Műszaki Katonai Közlöny

XXVII. évfolyam, 2017. 3. szám

Sági Gábor[1]

INFORMATIKAI RENDSZER TÁMADÁSI FOLYAMATA (PROCESS OF INFORMATION SYSTEM ATTACK)

Az információs rendszerek megfelelő szintű védelme elengedhetetlen a társadalom, a gazdaság, a védelmi szektor működése szempontjából. Ugyanakkor az egyre szaporodó sikeres támadások jól mutatják, hogy a jelenleg alkalmazott védelmi megoldások nem, vagy csak korlátozottan működnek.

A szerző művében bemutatja a napjainkban egyre szaporodó fejlett támadások folyamatát, illetve a támadási folyamatok egyes lépéseiben alkalmazható védelmi megoldásokat a támadások felismerésében, illetve a támadások folytatásának megakadályozásában. Bemutatásra kerül továbbá, hogy a jelenleg széles körben elterjedt védelmi megoldások miért nem alkalmasak a fejlett támadások megakadályozására.

Kulcsszavak: *kibertámadás folyamata, behatolás megállítási lánc, fejlett támadás, kibervédelem, kibertámadók*

Adequate protection level of the information systems are essential for the suitable operations in the social, economic and defense sectors. The growing number of successful attacks illustrate that the currently used security solutions have only limited capabilities. The author of the article demonstrates the process of the ever-growing number of advanced attacks and the protection solutions for each individual process steps which are used in recognizing and preventing the chain of the attack. Furthermore, todays widely used protection solutions are introduced and the reason for their limited capabilities in preventing advanced attacks are examined.

Keywords*: process of cyber attack, Intrusion Kill Chain, APT, cyber defense, cyber attacker*

BEVEZETŐ

Manapság a legtöbb információs rendszer vagy információs rendszert használó infrastruktúra közvetve vagy közvetlenül kapcsolódik az internethez, függetlenül attól, hogy társadalmi, gazdasági, védelmi szektorról van-e szó. Ezen rendszereket a szolgáltatásokat igénybe vevő felhasználók és üzemeltetők legtöbbször az interneten vagy internet alapú technológián keresztül érik el.

Az informatikai rendszerek fontosságának, illetve a felhasználók számának jelentős növelése magával hozta az információs rendszerek értékének növekedését, ezzel együtt jelentősen megnövelve a motivációt az információs rendszerek működésének zavarására, az információs rendszerekből történő illetéktelen adatszerzésre, illetve a rendszerekben tárolt adatok manipulálására.

A hatékony információvédelem kialakítását a jelenleg érvényben lévő jogszabályok, szabványok, az egyes védelmi megoldások szükségességét, a védelmi képesség kialakítását kockázatelemzés eredményéhez kötik, figyelembe véve a vélt vagy valós fenyegetettségüket. Ilyen elvek mellett készült a NIST 800-53r4 szabvány [1] és a szabvány felhasználásával

[1] orcid.org/0000-0002-4473-0895; email cím: gabor.sagi@yahoo.com Nemzeti Közszolgálat Egyetem Katonai Műszaki Doktori Iskola 3. éves Phd hallgató

készült hazai szabályozás is, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben [2] meghatározott technológiai, biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. BM. rendelet [3]. Ezen követelmények jellemzően figyelembe veszik a védendő rendszer „értékét", azaz igazodnak az adott szervezet, rendszer veszélyeztetettségéhez. A fokozatosan szigorodó követelmények hivatottak a rendszer olyan szintű védelmének megteremtésére, hogy a támadónak ne legyen érdeke sikeres támadást végrehajtani. A gyakorlatban ez azt jelenti, hogy olyan védelem kerül kialakításra, hogy a támadónak már ne érje meg az adott rendszerbe történő behatolás, ne tudja a rendszerben tárolt adatokat megszerezni, manipulálni, illetve a rendszer működését zavarni, megakadályozni. Ugyanakkor ezen előírások esetén nem jellemző, hogy konkrét műszaki megoldásokat adjanak egy adott információbiztonsági követelmény teljesítésére. Jellemzően meghatározzák azon folyamatokat, minimális paramétereket, amelyek egy adott követelmény megfeleléséhez elegendőek, de a legtöbb esetben nem mondják meg, hogy ezt milyen kontrollokkal kell megvalósítani, mi elegendő a megfeleléshez.

A kockázat alapú megközelítés nem, vagy csak részben veszi figyelembe magát a potenciális támadót vagy támadó csoportot, illetve a támadás motivációját, annak lehetséges folyamatát.

„Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. [1]222 A négy fajta fenyegetési forma más-más motivációt takar, illetve részben más-más eszközrendszert alkalmaz a támadás végrehajtásához. Az egyes támadási formákhoz jellemzően a rendelkezésre álló erőforrások fajtája és elérhetősége is más.

A sikeres támadás végrehajtásához – köszönhetően a már széles körben elterjedt védelmi rendszereknek – sok esetben nem elegendő a szándék, hanem számos egyéb feltétel megléte szükséges:

- erős motiváció,
- a támadás komplexitásától függően idő,
- megfelelő szaktudás a támadás kivitelezésére,
- a támadott rendszer hibája, gyenge védelmi képessége, illetve
- anyagi forrás, amennyiben nem áll rendelkezésre a fenti feltételek közül valamelyik.

Ahhoz, hogy hatékony védelmi rendszert tudjunk kialakítani, mindenképpen figyelembe kell venni a támadó motivációját, a támadás végrehajtásához várhatóan használt eszközöket, illetve a rendelkezésére álló erőforrásokat.

MOTIVÁCIÓ

Egy támadás megindításának a legfontosabb feltétele, hogy meglegyen a kellő motiváció a támadóban, az informatikai rendszer kompromittálására. A motiváció forrása lehet valamiféle meggyőződés (akár politikai, vallási, személyes), politikai vagy egyszerűen csak gazdasági, pénzszerzési jellegű. Amennyiben az elérendő vélt vagy valós morális, politikai, gazdasági

haszon meghaladja a befektetett erőforrásokat, úgy nagy valószínűséggel az informatikai rendszer támadása sikeres lesz.
A támadás sikerességének másik alapfeltétele, hogy álljon rendelkezésre elegendő erőforrás. A védelem kialakításakor célszerű a potenciális támadó lehetőségét, mint fontos paraméter is figyelembe venni. A potenciális támadó erőforrásainak ismerete lehetőséget biztosít arra, hogy a rendszer védelmének kialakítása kockázatarányosan történjen meg.
A különféle szakirodalomban [5][6][7] számos csoportosítási lehetőséget találhatunk, a támadás szempontjából véleményem szerint a támadó képességei, erőforrásai és annak rendelkezésre állása alapján öt csoportot célszerű megkülönböztetni:

- **Kevés tudással, kevés erőforrással rendelkező támadó** (piti bűnöző, scriptkidi): fő jellemzője, hogy a támadáshoz használt technikát nem saját maga dolgozza ki, hanem kész megoldásokat alkalmaz, ismert sérülékenységeket próbál kihasználni, új hiányosságok feltárására nem képes, olyan sérülékenység kereső alkalmazásokat használ, amelyek bárki számára elérhetőek és néhány óra alatt megtalálják azon rendszereket, ahol egy általa ismert sérülékenységet ki tud használni. Jellemzően kis hatékonysággal és kevés károkozással dolgozik. Megfelelő védelmi megoldásokkal alkalmazásával (pl.: hálózati védelmi eszközök, vírusvédelem), az alapvető biztonsági szabályok betartásával (pl. patch management, hozzáférés szabályozás) a támadás sikerességének esélye jelentősen csökken. Jellemzően nagy „zajjal”, tevékenységük után számos nyomot hagyva tevékenykednek, ami nagy segítséget nyújthat egy esetleges incidens vizsgálat során.
- A **különböző társadalmi csoportok** is egyre gyakrabban használják céljaik eléréséhez az információs rendszerek támadását. A támadások általában jól szervezettek egy adott cél vagy célcsoport ellen irányulnak. A konkrét támadási (pl.: szolgáltatás megtagadásos támadások, weboldal módosítások) tevékenységet általában a nagyszámú szimpatizáns végzi, a központi irányító utasításainak megfelelően. Jellemzően a támadók egy közösség részeként (pl. Anonymous, nemzet szimpatizánsai) végzik tevékenységüket. A cél inkább a figyelem felhívás, mint a komoly károkozás. Megfelelően konfigurált védelmi eszközök hatékony védelmet nyújthatnak a támadóval szemben.
- **Nagy szaktudással, de kevés erőforrással rendelkező támadó** jellemzően civil munkája mellett végzi tevékenységét, elsősorban saját szakmai tudásának megmutatására. A tevékenység irányulhat a rendszerek hiányosságainak felderítésére, a hiányosság javításának kikényszerítésére, de irányulhat a támadott rendszer kompromittálására is. Különösen nagy kockázatot jelent egy vállalat számára az elbocsájtott munkavállaló, aki vélt vagy valós sérelme miatt akar bosszút állni. Mivel a támadónak olyan ismeretei vannak a rendszerrel kapcsolatban, amely a védelem számára nem ismert, így a kialakított védelem sokszor nem elég hatékony.
- A tervezett támadás által elért haszon nagysága határozza meg a **szervezett bűnözői csoportok** által - racionalitáson alapuló - felhasznált erőforrások nagyságát, azaz a várható haszon reményében történik a támadáshoz szükséges erőforrás biztosítása. A támadáshoz szükséges tudás rendelkezésre állhat a támadó csoport tagjaitól, illetve pénzügyi lehetőségek birtokában lehetőség van akár káros kódok vásárlására, vagy

