Felhők biztonsági kérdéseinek aktualitásai

KOVÁCS ZOLTÁN
Vodafone Magyarország Zrt.
zkovacs.24@gmail.com

Kulcsszavak: felhő, mesterséges intelligencia, ellátási lánc, kiberbiztonság

Jelen cikk rávilágít a felhőalapú rendszerek megkerülhetetlenségére, példákat hoz a speciálisan a felhőalapú rendszereknél jelentkező biztonsági problémákra, majd bemutat egy lehetséges módszertant annak eldöntésére, hogy egy felhőalapú rendszer teljesíti-e a minimálisan elvárt biztonsági szintet. A biztonság szemszögéből felvázolja a privát és az állami szférában használt felhőalapú rendszerek lényegesebb különbségeit, valamint példákon keresztül mutatja be az ellátási lánc védelmének jelentőségét. Példákat hoz a mesterséges intelligencia, és annak felhőben működő megoldásainak védelmi célú használatára, amely mellett bemutatja annak támadó oldalon történő felhasználást is.

1. Bevezetés

Napjainkban a felhőalapú rendszerek használata megkerülhetetlen. Ma már állami szervezetek is egyre gyakrabban használnak ilyen rendszereket, kihasználva annak költséghatékonyságát és egyéb előnyös tulajdonságait. Ez Magyarországra is igaz. Ugyanakkor a felhőalapú rendszerek használatakor bizonyos, több esetben a teljesen saját infokommunikációs rendszertől eltérő biztonsági kihívással is számolniuk kell a felhasználóknak. Ezeket pedig a kockázatelemzésük során figyelembe kell venniük.

A felhőalapú rendszerek biztonsága az elmúlt években sokat fejlődött. Sok esetben akár biztonságosabb is lehet a felhasználó számára, mint egy teljesen saját rendszer használata. Annak elemzésére, hogy egy felhőalapú rendszer biztonsági szempontból mennyire felel meg egy adott szervezet elvárásainak, ma már megvannak a módszerek.

Mindezek mellett egy olyan jelenség is megfigyelhető, hogy épp a felhőalapú rendszerek használatával egyre több kiszervezés, majd onnan bizonyos feladatok további kiszervezése, azaz újabb felek bevonása valósul meg. Így a korábbihoz képest is újabb ellátási láncok jönnek létre, az egyes szervezetek pedig egyre inkább csak az alaptevékenységükre koncentrálnak. Ez azonban új veszélyeket is rejt, amelyekkel a jövőben számolniuk kell.

Jelen cikk az első szakaszában előrejelzéseken keresztül világít rá a felhőalapú rendszerek megkerülhetetlenségére, példákat hoz a speciálisan a felhőalapú rendszereknél jelentkező biztonsági problémákra, majd bemutat egy lehetséges módszertant annak eldöntésére, hogy egy felhőalapú rendszer teljesíti-e a szervezet által minimálisan elvárt biztonsági szintet. A második szakasz biztonsági aspektusból felvázolja a privát és az állami szférában használt felhőalapú rendszerek lényegesebb különbségeit, valamint példákon keresztül mutatja be az ellátási lánc védelmének jelentőségét. A harmadik szakasz a mesterséges intelligencia védelmi célú használatára hoz példákat.

2. A felhőalapú rendszerek megkerülhetetlensége és biztonsága

A felhőalapú rendszerek használata egyre jobban terjed. Érezzük ezt mindennapjainkban is, hiszen magánemberként is egyre több ilyen rendszert használunk. Igénybe vehetünk banki szolgáltatásokat és fizethetünk webáruházakban, játszhatunk, szerkeszthetjük dokumentumainkat, képeinket, tárolhatjuk, megoszthatjuk adatainkat, készíthetünk útvonaltervet, és még nagyon hosszan lehetne folytatni a felsorolást. Igaz ez a vállalati felhasználásra is. Az elmúlt években egyre nőtt és az előrejelzések szerint várhatóan a jövőben is tovább növekszik a felhőalapú rendszerek felhasználása. A Canalys cég elemzése szerint a felhő-infrastruktúrára költött összegek világviszonylatban negyedévről negyedévre folyamatosan nőttek, és bár a növekedés üteme kicsit lassult, az még így is 35% körül mozog [1]. Ezt mutatja be az *1. ábra*.

