KRASZNAY CSABA

Adatok és automatizáció a kiberbiztonság szemszögéből

Absztrakt

A 2020-as évek kezdetén a negyedik ipari forradalom zajlik éppen, és talán észre sem vesszük, hogy a digitális technológia átalakítja a mindennapi életünket. A hétköznapi ember ezeket a változásokat leginkább úgy érzékelheti, hogy egyre több okostelefont, okosórát, okosvillanykörtét használ, miközben a háttérben az ipar, a termelés, a közművek, általánosságban az egész gazdaság is egyre jobban függ ezektől a hálózatba kötött eszközöktől, az általuk generált adatoktól és mesterséges intelligencia által támogatott automatizációtól. Ez a függés pedig komoly kitettséget jelent a kibertéri fenyegetésekkel kapcsolatban. Jelen tanulmány célja bemutatni, hogyan hatnak a kiberbiztonsági kihívások napjaink társadalmára és bemutatni, milyen módon jelenik meg az adat és az automatizálás a támadók és a védelem oldalán.
Kulcsszavak: kiberbiztonság, automatizáció, adat, negyedik ipari forradalom

Abstract

In the early 2020s, the Fourth Industrial Revolution is underway, and we may not even realize that digital technology is transforming our daily lives. Ordinary people can best perceive these changes by using more and more smartphones, smartwatches, smart light bulbs, while in the background industry, production, utilities, and the economy as a whole are increasingly dependent on these networked devices, the data and automation supported by artificial intelligence. Meanwhile, this dependence is a serious exposure to cyber threats. The goal of this study is to show how cybersecurity challenges affect today's society and to show how data and automation appear on the side of attackers and defense.

Keywords: cybersecurity, automation, data, Fourth Industrial Revolution

Bevezetés

Számos helyen írták már le azt, hogy a 21. század az adatok évszázada, illetve azt, hogy az adat az új olaj. Valójában az adatkapitalizmus jelensége a negyedik ipari forradalom egyik leglátványosabb jele, mely ugyan a szemünk előtt zajlik, mégis igen keveset tudunk róla. Maga a fogalom sokak szerint Klaus Schwab nevéhez kötődik, aki az alábbi meghatározást használta:

„Mint ahogy az első ipari forradalom gőzzel működtetett gyárai, a másodiknál a tömeggyártás tudományának alkalmazása, továbbá a harmadik ipari forradalom során a digitalizáció elkezdése, addig a negyedik ipari forradalom olyan technológiái, mint a mesterséges intelligencia, a genomszerkesztés, a kiterjesztett valóság, a robotika és a 3D nyomtatás, gyorsan megváltoztatják azokat a folyamatokat és módszereket, ahogy az emberiség az értékeket létrehozza, cseréli és elosztja. Ahogy az az előző forradalmak során is történt, ez a változás is mélyen átalakítja az intézményeket, iparágakat és a magánszemélyeket is. Ennél is fontosabb azt észrevenni, hogy ezt a forradalmat az emberek ma meghozott döntései vezérlik. A világ 50–100 év múlva nagymértékben függ majd attól, hogy hogyan gondolkodunk ma ezekről a befektetésekről, és hogyan vezetjük be ezeket az erőteljes új technológiákat."[1]

Nagy Judit több szerző meghatározása alapján a következő szintézist alkotta a fogalomra:

„A negyedik ipari forradalom alapja a digitalizáció és az adat, a számítógép csupán eszköz. Az internet és a technológia fejlődése megteremti az emberek, gépek és vállalatok folyamatos összeköttetésben lévő hálózatát, és az értékteremtő folyamatok adatainak folyamatos megosztásával elérhetővé válik a versenyképes, a vevő számára teljesen testreszabott termék előállítása. A versenyelőny forrása tehát nem csupán az összehangolt, vagy éppen teljesen új alapokra helyezett termelés (pl. additív termelés) lesz, hanem a termékek digitális szolgáltatásokkal való körbeágyazása, valamint, hogy melyik vállalat hogyan válogatja ki a keletkező adatokból a releváns információt a döntéshozatal támogatásához."[2]

Bármelyik definíciót nézzük is, az egyértelmű, hogy a gazdaság függ a digitális adatoktól, azok pedig függenek az őket létrehozó, továbbító és feldolgozó informatikai infrastruktúrától. Az informatika és a függés szavak megjelenése egy mondatban pedig azonnal indokolttá teszi azt a kérdést, hogy vajon mekkora is ez a kitettség, mi határozza meg annak mértékét és mit lehet tenni annak érdekében, hogy az esetleges negatív hatások ne okozzanak helyrehozhatatlan károkat egy szervezet, egy nemzet, egy nemzetközösség vagy egy teljes civilizáció életében? Mivel

[1] Schwab 2021.
[2] Nagy 2019.

a káros hatások jellemzően az informatika oldaláról érkeznek és a valós életben okoznak kárt, ezeket kiber-fizikai hatásoknak nevezzük, kezelésük pedig a kiberbiztonság feladata, amely a 2013. évi L. törvény meghatározása szerint

„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez".[3]

Fontosabb kibertéri kihívások

Ha nagyon le akarjuk egyszerűsíteni a kibertéri fenyegetést jelentő aktorok körét, akkor négy fontosabb típussal kell számolnunk: a kiberbűnözői csoportokkal, a kiberkémekkel, a kiberterroristákkal és a kiberhadviselést művelő haderőnemekkel. A kiberbűnözői csoportok célja az informatikai erőforrások bármilyen jellegű monetizálása, a lehető legnagyobb anyagi haszon megszerzése. A kiberkémkedéssel foglalkozó állami hírszerző és magánbiztonsági cégek feladatkörébe a digitálisan tárolt szervezeti és magántitkok kifürkészése tartozik. A kiberterrorizmus olyan bűncselekmény, amelyet számítógépek és távközlési eszközök felhasználásával követnek el, és amely erőszakot, pusztítást és/vagy a szolgáltatások megszakítását eredményezi, azért, hogy zavart és bizonytalanságot okozzanak a lakosságban, ezáltal pedig befolyásolják a kormányt vagy a lakosságot egy adott politikai, társadalmi vagy ideológiai menetrendhez való alkalmazkodásra. A kiberhadviselés az egyes államok katonai szervezetei által végrehajtott kibertéri műveletek összessége, mely más államokkal szemben történik, a végrehajtó állam stratégiai érdekeinek mentén. Ezen aktorok mindegyike jelentős fenyegetést jelent a negyedik ipari forradalom alapját jelentő adatokra és infrastruktúrákra.[4]

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[4] Berki 2018.