DDoS kapacitás bérlésére is. Amennyiben a rendelkezésre álló erőforrások jelentősek, úgy a támadó képes fejlett (APT2 jellegű) támadást végrehajtani, ami ellen a jelenleg széles körben elterjedt védelmi megoldások nem nyújtanak védelmet.

- Információbiztonsági szempontból talán a legnehezebb az **állam által támogatott** (state sponsored) támadások elleni védekezés, mivel a támadó szinte „korlátlan" erőforrással rendelkezik, legyen szó szolgáltatás megtagadás jellegű vagy új generációs fejlett (APT jellegű) támadásról. A támadó számára általában ismertek az informatikai eszközöket gyártó vállalatoktól szerzett/kapott, a termékre vonatkozó információk, rendelkezhetnek egyéb (pl.: hírszerzői) forrásokból számos információval, amely a támadás sikeres végrehajtásához elengedhetetlenek. Ugyanakkor – néhány eset kivételével - szerencsére „bár az országok képesek egymás elektronikus információs rendszereire pusztító hatású csapást mérni, de mivel ismerik saját sérülékenységüket és a potenciális ellenfelek képességeit, ezzel a fegyverrel inkább nem élnek." [1]

A védelmek kialakítás szempontjából a kiberterroristákat az állam által támogatott szervezetek csoportjába sorolnám, azzal a megjegyzéssel, hogy a rendelkezésükre álló információk és erőforrások szűkösebbek, de az elérni kíván cél azonos.
Az egyes csoportok között sokszor nem húzható éles határ, illetve sokszor csak sejthető, hogy egy támadás mögött milyen csoport is húzódik meg (pl. észt-orosz konfliktus, Stuxtnet).

TÁMADÁSOK KATEGORIZÁLÁSA

A védekezés során elsődleges fontosságú felmérni a lehetséges veszélyforrásokat, a támadók által alkalmazott módszereket. A támadási módszerek több szempontból is csoportosíthatók.
Az elérni kíván cél szempontjából egy számítógépes hálózat elleni támadást alapvetően három fő kategóriába sorolhatunk:

- „Sérülés (corruption), vagyis az informatikai rendszerben található adatokat a támadónak sikerül megváltoztatnia, vagy törölnie.
- Szivárgás (leakage), amikor a támadónak olyan adatokat sikerül megszereznie, amihez nem szabadna hozzáférnie.
- Megtagadás (denial), a megtámadott rendszer működése lehetetlenné válik. A besorolás nem foglalkozik azzal, hogy a támadónak milyen módszerrel sikerült elérnie, csak a céllal magával [8]

A rendszer kompromittálódása szempontjából további csoportosítási lehetőség, hogy a támadó átveszi-e az információs rendszer, vagy annak egy része feletti uralmat vagy sem:

2 APT (Advanced Persistent Threat): "Informatikai rendszerekbe észrevétlenül, célzott módon, adatszerzés és/vagy rombolás céljából bejuttatott különleges képességű folyamatok, melyek külső kapcsolat segítségével, távolról kiadott vezérlőparancsok végrehajtásával folyamatosan működve fejtik ki jogszerűtlen tevékenységüket" [12]

- Kompromittálódott a rendszer: A támadó a rendszerben tárolt információhoz hozzáfért, a rendszer működését az informatikai rendszer módosításával zavarja, vagy működésképtelenné teszi
- Hozzáférés nélkül vált a rendszer korlátozottan vagy teljesen működésképtelenné. A támadó a rendszer vagy annak egyes elemeit a rendszer módosítása nélkül, külső úgynevezett szolgáltatásmegtagadással járó támadást (Denial of Service vagy DoS) vagy elosztott szolgáltatásmegtagadással járó támadást (Distributed Denial of Service vagy DDoS) hajt végre. Ezen támadások jellemzően rövid ideig (néhány perctől, néhány napig tartanak), és intenzitásuk nagy mértékben függ a támadás végrehajtójától.