A Technavio szerint a növekedés valóban lassul, de 2025-ig szóló előrejelzésük szerint a globális felhőpiac átlagos éves növekedési üteme 2021–2025 között még így is 17% felett várható. A növekedéshez egyedül Észak-Amerika mintegy 40%-kal járul majd hozzá [2]. A Grand View Research 2028-ig szóló előrejelzésében a növekedés éves átlagos ütemét globálisan 19,1%-ra becsüli, az Egyesült Államok piacán pedig 18,1%-ra úgy, hogy a piac megoszlása a szolgáltatási modellek (infrastruktúra mint szolgáltatás, platform mint szolgáltatás és szoftver mint szolgáltatás) között arányaiban nem változik jelentősen [3].

A fentiekből látszik, hogy a felhőalapú rendszerek felhasználása a közeljövőben is erőteljesen növekedni fog.

A felhasználásnál azonban a biztonságra, különös tekintettel a felhőalapú rendszereknél jelentkező biztonsági kihívásokra is figyelemmel kell lenni. Ezek azok a kérdések, amelyek egy teljesen saját infokommunikációs rendszer esetében lényegesen más hangsúlyokkal jelennek meg, vagy adott esetben egyáltalán nem jelennek meg. Kiragadott példák ilyenek lehetnek:

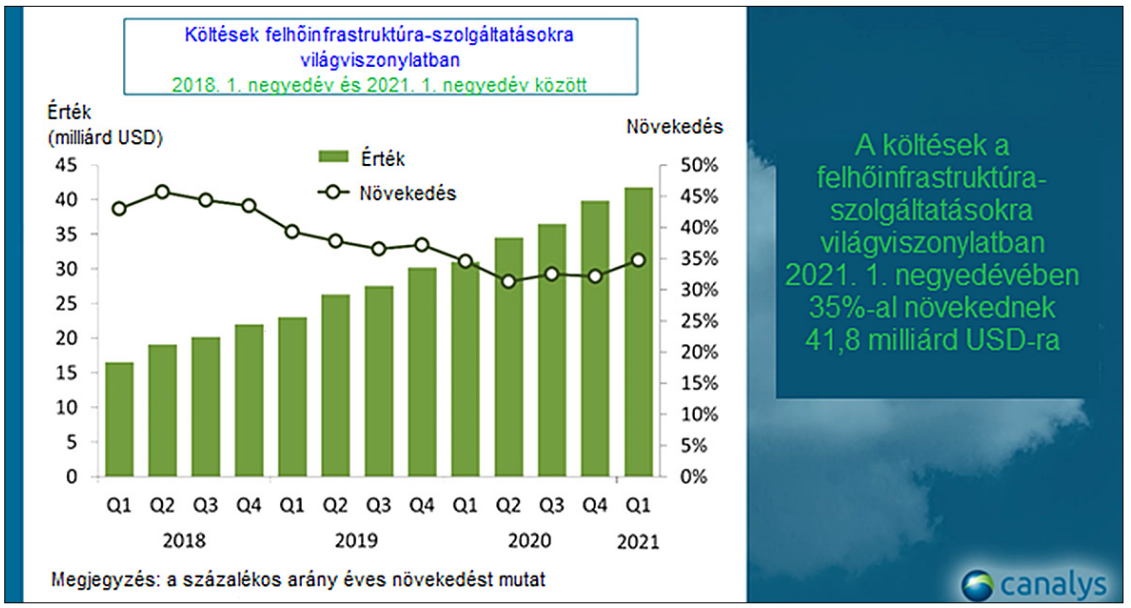
- *adatokkal kapcsolatos biztonsági meggondolások* (adatok, naplóadatok tulajdonjoga, adatok migrációja, adatok biztonsága és adatvédelemi kérdések, biztonsági tesztelések célja és hatálya, hibajavítások, adatmegőrzés és -törlés, interoperabilitás stb.);
- *adatmegőrzési kérdések* (adott esetben a jogszabályi kötelezettségekből adódó adatmegőrzés hogyan biztosítható, az adataink valóban törlésre kerüljenek, azok ne legyen visszaállíthatók, még a back-up-ból sem stb.);
- *a kínált és szükséges biztonsági intézkedések* (hozzáférési pontok, biztonsági értékelések és jogosultságok, folyamatos ellenőrzés, biztonsági ellenőrzések implementálása stb.);
- a felhőben használt *virtuális operációs rendszerek biztonsága* (többfelhasználós környezet problémái, izoláció stb.);
- *titkosítás* szükségessége (a felhő használatához, a felhő-erőforrások felügyeletét szabályozó interfész, operációs rendszerek, alkalmazások, adatok eléréséhez);
- *naplózási* kérdések (mi kerül naplózásra, ki és hogyan férhet hozzá a naplóadatokhoz stb.);
- *szolgáltató kémkedésének* kérdésköre;
- *harmadik fél bevonása* (mikor és mihez férhetnek hozzá a szolgáltató olyan alvállalkozói, akikkel a felhasználónak nincs szerződése stb.).