A kibertéri kihívások nem újkeletűek. A kiberbűnözés elleni első jogszabály már 1984-ben megszületett az Egyesült Államokban. Az első hacktivista jellegű megmozdulások, melyeket elkövetési módjuk miatt leginkább a kiberterrorizmussal lehet rokonságba állítani, az 1990-es évek első felében kaptak szárnyra. Az államok egymással szembeni kiberkémkedési tevékenységét is az 1990-es évek közepére lehet visszavezetni. A kiberhadviselés témájában pedig 1998-ban történt az első felszólalás az ENSZ-ben, Oroszország részéről. A folyamatosan evolválódó műveletek 2010 körül kerültek látványosan a közvélemény elé, például a 2007-ben Észtországgal szemben elkövetett, Oroszországból induló kibertámadással, a feltételezhetően az Egyesült Államok és Izrael által végrehajtott *Stuxnet,* hivatalos nevén *Operation Olympic Games* művelettel, melynek célpontja az iráni nukleáris program volt, vagy éppen az Edward Snowden által kiszivárogtatott amerikai titkosszolgálati megfigyelési programokkal. 2021-ben mindezen műveletek már a mindennapok részei, a felhasznált eszközök, technikák és eljárások azonban elképesztően változatosak, szervezeti szinten gyakorlatilag lehetetlenné téve a kielégítő műszaki védelem megteremtését.

Az Európai Kiberbiztonsági Ügynökség (*European Union Agency for Cybersecurity* – ENISA) minden évben kiadja azt a jelentését, mely bemutatja a legfontosabb kibertéri fenyegetéseket.[5] A 2021-es kiadvány hűen tükrözi azt a reménytelen állapotot, mellyel a szervezeti biztonságnak szembesülnie kell. A következő bekezdésekben ennek a kiadványnak legfontosabb megállapításai kerülnek összefoglalásra, a szerző kommentárjaival. A főbb trendek közül elsőként a zsarolóvírusokat emeli ki a kutatás. Röviden összefoglalva, a zsarolóvírus célja eredetileg egy szervezet informatikai infrastruktúrájának megfertőzése, az azokon található digitális adatok titkosítása, majd váltságdíj követelése a dekódoláshoz szükséges kulcs kiadásáért cserébe. A hosszú éveken át működő *modus operandi* azonban jelentősen megváltozott. A célpontok ma már az egyéni felhasználók helyett a milliárd dolláros bevételű cégek, nem egyszer kritikus infrastruktúrák. A fertőzés során nemcsak titkosítás történik, hanem ezeket az adatokat el is lopják a szervezetektől, így az áldozat eldöntheti, hogy a nem működő infrastruktúra vagy az ellopott adatok visszaszerzé-

[5] ENISA 2021

séért fizet. Mivel egy szervezet működésétől más szervezetek működése is függhet, ma már előfordul, hogy nem is a megfertőzött céget zsarolják, hanem azt, amelyik az előbbitől függ. Maga a támadás pedig olyan szofisztikált, amit korábban csak titkosszolgálatoktól lehetett látni. Ráadásul a legnagyobb bűnözői csoportok „partnerprogramokat" hirdetnek, aminek a lényege, hogy a támadó-infrastruktúrát bármelyik kisebb, helyi bűnszervezet felhasználhatja, a sikeres támadás utáni részesedés fejében. Sőt, nyíltan keresnek olyan belső embereket a legnagyobb vállalatoknál, akik a támadókódokat be tudják juttatni a belső hálózatokba, ezzel kikerülve a legtöbb védelmi intézkedést, természetesen busás fizetség fejében. A közeljövőben pedig az is várható, hogy a támadás során megszerzett hatalmas mennyiségű adatot a mesterséges intelligencia segítségével elemzik, mely lehetővé teszi további, célzott támadások végrehajtását.

Természetesen a zsarolóvírusok mellett számos más kártékony kód is létezik, ezek jelenléte sem csökkent. Míg a zsarolóvírusok ma már főleg a nagyvállalatokat célozzák, az egyéb károkozók a kibertér minden szereplőjének kellemetlenséget okozhatnak. A cél minden esetben a közvetlen vagy közvetett haszonszerzés. Egy kémprogram által megszerzett bankkártyaadat vagy internetbanki hozzáférés triviális példa a közvetlen anyagi haszonszerzésre, de ma már minden hozzáférés monetizálható. A teljesség igénye nélkül, például egy ellopott közösségi média fiókon keresztül kéretlen reklámokat lehet terjeszteni. Egy lakásban felszerelt, internetre kötött okoskamerához való hozzáférést a kukkolásra vágyóknak lehet eladni. A védtelen okoseszközöket pedig olyan hálózatokba, úgynevezett botnetekbe lehet szervezni, melyekről túlterheléses támadások indíthatók. Összességében tehát minden erőforrás, azaz a hardverek számítási és tárolási képessége, az internethozzáférés, a felhasználói fiókok és minden digitális adat érdekes lehet és pénzzé tehető a feketepiacon.