A védekezés megtervezése szempontjából kritikus pont, hogy a védendő rendszert fel kell-e készíteni olyan támadásokra, amelyeket a hagyományos védelmi megoldások nem tudnak elhárítani.

- hagyományos támadásnak tekintjük a támadást, amennyiben a rendelkezésre álló védelmi megoldások (tűzfalak, proxy-k, behatolás detektáló és megelőző (IDPS) vírusvédelmi rendszer) – megfelelő beállítás, használat esetén - képesek a támadást felismerni és hatékonyan megakadályozni a támadót céljainak elérésében,
- új generációs vagy folyamatosan fennálló fejlett (APT) támadások jellemzője, hogy a hagyományos védelmi rendszerek nem vagy csak igen korlátozottan képesek a támadás észlelésre, beavatkozásra. A támadás kifinomult, és olyan eszközöket alkalmaz, amelyekre nincsenek felkészítve a széles körben alkalmazott védelmi megoldások. További jellemzője ezen támadásoknak, hogy a káros tevékenység, hónapokig, évekig rejtve marad, maradhat.

ÚJ GENERÁCIÓS TÁMADÁS FOLYAMATA ÉS LEHETSÉGES VÉDEKEZÉSI MÓDOK

A hagyományos támadási formákról és a támadások elleni védekezésről számos tudományos mű született [9][10]**Hiba! A hivatkozási forrás nem található.**[12], amelyek részletesen elemzik a támadás módját, lefolyását, legyen szó káros kóddal elkövetett támadásról, vagy szolgáltatás megtagadáson alapuló támadásról.
Az új generációs támadások végrehajtásáról a hazai [13] és nemzetközi [14] irodalomban is találhatunk részletes információkat, ugyanakkor magáról a támadás fázisairól, az esetleges megelőzési lehetőségről a magyar nyelvű irodalom hiányos, annak ellenére, hogy a nemzetközi szak és tudományos irodalomban számos megközelítési lehetőség került publikálásra.
A behatolás jellegű támadás modellezésére számos megközelítés létezik (Cyber Attack Thread, Mandiant attack life cycle, Lockheed Martin Intrusion Kill Chain) és nincs mindenki által elfogadott modell [15]. A modellek megalkotásának célja minden esetben az volt, hogy a támadási folyamat olyan elemi részekre kerüljön felbontásra, amelyek lehetőséget biztosítanak a támadás részletes feltérképezésére és a védelem kialakításra.
Ugyanakkor megítélésem szerint a Lockheed Martin által publikált „Intrusion Kill Chain" [16] folyamat nyújt a legtöbb segítséget a hatékony információvédelem kialakításában.

1. ábra: Intrusion Kill Chain (Készítette: a szerző)

Felderítés (Reconnaissance)

A felderítés során a támadó megpróbál minél több információt szerezni a kiszemelt célpont által használt informatikai infrastruktúráról, a vállalat munkavállalóitól, hogy megkeresse azon gyenge humán és technikai pontokat, amelyek segítséget nyújtanak a támadás sikeres kivitelezésében. Az információszerzésnek számos csatornája lehet, nyilvános forrástól, akár egy dolgozó zsarolásáig.

Amennyiben a támadó a vállalati infrastruktúrán kívüli csatornákat használt (hírszerzési csatornák, keresőmotorok, újságok, tematikus portálok, hírportálok, közösségi média stb.), akkor a felderítésnek a vállalat által használt eszközökben nincs nyoma, így a védekezésre is csak korlátozott lehetőség van.

A nyilvános hírforrásokból történő felderítést egészítheti ki a vállalati hálózat megismerése, a nyilvánosan elérhető szolgáltatások és azok gyenge pontjainak feltérképezése. A feltérképezésnek része lehet a tűzfalakon nyitott portok és a mögöttük lévő szolgáltatások megismerése, a reakcióképesség, reakció idő tesztelése. A feltérképezésre általában a támadó az interneten szabadon elérhető eszközöket használ, és csak kisebb arányban van szükség és lehetőség manuális tevékenységre. Amikor a támadó a vállalati infrastruktúrát használja információszerzésre, akkor a támadásnak már vannak nyomai, ugyanakkor ezekből a nyomokból - néhány specifikus eset kivételével, pl.: portscan, ismert támadó cím - általában nem könnyű következtetni a támadás előkészületére, viszont ezen információk az utólagos vizsgálatban segítséget nyújthatnak.

Mivel a megszerzett információk jelentős része a vállalat munkavállalóitól származik pl.: közösségi média, social engineering) különösen fontos, hogy a munkavállalók ne osszanak meg olyan információkat, amelyből következtetni lehet a vállalti infrastruktúrára, esetleges zsarolási lehetőségre, illetve ismerjék fel az esetleges információszerzési tevékenységet.