A fentiekből látszik, hogy a kockázatelemzést és a kockázatok csökkentésére szóló intézkedéseket más hangsúlyokkal kell elvégezni, mint egy tisztán saját rendszer esetében, és a szolgáltatóval való együttműködés, adott kérdések szerződésben való rögzítése pedig elengedhetetlen. Annak érdekében, hogy megvizsgálhassuk, hogy egy felhőalapú rendszer és annak szolgáltatója megfelel-e a szervezet által támasztott biztonsági követelményeknek, több módszert is alkalmazhatunk.

Az egyik ilyen lehetőség, hogy megvizsgáljuk az alábbi kérdéseket:

Üzembiztonság
- – közösségi felhő közös üzembiztonsági alapkövetelményei
- – hordozhatóság és interoperabilitás
- – üzletmenet-folytonosság
- – rendelkezésre állás, ellenálló-képesség, megbízhatóság
- – szolgáltatási szintek, azok garanciái
- – skálázhatóság és erőforrás-menedzsment
- – redundancia
- – katasztrófa-elhárítási terv
- – biztonsági mentés és visszaállítás
- – életciklus-kezelés és változásmenedzsment
- – adatmigráció
- – adatformátum
- – adatközpont működése, rendszerkonfiguráció
- – alkalmazásbiztonság
- – javítócsomagok kezelése
- – ellátási lánc üzembiztonsága
- – üzembiztonsági kockázatcsökkentés

Adatbiztonság
- – közösségi felhő közös üzembiztonsági alapkövetelményei
- – irányítás
- – kockázatkezelés
- – azonosítás, hitelesítés jogosultságkezelés és hozzáférés-szabályozás
- – határvédelmi eszközök működtetése és ellenőrzése
- – folyamatos ellenőrzés
- – incidenskezelés
- – sérülékenység vizsgálata, kezelése
- – titkosítás és kulcskezelés



1. ábra
A felhő-infrastruktúrára költött összegek változása világviszonylatban.
(Forrás: https://canalys.com/newsroom/global-cloud-market-Q121)

– virtualizációból adódó biztonság kezelése
– kliensoldali védelem
– vezeték nélküli hálózatok biztonsága
– biztonsági architektúra
– adatok elvesztése, ellopása
– mobil eszközök kezelésének terve

Egyéb (jogi, fizikai stb.) biztonság

– jogi megfelelőség
– fizikai biztonság
– személyi biztonság
– gazdasági biztonság
– dokumentumbiztonság

Azért ezen kategóriákon keresztül és nem a szokásos bizalmasság-sértetlenség-rendelkezésreállás mentén érdemes foglalkozni a kérdéskörrel, mert egyrészt az egyes szervezeteknél különböző emberek, jobb esetben csoportok vagy szervezeti egységek foglalkoznak a fent említett témakörökkel, másrészt a szakirodalomban is találkozhatunk hasonló megközelítésekkel, így például felosztásában közel azonos jellegűt lehet találni a BSI [4] és szinte teljesen megegyezőt az ENISA [5] anyagaiban.

Az elemzéshez használható például az alább röviden ismertetésre kerülő elemző sablon, amely a felhőalapú rendszer minimálisan elvárt biztonsági szintjének megállapítására szolgál. Ebből mutat be egy részletet a *2. ábra*.

A sablon az említett három főcsoportra bomlik, az egyes főcsoportokon belül további alcsoportok találhatóak. Szürke színnel a kiemelt fő vagy összegző, míg fehérrel az egyes részletkérdések találhatók meg. A kérdésekhez igen/nem válaszok adhatók, a fehér kérdések közül a felhasználó döntése alapján egy vagy akár több is elhagyható, a szürkék kitöltése kötelező. A fehérrel jelölt alcsoporti kérdések esetében a nemleges válasz még nem jelenti automatikusan azt, hogy a vizsgált felhőalapú rendszer nem felel meg a megkívánt biztonsági követelményeknek. A szürkével jelölt összegző, vagy fő kérdések esetében a nemleges válasz viszont igen [6]. Egy ilyen elemző sablon kitöltése után a szervezet el tudja dönteni, hogy az adott felhőalapú szolgáltatás és annak szolgáltatója megfelel-e az általa elvárt minimális biztonsági követelményeknek. Amennyiben igen, akkor az ezen felüli részletes biztonsági követelményeket a későbbiekben tisztázni, majd a szerződésben rögzíteni tudják.

Az elemzéshez más, például a FedRAMP [7], vagy az ott leírtakhoz hasonló sablon is használható.

2. ábra Részlet a biztonsági elemző sablonból.