Modern korunk egyik érdekes tünete, hogy a társadalom egy része pénzügyi értéket lát a kriptovalutában, amely tulajdonképpen nem más, mint egy bonyolult matematikai művelet eredménye, és ebbe valódi, a nemzetközi pénzügyi rendszer által elismert valutát hajlandó befektetni. Ez a pilótajátékszerű gondolkodás természetesen akár a mindennapi pénzügyi tranzakcióink részévé is válhat, ahogy az államok és a nemzetközi közösség érvényesíteni tudja azokat a szabályozásokat, amelyek célja a pénzügyi biztonság garantálása, a megfelelő kontroll kialakítása az állampolgárok védelme érdekében. Ez a centralizáció egyébként homlok-

egyenest szembe megy a kriptovaluták eredeti koncepciójával, az állami felügyeletet megkerülő decentralizációval. Kriptovalutát kétféleképp lehet szerezni: vásárlással és bányászattal. Ez utóbbi számos kriptográfiai számítás végrehajtását jelenti egy számítógép processzorában. Leghatékonyabb formája az, ha az egyébként igen nagy energiafelhasználású videókártyák grafikus processzorában hajtják végre a számításokat. A kriptobányászat-mánia eredménye az, hogy a piacon nehezen lehet hozzájutni a videókártyákhoz, illetve a kriptovaluta-bányászat globális energiafelhasználása megegyezik egy kisebb országéval. Bűnözői nézőpontból azonban kriptovalutát szerezni vagy lopással vagy mások számítógépén való bányászattal a leginkább érdemes. A kártékony kódok egy része éppen ezért a megfertőzött eszközöket vagy bányászatra használja, vagy direkt módon, az azon tárolt kriptovaluták kifosztására optimalizálták őket. Az igazán nagy játékosok a kriptovaluta-kereskedelmet lebonyolító tőzsdék kifosztására szakosodtak. Mások egyszerű csalás útján próbálják rávenni a kriptoőrülettől megrészegült átlagfelhasználókat, hogy fektessenek be, de valójában csak a pénzüket csalják ki ezzel. Talán ez az a bűncselekménytípus, amely a legjobban mutatja be, mi vár ránk a negyedik ipari forradalom során. Az emberiség létrehoz egy kibertéri megoldást egy korábban nem létező problémára, amellyel viszont igen komoly társadalmi kihívást indít el a valós, fizikai térben, amelyre minden korábbinál gyorsabban kell reagálnia a védelemért felelős nemzeti és nemzetközi intézményrendszernek.

A legtöbb kibertámadás első lépése azonban még mindig jellemzően egy e-mail elküldése, mely vagy tartalmazza azt a kártevőt, melynek segítségével akár a zsarolóvírus, akár más típusú kártékony kód el tudja kezdeni pusztító hatását, vagy ráveszi az áldozatot egy olyan cselekményre, amely utat nyit a támadónak. Ezt az e-mailt pedig valakinek meg kell nyitnia, akit az úgynevezett pszichológiai manipuláció, angol kifejezéssel *social engineering* módszerével vesznek rá a veszélyes cselekményre. Első lépésben ki kell választani a megfelelő áldozatot. A közösségi média világában nagyon könnyen megtalálható és kiismerhető az a személy, aki az adott szervezetnél a megfelelő célpont lesz. Ezután fel kell vele venni a kapcsolatot egy olyan üzenettel, amely biztosan érdekes lesz neki. Például egy személyzeti ügyekkel foglalkozó munkatárs nagy valószínűséggel megnyit egy PDF formátumú önéletrajzot, egy pénzügyekkel foglalkozó kolléga pedig egy olyan levelet, amiben az állítólagos üzleti partner értesí-

ti a bankszámlaszám megváltozásáról. Arról nem is beszélve, hogy bárki, aki egy közműszolgáltató ügyfele, valószínűleg meg fogja nézni a látszólag a szolgáltatótól érkező e-mailt, melyben állítólagos számlatartozásról értesítenek, illetve az, aki mesés gyógyulást vár a Covid19 betegségből, bele fog tekinteni az ezt ígérő kéretlen reklámüzenetbe. Napjainkban ráadásul ezeket a támadásokat kiegészítik telefonon vagy hagyományos levélben érkező üzenetekkel is, hogy még hihetőbb legyen a támadás. A műszaki oldalról történő védelem nehézségét mutatja, hogy az elektronikus levelek szűrésére évtizedes technikák vannak, mégis az e-mailen keresztüli visszaélés bekerült a legfenyegetőbb 2021-es trendek közé.

A támadások egyik elsődleges célja tehát minél több adat megszerzése. Az adat az információ alapja, így az elkövetői gondolkodás szerint, mivel az „adat nem kér enni", azaz a nagy mennyiségű adat tárolása ma már igazából nem akadály, az a jó, ha egy-egy művelet során minden kinyerhető digitális adat megszerzésre kerül. Ezt a trendet ugyanúgy fel lehet fedezni a kiberbűnözésben, mint a kiberkémkedésben, és bizonyítékát lehet látni abban, hogy a Darkneten, az „internet sötét oldalán" hatalmas adatbázisokat kínálnak eladásra. A megszerzett adatok között vannak olyan „örökzöldek", mint a személyes adatok, a szellemi tulajdon vagy a felhasználói fiókok hozzáférési adatai, de szezonális jellegűek is, mint például a Covid19-hez kapcsolódó kutatási adatok. Aggasztó trend, hogy az állami hátterű támadások során olyan megoldásokat használnak a nagy mennyiségű adat megszerzéséhez, amelyekre lehetetlen felkészülni. Így nem nagyon lehet arra készülni, hogy a kínai és amerikai gyártóknak és digitális szolgáltatóknak bizonyos mértékben együttműködési kötelezettségük van országuk hatóságaival, tehát az általuk kezelt digitális adatokhoz az állami hatóságok elméletileg úgy férhetnek hozzá, hogy a keletkeztetés, tárolás és feldolgozás költségeit gyakorlatilag a szolgáltatóknak kell viselniük a normál üzletmenetük keretében. De hasonló mintákat lehet Oroszországban is észlelni, ahol a nemzeti szabályozás kimondottan agresszívan követeli meg a digitális szolgáltatók együttműködését, még akkor is, ha azok nem helyi vállalatok.

