SUPPLY CHAIN ATTACK

CTI Jelentés

Ellátásilánc-támadás

(Supply chain attack)

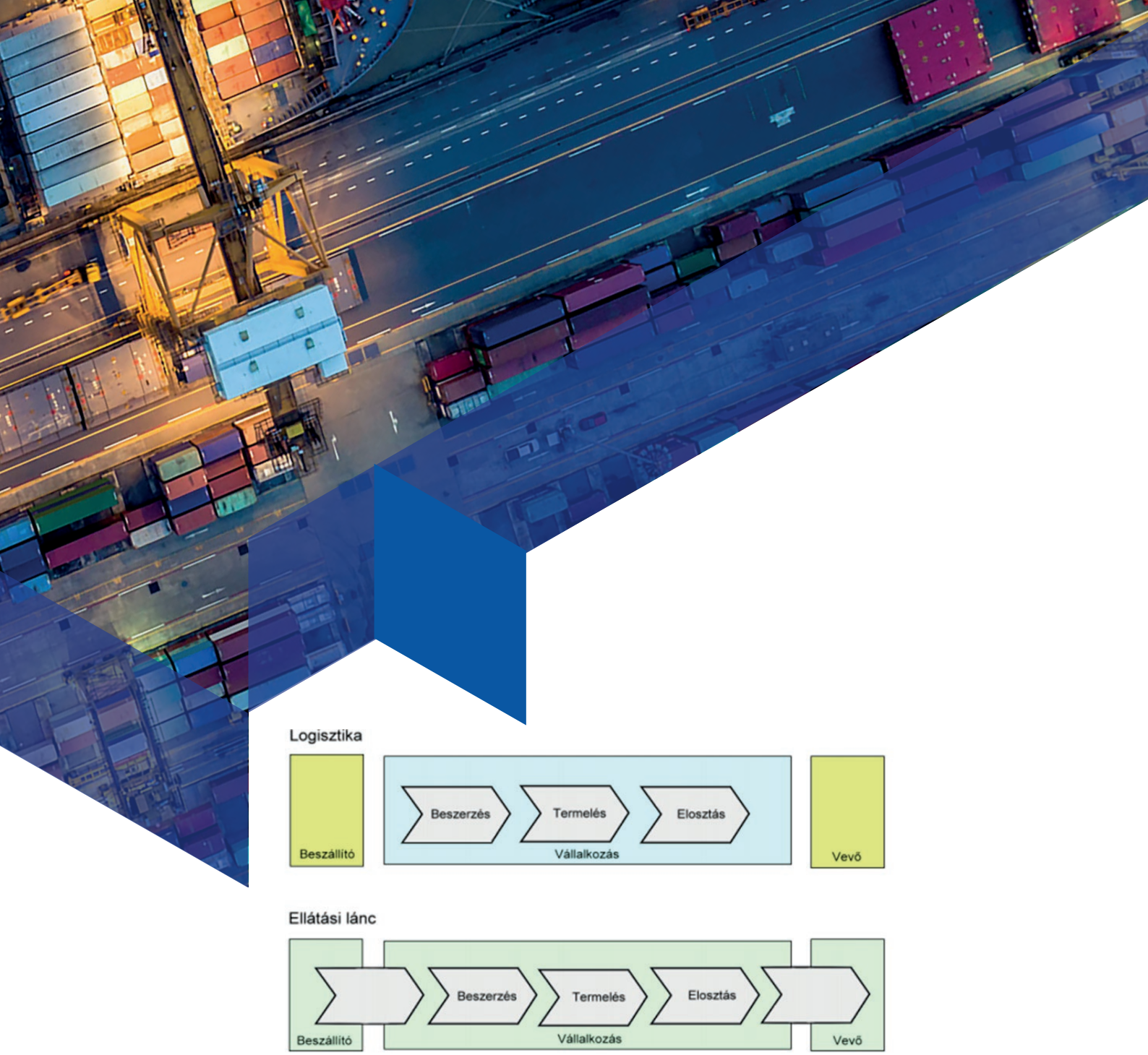
Mi is az ellátási lánc támadás?

Az ellátási lánc folyamata a nyersanyagok kitermelésétől, azok feldolgozásán keresztül, egészen azok végfelhasználóig történő eljuttatásáig tart, beleértve az egyéb, kapcsolódó tevékenységeket és szolgáltatásokat, mint a hulladékkezelés vagy a szerviz.

Ellátási lánc támadásról abban az esetben beszélhetünk, ha egy célszervezetet nem közvetlenül, hanem annak valamely partnerén keresztül (beszállítói partnerek, üzemeltetési partnerek) éri támadás. Nehéz pontos definíciót adni a kifejezésről, mert nem minden esetben lehet pontosan eldönteni, ki is volt a támadás célpontja, vagy milyen célból történt maga a támadás.