Kategóriák vizsgálandó kérdései	válaszok	
	igen	nem
Üzembiztonság:		
1. közösségi felhő közös üzembiztonsági alapkövetelményei		
A felhasználó számára megfelelő és elfogadható a közösségi felhő felhasználói által kialakított közös üzembiztonsági alapkövetelmény rendszer?	☐	☐
2. hordozhatóság és interoperabilitás		
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az adatok hordozhatóságát és a különböző (szolgáltató, felhasználó, harmadik fél) rendszereinek együttműködését?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más, saját országbeli érintett hatóság vagy közigazgatási szervvel?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más országok vagy EU érintett rendvédelmi szerveinek rendszereivel?	☐	☐
◦ A szolgáltató nyilvános, publikált API-kat használ?	☐	☐
◦ A szolgáltató által kínált interfészek interoperabilisak		
▪ a felhasználó rendszereinek interfészeivel?	☐	☐
▪ a felhasználó munkafolyamataihoz kapcsolódó harmadik felek rendszereinek interfészeivel?	☐	☐

3. Az ellátási lánc védelmének jelentősége

Mielőtt rátérnénk az ellátási lánc védelmének kérdéseire, érdemes áttekinteni, mit jelent egy kormányzati felhő használata biztonság szempontjából. Egyrészt azért, mert mások lehetnek a biztonsági elvárások, az állami szervezetek által használt felhőalapú rendszereknél sokszor vagy szigorúbbak, vagy – a jogszabályi előírások miatt – kötöttebbek. Másrészt pedig azért, mert hazánkban is használnak felhőalapú megoldásokat a kormányzati szervek.

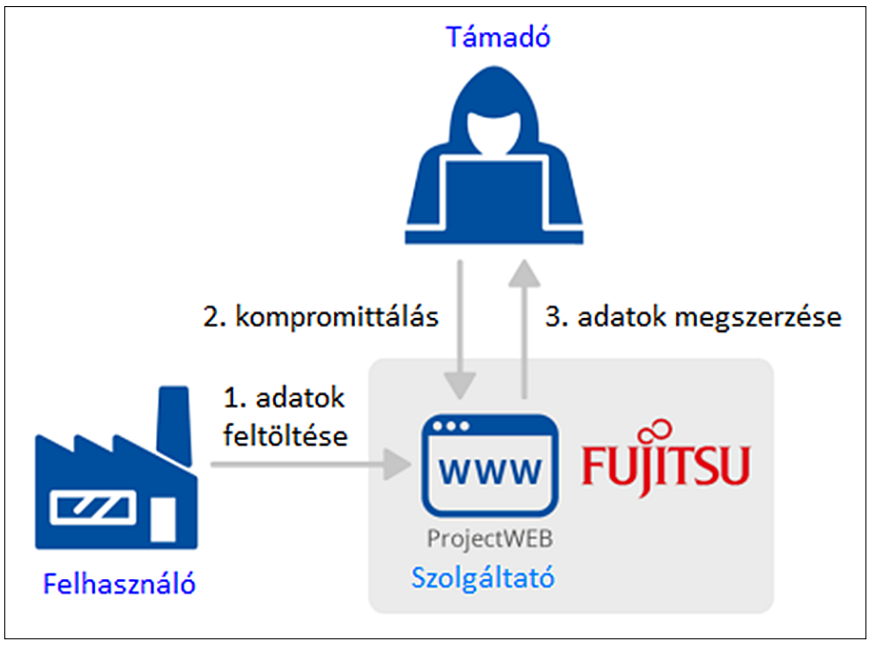
Magyarországon a NISZ Zrt. nyújtja a kormányzatifelhő-megoldásokat, így hazánkban – előremutató módon – állami szolgáltatás keretében biztosítanak meghatározott szervezetek számára felhőalapú rendszereket. Ezzel sikerül kihasználni a felhő előnyeit (pl. költséghatékonyság, megfelelő színvonalú hardver- és szoftverelemek, megfelelő mennyiségű és tudású szakembergárda stb.) és azokat ötvözni egy magasabb szintű biztonsággal. Azzal ugyanis, hogy a szolgáltató hazai, ráadásul állami tulajdonú is, a biztonsági problémák jelentős részét megoldották. A korábban a felhőalapú rendszerek kapcsán jelzett biztonsági felvetéseket ugyanis egyrészt jogszabályi alapon lehetett kezelni, másrészt az államnak minden lehetősége megvan ezen előírások betartatására és azok ellenőrzésére. Ez pedig olyan kérdésekben is megnyugtató választ tud adni, mint a lentebb ismertetésre kerülő ellátási lánc elemei esetében a megfelelő biztonság kialakítása.