A támadások egy másik célpontja a digitális infrastruktúra. A zsarolóvírusokról már szót ejtettünk, ez jelenleg a szervezetek egyik legnagyobb kiberellensége világszerte. De emellett megjelentek a váltságdíjat követelő túlterheléses támadások is (*Distributed Denial of Service* – DDoS). Ez a feltörekvő fenyegetés újabb példát ad arra, hogyan alkalmazkodnak

a kiberbűnözők az áldozatok informatikai infrastruktúrájához és kibervédelméhez. A zsaroló céllal indított DDoS támadás valójában nem egyfajta új támadás, az elmúlt évtizedekben láthattunk már ilyen incidenseket. Általában sok nem legitim, internet felől érkező lekérdezéssel kezdődnek, különböző forrásokból, melyeket egy e-mail követ, amelyben a támadó jelentős összeget kér a tevékenység leállításáért cserébe. Korábban egy ilyen támadás pusztító volt, mivel a digitális szolgáltatás leállt, és nem volt valódi védelem ellene. Aztán megjelentek a felhőalapú terheléselosztók, melyek még a legkisebb cégek számára is jó megoldást tudtak nyújtani.

De a DDoS visszatért. Először is, úgy tűnik, hogy a támadók új botnet-típussal rendelkeznek. Miközben egy korábbi, Mirai néven ismert botnet még mindig fertőzi az okoseszközöket, jelenleg egy chip-sérülékenységét kihasználva, megjelent a Meris nevű kártékony kód is, mely egy széles körben használt hálózati eszköz, úgynevezett útválasztó (router) sérülékenységét célozza meg. Az útválasztókból felállított botnet sokkal hatékonyabb, mint egy meglehetősen gyenge hardverrel rendelkező okoseszköz-hálózat. Másodszor, a támadási módszertan is megváltozott. Amint arról jelentősebb gyártók beszámoltak, az átlagos DDoS mindössze 1-2 óráig tart jelenleg. Ezalatt a rövid idő alatt a működés megszakadhat, de hatékony ellenintézkedéseket nem lehet végrehajtani. Mivel a támadás előtt sok cég kapott egy e-mailt, melyben váltságdíjat követeltek, elképzelhető, hogy a támadók megpróbálták bebizonyítani, hogy komolyak a szándékaik. Harmadszor, az áldozatok nem kizárólag a hagyományos célpontok közül kerülnek ki. A megtámadott szervezetek között vannak online játékplatformok, médiaszolgáltatók, politikai csoportok is. Negyedszer, a támadók jól felkészültek a célpontra. Jól látható, hogy a bűnözői csoportoknál is megjelenik az államilag támogatott csoportok tudása, ahogy az a zsarolóvírusoknál is látszódik. Ötödik új irányzatként pedig meg kell említeni a célzás változását. Ha egy DDoS egy adott eszközt céloz meg az IT infrastruktúrában, az eredmény sokkal hatékonyabb támadás. Ez a speciális eszköz manapság a „biztonsági doboz". Pontosabban, a támadások a kliens és a szerver között elhelyezkedő biztonsági eszközöket (úgynevezett *middlebox*okat) célozzák meg – tűzfalakat, terheléselosztókat, hálózati címfordítókat (*Network Address Translation* – NAT), mély csomagvizsgáló (*Deep Packet Inspection* – DPI) eszközöket.

Egészen újszerű fenyegetést jelent az információs műveletek mindennaposság válása a kibertérben. A jobbára katonai tevékenységként ismert

művelettípus, amelynek körébe tartozik a dezinformáció, az álhírek jelensége is, ma már nem kizárólag a kiberhadviselés eszköztárát színesíti, hanem más állami és nem állami aktorok is előszeretettel használják azt. Különösen általánossá a Covid19 kapcsán vált a jelenség, amikor is számos véleményvezér a vakcinaellenes kinyilatkoztatásokat saját gazdasági haszonszerzése érdekében tette meg, hiszen minél nagyobb a pánik, annál több embernek tudják eladni a megelőzést segítő saját „csodaszereiket". Az álhírek terjesztésének fő platformja a közösségi média, ezen belül pedig nagy segítség az álprofilok automatizált létrehozása, ezeken keresztül pedig szintén az automatizmusok által terjesztett dezinformáció már könnyen célba tud érni. A támadások végrehajtói ezen a területen vetették be elsők között a mesterséges intelligencia adta lehetőségeket, hiszen egyre gyakrabban lehet találkozni az úgynevezett *deep fake* jelenségével, amely olyan audió- és videótartalmakat jelent, amelyeket a gép hoz létre valós személyek korábbi tartalmai alapján úgy, hogy az esemény a valóságban nem történt meg. Ezeket a hamisított videókat például a kriptovalutás átveréseknél használják. A korábban csak titkosszolgálatok által használt technikákat újabban bizonyos marketingcégek is használják, teljesen természetessé vált, hogy például politikai vagy kereskedelmi kampányokat építenek fel a dezinformáció, álhírterjesztés módszerével.