A hálózat feltérképezése ellen hatékony védelmet tudnak nyújtani a hálózati védelmi eszközök (tűzfalak, hálózati behatolást detektáló és megelőző rendszerek – NIDS[3]/NIPS[4] - rendszerek), a honeypotok segíthetnek továbbá a támadási módszer felderítésében is. Ugyanakkor az általánosan elvárt biztonsági folyamatok működtetésével (pl.: patch management, megfelelő eszközkonfigurálás) jelentősen csökkenthető a feltérképezés eredményessége.

[3] NIDS: Network Intrusion Detection System: hálózati behatolás detektáló rendszer
[4] NIPS: Network Intrusion Prevention System: hálózati behatolást megakadályozó rendszer

Felfegyverzés (Weaponization)

A célpont informatikai rendszerének feltérképezése és a rendszerek, munkavállalók gyenge pontjainak megtalálása utáni lépés olyan káros kód (exploit) készítése, szerzése, összekapcsolása egy állománnyal, amit a célponton várhatóan valaki meg fog nyitni, emberi tevékenység nélkül képes lefutni vagy olyan weboldal készítése, amit a célponton valaki meg fog nézni.
A fertőzött csomag (payload) jellemzően Adobe Portable Document Format (PDF) vagy Microsoft Office formátumú, de minden olyan formátum elképzelhető, amely az állomány megnyitásával – egy sérülékenység kihasználásával - lehetőséget biztosít kód futtatására. A káros kód hordozó állományba történő beépítésére az interneten szabadon elérhető célszoftverek vannak.
A fertőző weboldalak általában hasonlítanak a célpont által látogatott oldalak valamelyikéhez, csak az oldal elérése tér el az eredeti oldaltól vagy olyan tartalmat tartalmaz, ami a célszemély számára érdekes, hívogató (pl.: kecsegtető nyeremény, szakmai oldal).
Ebben a fázisban a támadónak nincs kapcsolata a céllal, így ebben a fázisban nincs konkrét védekezési lehetőség. Nem célzott védekezést jelent a sérülékenység adatbázisok, szaksajtó figyelése, és felkészülés az új támadási technikákra.
Számos szakirodalomban azonban – és az Cyber Kill Chain eredeti dokumentációjában is – ebben a fázisban is vannak lehetséges védelmi megoldások (pl.: hálózati behatolás detektáló és megelőző rendszer alkalmazása), a tevékenység voltából adódóan a felkészülés segíthet a támadás további fázisainak megállításában.

Szállítás (Delivery)

A támadás ezen fázisában a támadó által elkészített fertőzött csomag bejuttatása történik a cél rendszerbe. A káros kód eljuttatásának három leggyakoribb módszere továbbra is az email (phishing, spear phishing), fertőzött weboldal, illetve a fertőzött reklám (malvertising). [17] Ugyanakkor célzott támadás esetén a hordozható adathordozón keresztüli fertőzés is gyakran alkalmazott módszer (például vélhetően a Stuxnet esetében).
Amennyiben a káros kód már tartalmaz a védelmi rendszerek (hálózati behatolás detektáló, megelőző – IDPS, vírusvédelmi rendszerek, spam szűrő) számára ismert kódrészletet vagy a támadás valamely paraméterét, akkor a csomag nem fogja tudni elérni a célját, nem fog a rendszerben lefutni. Amennyiben a káros kód a védelmi rendszerek számára nem ismert, úgy a hagyományos védelmi megoldások nem képesek a kód bejutását megakadályozni. A felhasználó által felismert fertőzött állományt tartalmazó levél törlésével, az ismeretlen forrásból származó adathordozók megtekintésének mellőzésével megelőzhető, hogy a támadás tovább folytatódjon.

Kihasználás (Exploitation)

A káros csomag bejutása után valamilyen trigger kiváltja a káros kód lefuttatását. A kód lefuttatásához általában valamely alkalmazás vagy az operációs rendszer sérülékenysége szükséges. A trigger lehet egy felhasználói tevékenység vagy a rendszer egyik sérülékeny elemének támadásával automatikus. Manuális tevékenység egy fertőzött dokumentum

megnyitása, fertőzött honlap meglátogatása, vagy egy fertőzött adathordozó számítógéphez csatlakoztatása USB porton keresztül, minden, ami kiváltja a káros kód lefuttatását.
A támadás ebben a fázisban megállítható a rendszerre telepített biztonsági frissítésekkel, végponti védelem (végponti behatolás védelem, vírusvédelem, stb.) kialakításával és naprakészen tartásával.
Amennyiben a védelmi rendszerek nem voltak képesek a támadás megállítására, akkor a felhasználói tudatosítás segíthet a védelemben (például a nem várt levélben lévő csatolmány, a levélben kapott hivatkozás megnyitásának mellőzésével).