Ugyanakkor meg kell jegyezni, hogy így is maradtak fenn kihívások. Az egyik, hogy a kormányzati felhőt meghatározott szervezeti kör használhatja. Ez természetes, mert ez a deklarált célja. Ugyanakkor ez azt is jelenti, hogy nem minden állami, önkormányzati szerv tudja használni. Nekik viszont vagy saját infokommunikációs rendszert, vagy – amennyiben ez lehetséges – publikus felhőt kell használniuk. A másik, hogy egy kormányzati célú felhőalapú rendszer továbbfejlesztése mindig korlátozottabb, mint egy privát rendszer esetében. Harmadrészt a kormányzati felhő felhasználói „shadow IT"-jelleggel használhatnak úgy privátfelhő-megoldásokat, hogy az nem engedélyezett, vezetőiknek arról nincs is tudomása. Például levelezést folytathatnak Gmail-en keresztül, vagy ezen keresztül küldenek át maguknak olyan anyagokat, amelyekkel az otthoni gépükön is dolgoznak egy szoros határidő miatt. Ezek mind olyan biztonsági kihívások, amelyekkel a szakembereknek foglalkozniuk kell.

A felhőalapú rendszerek egyre nagyobb arányú használata az ellátási láncokra is jelentős hatást gyakorolt. A korábban az egyes szervezetek által tulajdonolt és üzemeltetett rendszerek részben vagy egészben máshoz kerültek, bizonyos feladatokkal együtt. Ezzel új elemek vagy ágak jelentek meg az ellátási láncokban. Ugyanakkor biztonsági szempontból ennek veszélyei is vannak. Az ENISA 2021-ben kiadott tanulmánya [8] is erre hívja fel a figyelmet. Tanulmányukban 24 olyan publikusan is bejelentett és igazolt, az ellátási láncot ért támadást elemeznek, amelyek 2020. január és 2021. július között következtek be.

Ezek közül egy kiragadott példa a Fujitsu Projectweb elleni támadás. A Projectweb egy felhőalapú szoftver, amelyet a felhasználó szervezetek online együttműködésre, szoftvermenedzsmentre és fájlok megosztására használnak, és a japán kormányzati szervek is előszeretettel használják. A támadás következtében a támadók hozzáfértek kormányzati adatokhoz és többek között a japán légiforgalmi irányító adatait is ellopták. A támadás lefolyását mutatja be a *3. ábra*.

3. ábra A Fujitsu Projectweb elleni támadásának lefolyása. (Forrás: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)



Az ENISA tanulmánya jól szemlélteti az ellátási lánc védelmének jelentőségét. Elemzésük szerint az incidensek kb. 58%-ánál a támadások az ügyféladatok (beleértve a személyazonosításra alkalmas adatokat) és a szellemi tulajdont tartalmazó eszközök ellen irányultak, és a támadások 66%-ánál a beszállítók nem tudták, vagy nem jelentették az incidenst. Ez utóbbi jól szemlélteti azt is, hogy az ellátási lánc szereplői között más a kiberbiztonsági, ezen belül az incidensek jelentésének érettségi szintje. Az ENISA tanulmánya szerint az ellátási láncot ért támadások 2021-ben várhatóan 4-szeresére nőnek 2020-hoz képest.

Biztonsági szempontból ezt a problémakört mindenképp tovább kell vizsgálnia azon cégeknek, akik ilyen kiszervezéseket végeztek, és/vagy felhőalapú rendszereket használnak. Ennek kapcsán olyan kérdéseket is vizsgálniuk kell, mint az, hogy a szolgáltató cég is tovább szerződhet, azaz bizonyos feladatokat, funkciókat más beszállítótól vehet igénybe, vagy adott esetben egy felhőalapú szolgáltatást használhat a szerződéses feladatai teljesítéségez. Ebben az esetben is azonban a teljes láncon keresztül biztosítani kell az adatokat birtokló cég kiberbiztonsági követelményeit. Meg kell határozni, hogy ki és miért felelős pontosan, hogyan lehet védekezni a teljes ellátási láncban, kinek milyen kiberbiztonsági követelményeket kell teljesítenie, mikor és ki felé milyen jelentési kötelezettség van incidens esetén, hogyan lehet auditálni az alvállalkozók alvállalkozóit stb.

De más vagy akár fordított kihívások is jelentkeznek az ellátási láncok kapcsán. Ilyen például az 5G-magánhálózatok esete. Ebben az esetben valamely szolgáltató 5G-magánhálózatot létesít a felhasználó telephelyén, a felhasználó pedig ezen keresztül akár a teljes robotizált termelését irányíthatja néhány felügyeletet ellátó ember segítségével.