A támadók tevékenységét nagyban megkönnyíti az a technológiai átállás, ami a negyedik ipari forradalom kapcsán megfigyelhető. A folyamat leegyszerűsítve az, hogy az infrastruktúra egyre több okoseszközt tartalmaz, amelyek hálózaton keresztül továbbítják a digitális adatokat a felhőbe, ahol a mesterséges intelligencia feldolgozza azokat, amiből vagy automatikus döntések vagy döntéselőkészítés születik. Mind a dolgok internetét (*Internet of Things* – IoT) alkotó eszközöket, mind a hálózatokat, mind a felhőerőforrásokat, mind az algoritmusokat üzemeltetni kell, ami számosságuk és komplexitásuk miatt törvényszerűen magában hordozza a hiba lehetőségét. Az emberi hiba mellett tehát jellemzően üzemeltetési hibák, nem megfelelő konfigurációk szerepelnek a támadások elsődleges okai között. Köszönhető ez annak is, hogy a Covid19 miatti digitalizáció túl gyorsan érte a szervezeteket, melyek egyszerűen nem tudták megtervezni a megfelelő átállást és nem tudták a kellő szakértelmet biztosítani az üzemeltetéshez. Eközben százezrek, milliók élnek meg abból, hogy hibákat keresnek a rendszerekben és az általuk fellelt sebezhetőségek nem feltétlenül csatornázódnak be a gyártókhoz, fejlesztőkhöz, hogy azok ki-

javítsák a hibákat, illetve a felderített sebezhetőségeket az üzemeltetésért felelősök nem feltétlenül tudják vagy akarják kijavítani. A megtalált hibák fekete- és szürkepiaca jelentős volumenű, ezeket bűnszervezetek ugyanúgy megvásárolják, mint az államok számára kémszoftvereket fejlesztő vállalkozások. Kiváló példa erre a közismert, NSO Group által forgalmazott Pegasus kémszofver, mely olyan szoftveres sebezhetőségeket használt ki, amelyekről a szoftverek gyártói éveken keresztül nem értesültek. Így a támadók válogathatnak a rosszul beállított, hibákkal teli rendszerekből. Ha pedig minden rendben be van állítva és nincsenek benne ismert sebezhetőségek, akkor is bekövetkezhet egy olyan természeti katasztrófa vagy járulékos veszteség, amely magával rántja a digitális infrastruktúrát, ezen keresztül pedig a szervezet működését is.

Speciális fenyegetésként előretörtek az ellátási láncokat érő kibertámadások is. Ez azt jelenti, hogy a támadás egy olyan beszállítót, IT szolgáltatót ér, amely egy másik, tőle független nagyvállalat számára nyújt digitális szolgáltatást, sokszor úgy, hogy ez a kulcsfontosságú megoldás a nagyvállalat legtöbb dolgozója elől rejtve működik, azt csak kevesen ismerik. A támadó ebben az esetben a beszállító szolgáltatásának hibáját használja ki arra, hogy hozzáférjen a valódi célpont infrastruktúrájához, adatához. A támadást legtöbbször államilag támogatott csoportok hajtják végre, egyértelműen hírszerzési céllal, de a korábbiakban írtak szerint a kiberbűnözői eszköztárban is egyre inkább megtalálható ez a megoldás.

Automatizáció a kibertámadások során

Felsorolni is sok tehát azt a rengeteg kibertéri fenyegetést, amivel a szervezeteknek és a magánszemélyeknek szembesülnie kell nap mint nap. Ez pedig azt jelenti, hogy mind a támadói, mind a védelmi oldal kiterjedten használja az automatizációt, illetve a felgyülemlő hatalmas mennyiségű adat egyre jobb kihasználásával a mesterséges intelligenciát. Eközben pedig maga az automatizáció, az adatgyűjtés folyamata és mesterséges intelligenciát megvalósító rendszer is célponttá válik. A következőkben néhány példán keresztül kerül ismertetésre, hol is van jelenleg a helye ezeknek a megoldásoknak a kiberbiztonságban, figyelembe véve a támadó–védekező-rendszer háromszögének egymásra épülését.

A támadói eszköztár számos esete feldolgozásra került már jelen tanulmányban, ebből a jelenleg legfontosabbnak tartott zsarolóvírusok kapcsán érdekes áttekinteni, hogyan használják a kiberbűnözői csoportok a legmodernebb technikákat. A kiberbiztonsági szakterületen a támadás folyamatát és az ehhez kapcsolódó védelmi lehetőségeket a legjobban az úgynevezett *cyber kill chain*-modell írja le, mely hét lépés végrehajtását köti a sikeres támadáshoz.[6]

1. **Felderítés:** A felderítés célja a célpont minél jobb megismerése, a gyenge pontok felfedezése. Ez jellemzően két területen történik. Egyrészt az infrastruktúra gyengeségeit, másrészt a támadható munkatársakat próbálják megtalálni. Az informatikai rendszer felderítésének jelentős része automatizált, számos céleszköz áll rendelkezésre ahhoz, hogy akár hálózati, akár alkalmazási szinten azonosítani lehessen a belépési pontokat. Ezek az adatok ráadásul nagyon sokszor nem is közvetlenül a célpont befolyásolási körében vannak, hiszen ahogy az ellátási láncok támadása esetében arra volt már példa, egy szoftverfejlesztő cég terméktámogatási rendszerének feltörése után a célpont szinte teljes belső infrastruktúra-felépítése kikerült a támadókhoz. A humán felderítés is javarészt automatizált, hiszen ma már az emberiség jelentős része akkora digitális lábnyommal rendelkezik, hogy azt a megfelelő szoftveres támogatással egybe rendezve, kiváló személyes profil állítható össze.
2. **Fegyverzetkészítés:** A második lépésben a fellelt gyengeségek minél hatékonyabb kihasználása a cél, olyan támadókódok és pszichológiai manipulációk előkészítése, melyek biztosan működni fognak. Tekintettel arra, hogy a védelmi megoldások egyre komolyabb akadályt jelentenek, a támadóknak szimulálniuk kell a célpont környezetét, olyan kártékony kódokat kell létrehozniuk, amelyeket a határ- és végpontvédelmi megoldások nem ismernek fel. Esetleg olyan szoftveres sérülékenységeket kell megtalálniuk és ezeket kihasználniuk, amelyek még a gyártó számára sem ismertek, tehát úgynevezett nulladik napi (*0-day*) támadást tesznek lehetővé. Minden tevékenység jelentős időt vehet igénybe, amelyet az automatizáció segítségével lehet csökkenteni. A humán célpontok megté-

[6] Ságí 2017.

vesztésére – a korábban említetteknek megfelelően – napjainkban a mesterséges intelligencia nyújt támogatást. Néhány kattintással létrehozhatók olyan arcok, hangok, személyes és szervezeti profilok, teljes háttértörténetek, amelyek valójában nem léteznek, csak a gépi tanulás eredményei.