A 2021. május 7-i US Colonial Pipeline elleni eseményeknél a támadó (Darkside Group) célja egyértelműen a pénzszerzés volt, azonban nem zárhatóak ki politikai jellegű motivációk az incidensből a szervezet jellegéből adódóan. (A Darkside kelet-európai bűnözői csoport és annak „anya" -csoportja a REvil - az eddigi statisztikai adatok alapján - tipikusan USA-beli célpontokat részesít előnyben a támadásai során.)[1]

1 Forrás:https://www.mcafee.com



1. ábra A logisztika és az ellátási lánc értelmezése[2]

Fontos megemlíteni még a kritikus infrastruktúra kifejezést is, melyet az alábbiak szerint értelmezhetünk: egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtő, a gazdaság működését elősegítő vagy lehetővé tévő azon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége vagy ezek részei, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire negatív hatással jár.

2 A kép forrása: Szegedi Zoltán - Prezenszki József: Logisztika-menedzsment – Kossuth Kiadó,2005

Nemzetközi kritikus infrastruktúra és ellátási lánc elleni támadások

Stuxnet[3]

A jól ismert támadásban maga az iráni elnök beismerte, hogy néhány, az urándúsító programjaikban használt gázcentrifuga működését szabotálták, gyanújuk szerint az eszközöket a Stuxnet féregvírus vette célba. A szakértők szerint a férget, mely 2010 szeptemberében támadta meg a számítógépeket, speciálisan azzal a céllal hozták létre, hogy az urándúsításnál leggyakrabban használt centrifugák motorjait túlterheléssel tönkre tegye.

Supermicro

A Bloomberg által 2018. október 4-én publikált cikk nagy port kavart az Amazon, Apple és az amerikai Védelmi Minisztérium (USDoD) köreiben. Nem kevesebbet állít, mint ezen vállalatok eszközeinek kompromittálódását egy, a gyártó által elrejtett rizsszem méretű chipnek a következtében. Amerikai és brit kormányzati szervezetek támogatásukról biztosították az Amazont, az Apple-t és a Super Micro-t a Bloomberg cikkével szemben, amely azt állítja, hogy több mint 30 amerikai vállalat, valamint amerikai és brit kormányzati szervek után kémkedett a kínai kormány, amely beszállítóként működött közre ezen szervezetek eszközbeszerzéseiben. A témában felszólalt a brit kibervédelmi központ (NCSC) és az amerikai Belbiztonsági Minisztérium (DHS) is.[4] A Bloomberg által publikált cikk teljes egészében itt olvasható.

3 https://nki.gov.hu/figyelmeztetesek/
4 https://nki.gov.hu/it-biztonsag/hirek/

US Colonial Pipeline

A Colonial Pipeline rendelkezik a legnagyobb, közel 9 000 km hosszú üzemanyag-szállító hálózattal az Egyesült Államokban, amely a keleti part üzemanyag-ellátásának 45%-áért felel. A cég közleménye szerint az informatikai rendszereiket ért **zsarolóvírus támadás miatt le kellett állítaniuk a szállítást** a teljes hálózaton. A Bloomberg és a The Wall Street Journal információi szerint a DarkSide ransomware csoport a felelős az incidensért.[5]

Üzemanyaghiányra felhívó tábla a US Colonial Pipeline támadás után egy keleti országrészben található benzinkúton

SolarWinds

Állami – vélhetően **orosz – támogatású hackerek** az utóbbi évek legnagyobb volumenű kiberkémkedési akcióját hajtották végre azzal, hogy **hátsó ajtót (backdoor) telepítettek** – többek közt – egyesült államokbeli hivatalok rendszereibe a SolarWinds cég egyes termékein keresztül. A kivizsgálás jelen szakaszában annyit tudni, hogy a támadás a SolarWinds Orion Platform egy sérülékenységének kihasználásával, az ellátási láncon keresztül történt (supply chain attack): a támadók a backdoort (SUNBURST) egy **hitelesített plug-inba rejtették**, amit frissítésként juttattak a célrendszerekre. A támadási kampány kiterjedtségére vonatkozóan nem érhető el hiteles információ, azonban ismert, hogy a SolarWinds vállalatnak több, mint 300.000 ügyfele van világszerte.[6]

5 https://nki.gov.hu/it-biztonsag/hirek/
6 https://nki.gov.hu/it-biztonsag/hirek

JHB

A brazil JBS Foods a legnagyobb hústermelő vállalatnak számít globálisan, amely a világ számos pontján működtet üzemeket. A vállalat szűkszavú hétfői közleménye szerint a cég egyes ausztrál és észak-amerikai IT rendszereit „célzott kibertámadás érte”, azonban a biztonsági mentési rendszerek nem érintettek, és érzékeny adatok kompromittálódására utaló nyomokat mindeddig nem észleltek. Azincidenshatásajelenlegnemismert,azonbanazesetutániidőszakbantöbb JBS feldolgozó üzem is jelezte, hogy az alapvető karbantartási és készletkezelési feladatokon kívül átmenetileg beszüntetik a működést.[7]