Az 5G kapcsán az EU hathatós lépéseket tesz a biztonság megteremtése érdekében. Így kiadta az 5G-biztonsággal kapcsolatos uniós eszköztárat (EU toolbox on 5G Cybersecurity) [9], amelynek alapján az egyes nemzeti hatóságok szabályozhatják az 5G biztonsági kérdéseit. Ezek alapján szolgáltatói oldalról a megfelelő védelem biztosított lesz. Ebben az esetben a felhasználói oldalról rendkívül fontos a megfelelő szintű védelem kiépítése, hiszen a támadók adott esetben akár komoly – a vállalat profiljától függően akár még a környezetre is kiható – rombolást tudnak okozni.

4. Mesterséges intelligencia védelmi célú használata

Ma már a mesterséges intelligencia és a gépi tanulás azok közé a buzzwordök közé tartoznak, amelyeket lépten-nyomon hallhatunk. Ugyanakkor számos tudományos cikk, a témával foglalkozó fórum és blogbejegyzés foglalkozik a témával. Ma már elmondhatjuk, hogy mind a mesterséges intelligencia, mind a gépi tanulás a mindennapok részévé vált a kiberbiztonságban, és sajnos nem csak a védő, hanem a támadó oldalon is.

A védő oldalon megjelenő, mesterséges intelligenciával és gépi tanulással felvértezett eszközökről a gyártók is előszeretettel kommunikálnak, ám ezek hasznosságát, felhasználhatóságát a kibervédelemmel foglalkozó szakemberek is fel- és elismerik. Egy 2018-ban megjelent interjú szerint egy közepes méretű vállalat naponta kb. 200.000 biztonsági eseménnyel találkozik [10]. Ezek feldolgozása pedig csupán emberi erőforrással nem lehetséges. Egy 2021-ben megjelent tanulmány [11] szerint a mesterséges intelligencia használatának a kiberbiztonságban az alábbi fő előnyei vannak:

A mesterséges intelligencia:

1. *idővel egyre többet tanul,* így jól fogja ismerni az üzleti folyamatokat, a hálózati forgalmat, az ott zajló folyamatok normál viselkedését;
2. *azonosítja az ismeretlen fenyegetéseket,* amelyeket az ember sok esetben nem ismer fel;
3. *sok adatot képes kezelni,* így az egyre növekvő mennyiségű logot, riasztást, eseményt stb. is;
4. *jobb sérülékenységmenedzsmentet biztosít,* mert gyorsabb értékelést és felmérést biztosít;
5. *jobb általános biztonságot nyújt,* mert rengeteg támadási formát képes felismerni és priorizálni azokat;
6. *csökkenti az ismétlődő folyamatokat,* így fizikai és lelki terhelést is levesz a kiberbiztonsági szakemberekről;
7. *felgyorsítja az észlelési és válaszidőt,* ezáltal jelentősen növeli a hálózat biztonságát;
8. *biztonságosabb hitelesítést biztosít,* mert számos eszközt tud használni ehhez (pl. biometrikus azonosítás, CAPTCHA[1], brute force[2] felismerés).

A mesterséges intelligencia védő oldali használatával kapcsolatban a FireEye kiberbiztonsági cég 2018-as „FireEye Cyber Defense Summit 2018” című konferenciáján volt egy kerekasztal-beszélgetés. Ezen David Gunning, a DARPA[3] mesterséges intelligenciát kutató programjának menedzsere azt jósolta, hogy a kibervédelemben az ún. Tier1-szintű operátorokat öt éven belül kiváltja a mesterséges intelligencia. A Tier1-szintű operátorok azok a szakemberek, akik a riasztások, kiberbiztonsági események közvetlen és gyors feldolgozását végzik, vagy gyorsan lezárva az adott vizsgálatot (vagy azért mert ismert esemény, vagy azért mert téves, azaz fals positive riasztás volt), vagy ha az további vizsgálatot igényel, akkor továbbítják azokat az ún. Tier2-szintű elemzőknek. Bár az Egyesült Államokban a Tier1-operátorok feladatköre meglehetősen egyszerű és jórészt betanított feladatokból áll, azért ez a jóslás így is jól szemlélteti a mesterséges intelligencia fejlődését és előretörését napjainkban.