Település (Installation)

A káros kód lefutásával a támadó egy trójai programot vagy hátsó bejáratot (backdoor) telepít, amely felhasználásával a támadónak lehetősége van a távoli kapcsolat állandó, folyamatos fenntartására a támadott környezetből. A telepítés során a számítógépen olyan műveletek hajtódnak végre, amelyek végrehajtását megakadályozhatják a vírusvédelmi, vagy végpont védelmi rendszerek vagy olyan alkalmazások, beállítások, amelyek nem engedik alkalmazások telepítését.

Vezérlés és irányítás (Command and Control - C2)

A Település fázisban kialakított csatornán keresztül kommunikál a fertőzött számítógép, illetve a támadó speciális célú számítógépe. A C2 szerver a támadó által felügyelt, a fertőzött számítógépek vezérlésére és ellenőrzésére használt számítógép. C2 szerver alkalmazásával lehet nagy mennyiségű számítógéppel (botnet hálózat) DDoS támadást is végrehajtani, illetve fejlett támadás esetén a fertőzött gépen egyedi utasítást végrehajtatni. A C2 szerverrel történő kommunikációnak számos jele van a fertőzött infrastruktúrában, így a támadás típusától, a rendelkezésre álló védelmi megoldásoktól függően nagyobb lehetőség van a detektálásra (hálózati behatolás detektáló eszköz), beavatkozásra (tűzfal, hálózati behatolás megelőző eszköz).

Tevékenység (Actions on objectives)

Amennyiben az előző fázisokban felsorolt tevékenységek sikerrel jártak, a támadási szándék nem került feltárásra, a támadás nem került blokkolásra, akkor a támadó elérte eredeti célját, azaz lehetősége van titkos csatornán keresztül adatszivárogtatásra, a támadott rendszer vagy az rendszerben tárolt adatok illetéktelen módosítására, törlésére, rendelkezésre állásának zavarására. Mivel a támadó már az informatikai rendszeren belül van, így lehetősége van a fertőzött rendszert további rendszerek felé történő támadásra felhasználni.
Amennyiben az első hat lépés egyikében sem sikerült a támadást felismerni, megállítani, úgy a káros tevékenység várhatóan hosszú időn keresztül folytatódhat. A támadás felismerése célzott vizsgálattal, új védelmi technológia bevezetésével, vagy hasonló támadás elemzését követően, a támadásra jellemző paraméterek megosztása után lehetséges. Azonban így sem ritka olyan kártevő felfedezése, amely éveken keresztül ott volt egy adott rendszerben.

TÁMADÁS MEGELŐZÉSE

Az elmúlt időszakban nagy nyilvánosságot kapott incidensek kapcsán látható, hogy a támadások egyre kifinomultabbak, a védekezés egyre nehezebbé válik. Több szakértő szerint már nem az a kérdés, hogy az általunk felügyelt informatikai rendszer kompromittálható-e, hanem az, ha még nem kompromittálódott, akkor mikor fog [18].
Mivel a támadások jelentős része még mindig az emberi hiszékenységet, alacsony információbiztonsági tudatosságot, tudást használja ki, ezért egyre jelentősebb szerep jut a tudatosításra, a felhasználók felkészítésére a támadás jeleinek felismerésére. A tudatosításnak a Felderítés, illetve a Kihasználás fázisában van kiemelkedő szerepe, a dolgozóknak meg kell tanítani, hogy milyen információt, mikor és kivel oszthatnak meg, illetve fel kell tudniuk ismerni a rajtuk keresztül végrehajtott támadásokat.
A felhasználó tudatosítása mellett nagyon fontos, hogy a szabványokban, jogszabályokban meghatározott információbiztonsági folyamatok – elsősorban patch menedzsment, változáskezelés - működjenek, a védelemre hivatott eszközök konfigurációja megfelelő legyen.