3. **Célba juttatás:** Az előkészített támadás első mozzanataként el kell juttatni a támadókódot a célrendszerhez vagy célszemélyhez. Ennek során fokozottan kell ügyelni a műveleti biztonságra, azaz olyan szervereket kell használni, amelyeken nem lesz fellelhető a támadás műszaki nyoma egy esetleges nyomozás során. Ez egyrészt úgy megvalósítható, hogy a támadó más tulajdonában álló, korábban megfertőzött eszközöket használ, ahol az eredeti tulajdonosnak fogalma sincs arról, hogy erőforrásait nem csak ő használja. Másrészt számos olyan felhőszolgáltatás is elérhető, melyek használat után nyom nélkül törölhetők, sőt, a szolgáltató esetleg még vállalja is, hogy nem őriz meg semmilyen nyomot az ügyfeleiről, azok „privát szférájának" védelme érdekében. Ezen infrastruktúrák üzemeltetése, durva anglicizmussal „orkesztrálása" (*orchestration*) olyan automatizmusokkal történik, melyek egy kattintással tudnak létrehozni vagy éppen megsemmisíteni informatikai erőforrásokat, így szinte lehetetlenné téve a nyomok visszakövetését a támadóig. Nem véletlen, hogy az egyik legfőbb nemzetközi törekvés az államok részéről az informatikai nyomok megőrzésére való kötelezés az ilyen szolgáltatók esetében.
4. **Kihasználás:** A kihasználás feltételezi, hogy a korábban elvégzett szimulációk működnek, a megtámadott rendszer valóban sebezhető. Viszont minél fejlettebb a védelmi rendszer, annál nagyobb autonómiával kell rendelkeznie a kártékony kódnak. Az automatizmus minimum ki kell, hogy terjedjen a futtatás után a végpontvédelmi rendszer („vírusirtó") kikapcsolására, egy hátsókapu (*backdoor*) nyitására, melyen keresztül a megfertőzött számítógép kommunikálni tud az internet felé, majd az interneten levő parancsvezérlő (*Command and Control* – C2) szerverrel való kapcsolatfelvételre. Bonyolultabb esetekben, például akkor, ha a megfertőzött számítógépnek nincsen közvetlen internetkapcsolata, akkor a kihasználást követő lépéseket is automatikusan kell megtenni. Amennyiben a kihasználás sikertelen, akkor pedig úgy kell a támadókódnak törölnie magát,

hogy véletlenül se maradjon semmilyen nyom, amelyből egy mélyelemzés bármilyen következtetést le tud vonni és felfedni, hogy a támadó ki volt és milyen módszert használt.

5. **Telepítés:** A sikeres kihasználást követően a támadó bent van a gépen, de a további lépések végrehajtásához további eszközökre van szükség. Ezeket az eszközöket, céltól függően, a C2 szerverről töltik le. Tipikusan ilyenkor kerül telepítésre az az eszköz, melynek segítségével a számítógépen tárolt jelszavak kinyerhetők, a belső hálózat felderítését segítő megoldások, illetve maga a zsarolóvírus is. Ez a folyamat is teljes mértékben automatizált, szakzsargonnal élve „szkriptelt" folyamat, hiszen ekkor a támadó már magas jogosultsággal rendelkezik, gyakorlatilag bármit megtehet az áldozat gépével. Ebben a lépésben kell megoldani az állandó jelenlétet is, hiszen a számítógépek időnként újraindításra, frissítésre kerülnek, a támadó szempontjából nem lenne jó, ha egy egyszerű ki-bekapcsolás után minden esetben újra végre kellene hajtani a támadóműveleteket. Az esetek túlnyomó többségében a teljes folyamat automatizált, emberi beavatkozást nem igényel.
6. **Irányítás és vezérlés:** Magának a C2 szervernek a legfontosabb feladata a parancsok kiadása a támadó uralma alá hajtott számítógép felé. A támadásra használt botnet hálózatot többszázezer, akár több millió megfertőzött gép alkotja, teljesen esetleges, hogy ezek közül éppen melyik lesz a felelős az irányításért és vezérlésért. Annak érdekében, hogy a botnet irányítója, a „bábmester" (*puppet master*) kontroll alatt tudja tartani ezt a hihetetlen informatikai erőforrást, igen komoly automatizációs megoldásokat használ fel. Tulajdonképpen egy botnet is csak egy nagyvállalati IT megoldás, amelyet üzemeltetni kell, így elkerülhetetlen a nagyvállalati gondolkodás.
7. **Feladat végrehajtása:** A támadásnak mindig van valami célja. A zsarolóvírus esetében ez a cél kettős. Egyrészt minél nagyobb mennyiségű digitális adat letöltése az áldozattól, másrészt ezen adatok titkosítása oly módon, hogy a szervezet ne tudja ezeket használni és olyan helyzetbe kerüljön, hogy fizetnie kelljen, vagy azért, hogy a működéséhez szükséges adatokat újra elérhesse, vagy azért, hogy ezek ne kerüljenek nyilvánosságra. A sikeres feladatvégrehajtás alapja az, hogy a támadó ki tudjon jutni a megtámadott számítógépről és minél több, az áldozat hálózatához tartozó számítógépre jusson be, lehetőleg mi-

nél gyorsabban és minél észrevétlenebbül. Erre leggyakrabban a Microsoft Windows rendszergazdai automatizálásra használt, beépített, tehát minden gépen megtalálható megoldását, a PowerShellt használják. Az iparági tapasztalatok alapján ennek segítségével napok vagy nagyobb, „értékesebb" célpontok esetén hetek alatt teljes sikert lehet elérni úgy, hogy az áldozat gyakorlatilag semmit nem vesz észre.