7 https://nki.gov.hu/it-biztonsag/hirek/

Magyar vonatkozás

Több száz magyar ipari vezérlőeszköz az interneten

A https://icsmap.shodan.io/ oldalon az internetre csatlakozó ipari vezérlőeszközök (ICS/SCADA) listáját tették közzé. A nyilvánosságra hozott több mint hetvenezer eszközből körülbelül négyszáz (0,6 %) magyar vonatkozású. Ezen eszközök megfelelő védelem nélkül igen nagy sebezhetőséget jelentenek az adott intézményekre, mivel ezen eszközök szoftverét ritkán vagy egyáltalán nem frissítik, így a nyilvánosságra került sérülékenységek könnyen kihasználhatóak lehetnek.[8]

Adobe adatszivárgás

Mint ahogy arról az NBSZ NKI weboldalán már többször is beszámoltunk, 2013 októbere folyamán sorra derültek ki újabb információk arról, hogy az Adobe cégtől milyen jellegű adatokat tulajdonítottak el a támadók. Szerencsére felhasználói jelszavak nem, csupán titkosított változatuk, illetve a jelszóemlékeztetők kerültek ki a világhálóra, amely tömeges, automatikus támadási lehetőséget ugyan nem tettek lehetővé, azonban egyedi támadások lehetségesek.

8 https://nki.gov.hu/figyelmeztetesek/

Kritikus infrastruktúrák és védelmük Magyarországon

> Az uniós folyamatok alapján egyértelmű volt, hogy a magyar nemzeti programnak meg kell felelnie a kormány és a tulajdonosok, üzemeltetők elvárásainak, miközben biztosítania szükséges az állami közreműködés és a jogi háttér meglétét egyaránt." …" A hazai Zöld Könyv – összhangban az EU Zöld Könyvével – célja, hogy az érintettek részére (állam – tulajdonos/ üzemeltető – felhasználó) biztosítsa azokat az alapvető információkat, definíciókat, elveket és folyamatokat, amelyek a későbbi uniós irányelv értelmezése és megvalósítása során nélkülözhetetlenek.[9]

A Zöld Könyvön kívül a 2013. évi L. törvény és a 41/2015. (VII. 15.) BM rendelet (aminek az értelmezéséhez készített kézikönyv megtalálható az NKI weboldalán) rendelkezik hazánkban a kritikus infrastruktúrák, többek között az állami és önkormányzati szervek elektronikus információbiztonságáról.

Szakmai körökben üdvözölt kezdeményezés a SeConSys, amely „az élvonalbeli magyar villamos energetikai védelmi, irányítástechnikai, kiberbiztonsági, villamosenergia termelő és szolgáltató cégek, szabályozó és felügyeleti szervezetek, valamint energetikai és kiberbiztonsági szakemberek önkéntes, nonprofit szakmai együttműködése.

> Bármely ország, így Magyarország zavartalan működésének egyik előfeltétele a villamosenergia-rendszer – mint" legkritikusabb kritikus infrastruktúra" – felügyeleti és védelmi rendszereinek folyamatos működőképessége. - Forrás: SecSonSys

9 Forrás: KRITIKUS INFRASTRUKTÚRÁK VÉDELME I. Szerkesztette: Bognár Balázs és Bonnyai Tünde, Dialóg Campus Kiadó, Budapest, 2019

A villamosenergetikai kiberbiztonsági kézikönyv aktuális verziója itt található.

Hogyan védekezhetünk az ilyen jellegű támadások ellen?

Mint azt a fenti számos példából láthatjuk, az ellátási lánc és a kritikus infrastruktúrák elleni támadások nem tartoznak a ritka események közé. A Symantec Internet Security Threat Report kiadványa alapján az ellátási lánc elleni támadások mennyisége 78 százalékkal növekedett a 2018-as évben a megelőző időszakhoz képest.[10] Az alábbi, NBSZ NKI által javasolt intézkedések betartásával csökkenthetjük kitettségünket:

- Rendszeres, a kibervédelem fontosságát kihangsúlyozó érzékenyítő oktatás az ágazatok dolgozói részére.
- A kritikus infrastruktúra elemekről elérhető információk korlátozása (need-to-know basis).
- Az infrastruktúra eszközeinek folyamatos frissítése és monitorozása a szükséges mértékben.
- Rendszeres sérülékenységvizsgálat és kockázatelemzés elvégzése. Mivel ezek gyakran meghaladják az üzemeltetési informatikai kapacitást, az NKI külön szolgáltatásként ajánlja ki ezeket a tevékenységeket.
- Javító változtatások bevezetése a fenti vizsgálatok és elemzések alapján.
- Információbiztonsági szabványok megkövetelése a partnerektől (pl. ISO 27001).

10 Forrás: Symantec: Internet Security Threat Report, Volume 24, 2019

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022