TÁMADÁS FELISMERÉSE

A fejlett támadások elhárításának első lépése, hogy az informatikai rendszer támadását a védelemre hivatott rendszerek (hálózati detektáló, végponti védelmi, vírusvédelmi, naplóelemző rendszerek) vagy a támadott személyek észleljék és az észlelés eljusson az arra hivatott személyzet részére.
A támadás észlelésére szinte valamennyi fázisban van lehetőség. A védelmi rendszerek által történő felismerés ugyanakkor nagymértékben függ az egyes fázisokban használt védelmi eszközök képességétől, lehetőségeitől.
A hagyományos védelmi megoldások úgynevezett szignatúra alapú elemzést végeznek, amelynek lényege, hogy az adott védelmi rendszer csak azt a kódot, viselkedés mintát ismeri fel, mint támadás, amely korábban „meg lett tanítva” a rendszernek.
Amennyiben a védelmi rendszer része működő naplóelemző megoldás, úgy az egyes védelmi rendszerek által beküldött riasztások, illetve különböző eszközökből beküldött esemény bejegyzések (logok) is lehetőséget biztosítanak összetettebb támadás felismerésére is.
A működés mechanizmusból fakadóan a szignatúra vizsgálat alapú megoldások nem képesek a fejlett támadások tevékenységeinek észlelésére, mivel ezen támadások alatt jellemzően olyan kódokat, viselkedés mintákat használnak, amelyek ezen rendszerek számára nem ismertek, így a támadás sem kerül felismerésre. Nem egyedi, de célzott támadás felismerését segítheti olyan forrásokhoz (cyber threat intelligence center) történő csatlakozás, amelyek megosztják a támadóról, a támadás módjáról azon stratégia, taktikai, műveleti, technikai [19] információkat, amelyek szükségesek a támadás felismeréshez.
Egyedi vagy korábban még nem elemzett támadás esetén a viselkedés anomália alapú (behavior based anomaly detection) elemzés jelenthet megoldást. Manapság már elérhetőek azok a hálózati, illetve végponti védelmet biztosító megoldások, amelyek képesek a korábban nem ismert viselkedés kockázatainak felmérésére és a szükséges riasztás leadására. (Pl.: anomális alapú IDS/IPS rendszerek) Fontos azonban, hogy jól definiált esetek kivételével

ezen rendszerek csak valószínűsíthetik a támadást, de biztosat nem tudnak jelezni, a támadás tényének megállapításához emberi közreműködés szükséges.
Számos vállalkozás számára – a védelmi megoldások jelentős költsége miatt – a felhő, mint biztonsági szolgáltatás (Security, as a Service - SaaS) igénybevétele jelenthet megoldás. Ebben az esetben a szolgáltató adja a védelmi megoldást, legyen szó vírusvédelemről, webes alkalmazás sérülékenység-vizsgálatról, hálózati sérülékenység menedzsmentről, DDoS támadás menedzsmentről, fájl integritás monitorozásról, tűzfal és megfelelőség menedzsmentről, változáskezelésről [20]. A felhő másik felhasználási területe a káros kód tevékenységének elemzése úgynevezett sandbox-ban, kihasználva a jelentős számítási kapacitást.
Várhatóan a következő nagy áttörést a Big Data megoldások elterjedése fogja jelenteni az információvédelem területén, hasonlóan ahhoz, ahogy a gazdaság egyéb ágazataihoz. Ez az irány azért is elkerülhetetlen, mivel az egyre szaporodó védelmi megoldások, az üzleti alkalmazások olyan mennyiségű esemény bejegyzést keletkeztetnek, amelyek hagyományos technológián, hagyományos algoritmusokkal már nem dolgozhatók fel hatékonyan.
A viselkedési anomália alapú rendszerek, illetve a Big Data alapú megoldások sikerességének egyik kulcs tényezője a rendszerek tanulási képességeinek (gépi tanulás) hatékony megvalósítása. [21] A viselkedés alapú rendszer esetében nagy mennyiségű adat felhasználásával, nagy hatékonysággal, a lehető legrövidebb időn belül kell megállapítani a korábbi viselkedés minták alapján, hogy az „újdonság” biztonsági eseményt jelent-e, mivel a túl sok valótlan jelzés feldolgozása olyan mértékű erőforrást igényel, hogy a vállalat vélhetően nem tud tolerálni, illetve a jelzés elmulasztása sem kívánatos esemény. Ugyanakkor a két új technológia ötvözése olyan lehetőséget biztosít az eddig rejtett összefüggések megtalálására, amelyek komplexitásuk, időbeni elhúzódásuk miatt korábban nem volt lehetséges, biztosítva, hogy a rendszerekben ne történjen nemkívánt tevékenység.