A felhőalapú rendszerek, a mesterséges intelligencia felhasználható a csalás elleni küzdelemben is. A több országban is működő nemzetközi vállalatok önmagukban is hatékonyan tudják használni a felhőalapon működő, mesterséges intelligenciát használó csalás elleni platformokat, hiszen olyan előnyöket tudnak kiaknázni, mint a szabályrendszerek egységesítése, a legjobb gyakorlatok beépítése, vagy egy újonnan felismert csalási formák elleni védekezés azonnali elterjesztése az összes leányvállalatnál stb. Ugyanakkor felmerül a kérdés, hogy ha ezek a rendszerek az adott ágazatban dolgozó vállalatok számára is hasonló előnyökkel járnának, miért nem épültek még ki? Ebben az esetben hasonló problémák jelentkeznek, mint a kiberbiztonság kapcsán a felismert fenyegetések egymás közötti megosztásakor. Ebben az esetben is a bizalom, a lehetséges veszteségek és az egymás közötti verseny jelentkeznek mint befolyásoló tényezők, amelyek jelentősen lassítják vagy akár el is lehetetleníthetik az ilyen ágazati platformok létrejöttét, működését. A költségek megosztása és a várható nyereség okán ugyanakkor érdemes lenne ilyeneket működtetni.

A mesterséges intelligencia természetesen a támadó oldalon is megjelenik. A támadók mesterséges intelligenciát – valamint annak részhalmazát, a gépi tanulást – is használják hatékonyabb, automatizáltabb, agresszívabb és összehangoltabb támadások indítására. Ezek segítségével ugyanis jobban fel tudják térképezni és meg tudják érteni, hogy a célpont-szervezetek hogyan védik a rendszereiket. Erre egy példa az ügyfélszolgálatokon is használt, mesterséges intelligenciával támogatott nyelvi feldolgozó eszközök, amelyek a támadók kezében kifinomultabb adathalász-levelek előállítását teszi lehetővé [12]. A támadók a támadás különböző szakaszaiban használják, használhatják a mesterséges intelligenciát. Így például az önállóan működő kártékony kód elkészítéséhez és bejuttatásához, a hálózaton belüli terjedéshez, a védelmi technológiák intelligens megkerüléséhez, a kisméretű és alacsony sebességű adatlopáshoz, vagy a felhasználó „élethű” szimulálásához stb. [13]. A Dark Web piacterein számos mesterséges intelligenciát és gépi tanulást használó hackereszközt kínálnak, és a kibertámadásokra egy ökoszisztéma épült fel, amelyben a támadás, mint szolgáltatást[4] is igénybe lehet venni [14]. A gyakorlati tapasztalatok is azt mutatják, hogy a támadók használják már ezeket a technológiákat.

1 CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart, azaz teljesen automatizált nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére – egy olyan teszt, ami képes megkülönböztetni az emberi felhasználót a robottól (sz.géptől).

2 Brute force, azaz nyers erő. Ez egy titkosításokkal, jelszóvédelemmel szemben alkalmazott támadási módszer, amely során a támadó kipróbál minden lehetséges variációt a jelszóra.

3 DARPA (Defense Advanced Research Projects Agency), az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlege.

4 cyber-attack-as-a-service (CAaaS)

A fentiek alapján napjainkban a mesterséges intelligencia használata a támadó és a védő oldalon is a gépek közötti, sőt az intelligencia-intelligencia közötti küzdelemről szól. A 2019-ben megrendezett RSA-konferencián, amely a világ legnagyobb kiberbiztonsági eseménye, az egyik előadásban élőben bemutatták a gyakorlatban is, milyen az, amikor mesterséges intelligenciával támadunk és mesterséges intelligenciával védekezünk. Bár a bemutató olyan volt, mint a 90-es években, amikor a sakkszoftvereket/robotokat játszatták egymással, azért néhány dologra így is ráirányította a figyelmet. Az első, hogy ma már mindkét oldalon demonstrálható módon működik a technológia. A második, hogy mindkét oldalon hatékonyan fel is lehet használni ezt. A harmadik pedig az, hogy a bemutatottnál fejlettebb, egy vagy néhány, de adott feladat(ok)ra fókuszáló technológiával rendelkezik mindkét oldal.

5. Összefoglalás

Összefoglalásként elmondható, hogy a felhőalapú rendszerek biztonsága sokat fejlődött az elmúlt években. Vannak azonban olyan biztonsági kérdések, amelyek vagy csak a felhőalapú rendszereknél jelennek meg, vagy ott nagyon hangsúlyosak, és ezeket a felhasználónak egy felhőalapú rendszer használatának tervezése és igénybevétele során a kockázatelemzésnél és -kezelésnél figyelembe kell vennie. Ugyanakkor a felhőalapú rendszerek és a mesterséges intelligencia terjedésével, a kiszervezések bővülésével új kockázatok is megjelennek.