Automatizáció és adatok a kibervédelemben

A sikeres támadás előfeltétele a teljes, hétlépcsős folyamat során a „radar alatt maradni", úgy hajtani végre az egyes lépéseket, hogy az áldozat azt ne vegye észre. Ez azonban közel sem annyira könnyű, mint amilyennek azt a laikusok gondolják. Minden egyes tevékenység ugyanis valamilyen informatikai nyomot, úgynevezett naplóbejegyzést, más néven logot generál. Sőt, a humán célpontokat érő támadásokról akár teljes, visszajátszható felvételek is rendelkezésre állhatnak, amelyeket egy nyomozati eljárás során fel lehet használni. Az összes biztonsági adat begyűjtésével és elemzésével tehát elméletileg gond nélkül fel lehetne deríteni az összes kibertámadást még nagyon korai fázisban. Miért van az, hogy gyakorlatban ennek ellenére mégis folyamatosan hallani sikeres támadásokról és azok tovagyűrűző hatásairól?

A választ elsősorban a védelemben bevetett humán és technikai erőforrások rendelkezésre állásában és minőségében kell keresni. Nem véletlenül hallunk ritkán nagy pénzintézetek és digitális szolgáltatók elleni sikeres támadásokról, ahol minden szükséges erőforrás rendelkezésre áll a sikeres védelemhez. Ezzel szemben nem véletlenül hallunk sikeres támadásokról más iparágakból, ahol viszont nincsen több évtizedes tapasztalat, nincsenek széleskörű kiberbiztonsági előírások és nincsenek olyan tudású szakemberek, mint amilyenekre szükség lenne a jelenlegi fenyegetési trendek esetében. A különbség nem az, hogy az előbbieket nem támadják, a különbség az, hogy ezek képesek a korai észlelésre és elhárításra, hiszen hatalmas mennyiségben gyűjtik a biztonságilag releváns adatokat belső rendszereikről és külső forrásokból, majd ezeket élenjáró technológiával elemzik és akár autonóm módon is képesek gyors és hatékony védelmi intézkedéseket foganatosítani.

Az incidensmenedzsmentben felhasznált informatikai megoldások szédületes fejlődése néhány év alatt tette versenyképessé a kibervédelmet a támadókkal szemben. Az informatikai védelem kezdetétől bevett szokás volt a biztonsági szempontból fontos naplóbejegyzések gyűjtése és azok eseti, jellemzően incidenst követő vizsgálata, annak megértése érdekében, hogy mi is történt valójában. A Nagy Adatok (*Big Data*) diszciplínájának fejlődése azonban komoly áttörést hozott az évtizedek óta használatban lévő felfogásban, így a 2010-es évek elején megjelentek az első olyan megoldások, amelyek nemcsak gyűjtötték és kereshetővé tették a logokat, hanem az ismert sémák mentén automatikusan képesek voltak jelezni, ha valamilyen, korábbról már ismert kártékony tevékenység történik a hálózatban. Ezt követte a gépi tanulás megjelenése a védelemben. Mivel az adatok rendelkezésre álltak, azokból megismerhetővé vált a teljes hálózat „szokásos" működése, így az ezekhez képesti eltérések, anomáliák detektálása is megvalósíthatóvá vált. További fejlődést jelentett a szervezeten kívülről érkező adatok befogadásának a lehetősége, az ilyen, kereskedelmi, partneri vagy állami forrásból származó támadási információk (*cyber threat intelligence* – CTI) automatikus fogadása és a rendelkezésre álló tudás dúsítása tovább segítette a fejlett védelem kiépítését. A fejlesztések jelenlegi célja az, hogy a felismert támadási kísérletek mielőbbi elhárítása céljából a rendszer automatikusan, vagy az operátort értesítve, a döntést az embernek meghagyva, félautomatikusan tudjon beavatkozni.

Az automatizáció terjedésének legfőbb indoka az emberi kiszámíthatatlanságban keresendő. Az ember nem gép, fárad, figyelmetlen tud lenni, érzelmei befolyásolják a döntéseit, időnként felmond és más munkahelyet keres. A kiberbiztonságban a védelem hatékonyságát ezek a faktorok pedig jelentősen rontják. Először is, eleve kevés szakember van a kiberbiztonsági területen, csak Magyarországon a szerző saját felmérése szerint évente százas nagyságrendben keletkeznek olyan új kiberbiztonsági munkahelyek, amelyeket nem, vagy csak hosszú idő elteltével tudnak betölteni. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetének vezetője közlése szerint például a 2013. évi L. törvény hatálya alá tartozó önkormányzatok kevesebb mint fele jelentett be információbiztonságért felelős személyt, noha erre a jogszabály értelmében kötelezettek. Hasonlóan kiábrándító a helyzet az Európai Unió statisztikái alapján is, a magyar kis- és közepes vállalkozások nem igazán foglalkoznak az

információbiztonsággal, holott a fenyegetés egyre inkább nő.[7] A jelenlegi munkaerőhiány tehát jelentősen fokozódni fog, ahogy a digitalizáció hatására a magyarországi szervezetek is komolyabban fogják venni a kiberbiztonságot.

