány,* 30. (2020), 2. 98–108. Online: www.mhtt.eu/hadtudomany/2020/2020_2szam/098-108_Bodoroczki.pdf

Bodnár Zsolt: Rizsszemnyi mikrochipekkel hajthatta végre Kína a legnagyobb USA elleni támadást. *Qubit.hu,* 2018. október 5. Online: https://qubit.hu/2018/10/05/rizsszemnyi-mikrochipekkel-hajthatta-vegre-kina-a-legnagyobb-usa-elleni-hackertamadast

Boyens, – Celia Paulsen – Rama Moorthy – Nadya Bartol: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* National Institute of Standards and Technology, 2015. Online: https://doi.org/10.6028/NIST.SP.800-161

Casey, Tim[othy]: Understanding Cyberthreat Motivations to Improve Defense. *Intel White Paper,* 2015. február 16. Online: www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf

Chikán Attila: *Vállalatgazdaságtan*. Budapest, Aula, 2004.

Cserháti András: A Stuxnet vírus és az iráni atomprogram. *Nukleon,* 4. (2011), 1. 1–7. Online: https://nuklearis.hu/sites/default/files/nukleon/Nukleon_4_1_85_Cserhati_.pdf

Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

DeBusk, Steven S.: *What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack.* Fort Leavenworth, School of Advanced Military Studies United States Army Command and General Staff College (First Term AY 02-03), 2003.

DoD Defense Science Board: DSB Task Force Report on Cyber Supply Chain, 2017. Online: www.hsdl.org/?view&did=799509

Európai Parlament: Az Európai Parlament 2018. június 12-i állásfoglalása a kibervédelemről (2018/2004(INI)). 2018. június 12. Online: www.europarl.europa.eu/doceo/document/TA-8-2018-0258_HU.html

FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. *Fireeye.com,* 2020. december 13. Online: https://bit.ly/3yoJq4r

Flying Fraudulently – How a Weak Supply Chain Became the Usaf's Worst Enemy. *Airforce Technology,* 2012. szeptember 24. Online: www.airforce-technology.com/features/featuresupply-chain-us-air-force-fraudulent-parts

Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.

Heinbockel, William J. – Ellen R. Laderman – Gloria J. Serrao: *Supply Chain Attacks and Resiliency Mitigations, Guidance for System Security Engineers*. MITRE, 2017. október. Online: www.mitre.org/sites/default/files/publications/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf

Hippold, Sarah: 5 Trends From the Gartner Hype Cycle for Supply Chain Strategy. *Gartner,* 2020. október 2. Online: www.gartner.com/smarterwithgartner/5-trends-from-the-gartner-hype-cycle-for-supply-chain-strategy-2020.

Joint Publication 3-13, Information Operations, 2012. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Juhász Péter – Száz János – Misik Sándor: Ellátási láncok versenyképessége és finanszírozása – gondolatok az optimumról. *Közgazdasági Szemle,* 56. (2019), 1. 53–71. Online: http://dx.doi.org/10.18414/KSZ.2019.1.53

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7. (2012), 4. 142–151.

Lipovsky, Robert: Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. *WeLiveSecurity.com,* 2014. szeptember 22. Online: www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

Malik, Javvad: *Ethics, Security and Getting the Job Done.* AlienVault, 2015. november. Online: https://cdn-cybersecurity.att.com/docs/whitepapers/rsa-survey-report.pdf

Newman, Michael: Software Errors Cost U.S. Economy $59.5 Billion Annually. *National Institute of Standards and Technology (NIST News Release),* 2002. június 28. Online: www.abeacha.com/NIST_press_release_bugs_cost.html

NIST Computer Security Center: Definitions. Online: https://csrc.nist.gov/glossary/term/ict_supply_chain

Reed, Melinda – John F. Miller – Paul Popick: *Supply Chain Attack Patterns: Framework and Catalog.* Office of the Assistant Secretary of Defense for Research and Engineering, 2014. Online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.6043&rep=rep1&type=pdf

Robertson, Jordan – Michael Riley: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek,* 2018. október 4. Online: www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Schmidt, Andreas: The Estonian Cyberattacks. *Researchgate.net,* 2013. január. Online: www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

Supply Chain Attacks, Cybersecurity & Regulations: What to Expect in 2021. *Quointelligence,* 2021. január 27. Online: https://quointelligence.eu/2021/01/supply-chain-attacks-cybersecurity-regulations-in-2021

Vélemény: A sírás határán – a WannaCry-probléma. *Hwsw.hu,* 2017. május 16. Online: www.hwsw.hu/hirek/57252/microsoft-wannacry-it-biztonsag-kocsis-tamas-balazs-zoltan.html

West, Darrell M.: *Internet Shutdowns Cost Countries $2.4 Billion Last Year.* Center for Technology Innovations at Brookings, 2016. Online: www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

White House: *Executive Order on Securing the United States Bulk-Power System* (2020. május). Online: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

White House: *Executive order EO14017: America's Supply Chains. Executive Office of the President on 03/01/2021.* Online: www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

Yang, Lin – Quan Yu: *Dynamically Enabled Cyber Defense.* H. n., World Scientific, 2021.