Az ellátási lánc támadása korábban nem látott méreteket ölt, így az adatokat tulajdonló szervezet elemi érdeke, hogy a biztonság az ellátási lánc teljes egészében a rá vonatkozó szabályok szerint biztosított legyen. Ez pedig a korábbiaknál részletesebb, mélyebb kockázatelemzést és -kezelést igényel a felhasználóktól. Ennek módszertana még nem teljes mértékben kidolgozott, ezzel a szakembereknek még foglalkozniuk kell.

Hivatkozások

[1] Canalys: Global cloud services market Q1 2021, 2020.04.29. (Letöltve: 2021.08.31.) *https://canalys.com/newsroom/global-cloud-market-Q121*

[2] Global Cloud Computing Market, Over $287 Billion growth expected during 2021–2025. Technavio. Cision. 2021.06.05. (Letöltve: 2021.08.31.) *https://www.prnewswire.com/news-releases/global-cloud-computing-market—over—287-billion-growth-expected-during-2021-2025—technavio-301306058.html*

[3] Cloud Computing Market Size, Share & Trends Analysis Report by Service (SaaS, IaaS), by Enterprise Size (Large Enterprises, SMEs), by End Use (BFSI, Manufacturing), by Deployment, and Segment Forecasts, 2021–2028. Market Analysis report. Grand View Research. 2021.07. (Letöltve: 2021.08.31.) *https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry*

[4] Security Recommendations for Cloud Computing Providers (Minimum information security requirements), White Paper. 2011.06.22. (Letöltve: 2014.09.21.) *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.html*

[5] Daniele Catteddu (szerk.): Security & Resilience in Governmental Clouds. 2011.01. (Letöltve: 2014.11.18.) *http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds*

[6] Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai. Doktori (PhD) Értekezés, Nemzeti Közszolgálati Egyetem, 2015.

[7] FedRAMP. (Letöltve: 2021.08.31.) *https://www.fedramp.gov/documents-templates/*

[8] ENISA Threat Landscape for Supply Chain Attacks. 2021. július. (Letöltve: 2021.08.31.) *https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*

[9] Biztonságos 5G hálózatok: a Bizottság jóváhagy egy uniós eszköztárat, és meghatározza a következő lépéseket. 2020.01.29. (Letöltve: 2021.08.31.) *https://ec.europa.eu/commission/presscorner/detail/hu/ip_20_123*

[10] Dan Patterson: How AI, IoT, and big data will shape the future of cybersecurity. TechRepublic, 2018.08.13. (Letöltve: 2021.08.31.) *https://www.techrepublic.com/article/how-ai-iot-and-big-data-will-shape-the-future-of-cybersecurity/*

[11] Daniel Martin: 8 Benefits of Using AI for Cybersecurity. Cyber Management Alliance. 2021.05.04. (Letöltve: 2021.08.31.) *https://www.cm-alliance.com/cybersecurity-blog/8-benefits-of-using-ai-for-cybersecurity*

[12] Mercedes Cardona: When Bad Guys use AI and ML in Cyberattacks, What Do You Do? SecurityRoundtable.org, Powered by: Palo Alto Networks. (Letöltve: 2021.08.31.) *https://www.securityroundtable.org/when-bad-guys-use-ai-and-ml-in-cyberattacks-what-do-you-do/*

[13] DarkTrace: The Next Paradigm Shift AI-Driven Cyber-Attacks. Research White Paper, 2018. (Letöltve: 2021.08.31.) *https://www.oixio.ee/sites/default/files/the_next_paradigm_shift_-_ai_driven_cyber_attacks.pdf*

[14] Keman Huang, Michael Siegel, Keri Pearlson and Stuart Madnick: Casting the Dark Web in a New Light: A value-chain lens reveals a growing cyber attack ecosystem and new strategies for combating it. Massachusetts Institute of Technology, 2019. 06. (Letöltve: 2021.08.31.) *http://web.mit.edu/smadnick/www/wp/2019-19.pdf*

A szerzőről

KOVÁCS ZOLTÁN a Budapesti Műszaki Egyetemen szerzett diplomát a Villamosmérnöki Kar Híradástechnika szakán 1991-ben, ezt követően pedig 2004-ben mérnök-közgazdász diplomát a Budapesti Közgazdaságtudományi Egyetemen. PhD-értekezését 2015-ben védte meg a Nemzeti Közszolgálati Egyetemen. Dolgozott a Nemzetbiztonsági Szakszolgálatnál, a NISZ Zrt.-nél. Jelenleg a Vodafone Magyarország Zrt.-nél vezeti a biztonsági területet és tanít a Nemzeti Közszolgálati Egyetemen. Kutatási területe az infokommunikációs rendszerek biztonsági kihívásai.