ÖSSZEGZÉS

Az informatikai rendszereink védelme kulcsfontosságúvá vált a mindennapi élet szinte valamennyi területén. Ugyanakkor nap, mint nap tapasztalható, hogy a rendszerek nem képesek ellenállni sokszor a leggyengébb támadásoknak sem. Ennek oka a nem átgondolt tervezés, üzemeltetés. Számos megközelítés létezik a hatékony védelem kialakítására, ugyanakkor gyakorlati szempontból az egyik leghatékonyabb a Lockheed Martin által publikált Intrusion Kill Chain, amely segítségével a behatolás fázisain keresztül lehet kialakítani a megfelelő védelmet. A hatékony védelem kialakításának – a teljes folyamat lefedésén kívül - azonban vannak egyéb követelményei is. Ilyen követelmény, hogy a nem ismert káros kód, viselkedés se maradjon rejtve, kerüljenek feltárásra azon összefüggések, amelyekből következtetni lehet a támadásra. Az elmúlt időszak tapasztalatai azt mutatják, hogy a jelenlegi megoldások nem nyújtanak megfelelő védelmet és emiatt a védelem kialakításában is új technológiák alkalmazása szükséges. A fejlett támadások elleni védekezésben várhatóan a viselkedési anomália vizsgálata, a gépi tanulás, a Big Data, a felhő technológia, illetve ezek kombinációja fog hathatós segítséget nyújtani.

FELHASZNÁLT IRODALOM

[1] NIST Special Publication 800-53A Revision 4:Assessing Security and Privacy Controls in Federal Information Systems and Organizations Url: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf 2016.10.11.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[3] 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

[4] Krasznai Csaba: A polgárok védelme egy kiberkonfliktusban. Hadmérnök VII. Évfolyam 4. szám - 2012. december Url: http://hadmernok.hu/2012_4_krasznay.pdf 2016.08.20.

[5] Elméleti alapok és tudományos kutatási módszerek Szerkesztette: Nemeslaki András Url: http://real.mtak.hu/33733/1/E_kozszolgfejlesztes-nemeslaki.pdf

[6] Cynthia Fitch :Crime and Punishment: The Psychology of Hacking in the New Millennium Url: https://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795 2016.08.20.

[7] Larisa April Long: Profiling Hackers Url: https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 2016.08.20.

[8] GYÁNYI SÁNDOR: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem Url: http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf 2016.08.20.

[9] Leitold Ferenc: Biztonsági Technológiák Alkalmazása Url: http://vtki.uni-nke.hu/uploads/media_items/biztonsagi-technologiak-alkalmazasa.original.pdf 2016.08.21.

[10] Haig Zsolt, Kovács László: KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK Url: http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf 2015.12.20.

[11] Muha Lajos: A kritikus információs infrastruktúrák védelme, Budapest: Reinet Technológia Kft, 2015. 158 p. ISBN:978-963-12-4434-2

[12] Gyebrovszki Tamás: Folyamatos fenyegetések a kibertérben. Hadmérnök IX. Évfolyam 3. szám - 2014. szeptember Url: http://hadmernok.hu/143_10_gyebrovszkit.pdf 2016.08.20.

[13] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van I-II. Hadmérnök V. Évfolyam 4. szám - 2010. december és VI. Évfolyam 1. szám - 2011. március Url: http://hadmernok.hu/2010_4_kovacs_sipos.pdf 2015.12.20.

[14] A “Kill Chain” Analysis of the 2013 Target Data Breach. MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER MARCH 26, 2014 Url: https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf 2016.08.21.

[15] Koustav Sadhukhan , Rao Arvind Mallari, Tarun Yadav: Cyber Attack Thread: A Control-flow Based Approach to Deconstruct and Mitigate Cyber Threats Url: https://arxiv.org/pdf/1606.03182v1.pdf 2016.08.20.

[16] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains Url: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf 2016.08.20.

[17] Symantec: Internet Security Threat Report 2014 Url: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf 2016.08.21.

[18] Joseph Muniz, Gary McIntyre, Nadhem AlFardan: Security Operations Center: Building, Operating, and Maintaining your SOC CISCO PRESS 2016.

[19] Integrating Threat Intelligence Defining an Intelligence Driven Cyber Security Strategy Url: http://www.cpni.gov.uk/Documents/Publications/2015/11-jUNE-2015-CONTEXT_CPNI_Threat_Intelligence_FINAL.pdf 2016.08.21.

[20] Póser Valéria, Schubert Tamás, Kozlovszky Miklós, Prém Dániel: SECURITY ON-DEMAND MEGOLDÁSOK AZ INFORMATIKAI INFRASTRUKTÚRÁKBAN Hadmérnök VIII. Évfolyam 3. szám - 2013. szeptember

[21] Eszter Katalin BOGNÁR: Data Mining in Cyber Threat Analysis – Neural Networks for Intrusion Detection AARMS 2016. évfolyam 2. szám Url: http://uni-nke.hu/uploads/media_items/aarms-2016-2-bognar.original.pdf 2016.10.11.