Az emberi fáradtság, figyelmetlenség, kiégés szintén egy fontos indok az automatizáció mellett. Jellemzően ugyanis a már meglevő védelmi rendszerek teszik a dolgukat, jellemzően nem történik semmi rendkívüli, amivel a kiberbiztonsági szakembereknek foglalkoznia kellene. Az ISACA Magyarország felmérése szerint a magyarországi szervezetek nem tapasztalnak ilyet vagy évente csak 1-2 incidensről tudnak beszámolni.[8] Ennek egyik oka, hogy valóban nem jellemző ennél komolyabb kitettség, másik oka, hogy gyakran nem is érzékelik, hogy történt valami. Minden biztonsági területnek, így az információbiztonságnak is komoly csapda ez, hiszen a biztonságnak csak a hiánya látszódik, ha rendben működik, akkor előbb-utóbb arra jut a monetáris szemléletű szervezeti vezető, hogy úgysem lesz semmi baj, nem kell ilyen sokat költeni a szakterületre. Sajnos ugyanígy van ezzel a védelemben dolgozó szakember is, ha nem történik semmi, nem is tudja annyira komolyan venni a sűrűsödő jeleket, mint ahogy azt kellene. Ebben a helyzetben tud nagyon sokat segíteni az adatokra épülő, mesterséges intelligencia támogatott automatizáció, melynek figyelme biztosan nem lankad, illetve egyre gazdaságosabban beszerezhető és üzemeltethető egy teljes kiberbiztonsági csapat költségéhez mértve. A közeljövőben tehát folyamatosan láthatjuk majd megjelenni az adatokra épülő, automatizált döntéstámogató biztonsági rendszerek előretörését, amelyet a munkaerőhiány miatt leginkább külső szolgáltatók fognak üzemeltetni.

Összefoglalás

A támadók mindig a védelem előtt járnak, ez egy olyan evidencia, amelyet évezredek tapasztalata bizonyít. Nincs ez másképpen a kiberbiztonságban sem. De ha a védelem olyan megoldásokat vet be, melyek

[7] European Commission 2020.

[8] ISACA Budapest Chapter 2021.

komolyan megnehezítik a támadó dolgát, mit fog a támadó lépni annak érdekében, hogy újra fölénybe kerüljön? Mit tehet a támadó, hogy kikerülje a mesterséges intelligencia támogatott kibervédelmi megoldásokat? A választ a 2021-re jellemző támadási sémákból már részben láthatjuk. Egyrészt olyan célpontokat keres, amelyek még nem rendelkeznek a kibervédelem legmagasabb fokával, másrészt elkezdi ő maga is bevetni a mesterséges intelligenciában rejlő lehetőségeket. Mivel a katonai és a tudományos világban már évek óta foglalkoznak a mesterséges intelligencia felhasználásával végrehajtott kibertámadások kivitelezésével, megjósolható, hogy ez hamarosan a kiberbűnözésben is megjelenik majd. Mint korábban említésre került, a jelenlegi védelmi rendszerek a támadási kísérletek nagy részét megfogják. Ez egy adat a gépi tanulásnak, hogy mivel ne próbálkozzon, egy adat arról, hogyan reagál a célpont.

További lehetőség az, hogy a zsarolóvírus-támadások során kinyert több terrabájtnyi adat szolgál majd alapul egy szofisztikált támadás megtervezéséhez. Ha ezek az adatok tartalmazzák azt a halmazt is, amely a védelmi rendszerekből származik, még pontosabb, célzottabb támadások tervezhetők a mesterséges intelligencia által. Erre lehet egy példa az „adatmérgezés", amikor hosszabb ideig, tudatosan fals adatokat közöl a támadó a védelmi intelligenciával, annak érdekében, hogy az „megtanulja" a támadó viselkedését és azt normálisnak könyvelje el, tehát se jelzést ne küldjön az operátornak, se automatikus védelmi intézkedést ne foganatosítson. Ez azonban egyelőre még évekre van a jelenlegi helyzethez képest, elsőként pedig valószínűleg úgyis állami hátterű műveletekben fogunk ezzel a megoldással találkozni. A kibervédelemnek előbb át kell mennie azon a paradigmaváltáson, melyet zéró bizalomnak (*zero trust*) nevezünk, át kell terveznie a létező architektúrákat és implementálnia kell az újszerű védelmi megoldásokat. De ha ez meg is történik, még mindig milliószámra lesznek védtelen szervezetek és milliárdszámra eszköztelen magánszemélyek, akik elsőrendű célpontot jelentenek. A megoldást tehát csak részben kell a technológiában keresni. Sokkal inkább a kibertér békéje, legalábbis status quoja vezethet el oda, hogy átlagos felhasználóként a kibertéri kihívásokból semmit ne érezzünk, szakértőként pedig ne rettegjünk folyamatosan a negyedik ipari forradalom azonnali összeomlásától és a civilizáció egy évszázaddal ezelőtti szintjére való visszaesésétől.

Irodalom

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

Berki, Gábor 2018: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. *Nemzetbiztonsági Szemle,* 2018/3, 5–21.

ENISA 2021: *ENISA Threat Landscape 2021.* Athén, European Union Agency for Cybersecurity.

European Commission 2020: *Digital Economy and Society Index (DESI) 2020 – Cybersecurity.* Brüsszel, European Commission.

ISACA Budapest Chapter 2021: *Információbiztonság Helyzetkép 2021.* Budapest, ISACA Budapest Chapter.

Nagy, Judit 2019: Az Ipar 4.0 fogalma és kritikus kérdései – vállalati interjúk alapján. *Vezetéstudomány,* L. évfolyam, 1. szám. DOI: 10.14267/VEZTUD.2019.01.02

Sági, Gábor 2017: Informatikai rendszer támadási folyamata. *Műszaki Katonai Közlöny,* XXVII. évfolyam, 3. szám, 212–223.

Schwab, Klaus 2021: The Fourth Industrial Revolution. *Encyclopedia Britannica.* https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734