Tóth András

Az Internet of Things rendszerek biztonsági kihívásai

Jelen tanulmány célja, hogy átfogó képet adjon az Internet of Things (IoT) eszközök és rendszerek biztonsági kérdéseiről és ezek megoldásairól. Az IoT definíciója szerint ezek az eszközök a tárgyak azon csoportjába tartoznak, amelyek összekapcsolódva infrastruktúrát vagy infrastruktúra-csoportot alkotnak, amely lehetővé teszi az összes eszköz számára, hogy összekapcsolódjanak, kezeljék és hozzáférjenek az összes általuk generált vagy gyűjtött adathoz. Az IoT minden összekapcsolt technológiai eszköz, gép és kapcsolat fogalma. Az IoT az élet minden olyan aspektusát felöleli, amely ezeket a „dolgokat" nap mint nap szabályozza és irányítja. A mobil-számítástechnika, a társadalmi hálózati technológiák fejlődése, valamint az internetes alkalmazások és szolgáltatások exponenciális növekedése miatt széles körben elterjedt és rohamosan fejlődő IoT-eszközöknek köszönhetően a szerző kiemelten fontosnak tartotta egy olyan tanulmány elkészítését, amely az IoT-rendszerek hardveres és szoftveres biztonsági megoldásainak lehetőségeivel foglalkozik. A szerző a tanulmány elkészítéséhez az elemző értékelő módszert alkalmazta, amely során megvizsgálta az IoT-elemek képességeire és védelmi lehetőségeire vonatkozó jelenleg rendelkezésre álló releváns szakirodalmat. A tudományos cikkek és művek összegyűjtéséhez a Harzing's Publish or Perish szoftvert alkalmazta, és ennek segítségével elsősorban a Google Scholar adatbázisában kereste a releváns irodalmakat, könyveket, amelyek más akadémiai keresőmotorokban nincsenek indexelve. Ezt követően megvizsgálta az Elsevier Scopus adatbázisát is, és a két adatbázisból kapott szakirodalmakat vetette össze. A duplikált irodalmak kiszűrését követően kulcsszavas szűkítéssel, mint például hardveres védelem, szoftveres védelem, nyílt kulcsú titkosítás, átvitelbiztonság, csökkentette a releváns szakirodalmak listáját. Ezt követően a már szűkített szakirodalmakat elemezve készítette el ezt az összefoglaló tanulmányt, amelynek célja az eddig elért eredmények szintetizálása volt.

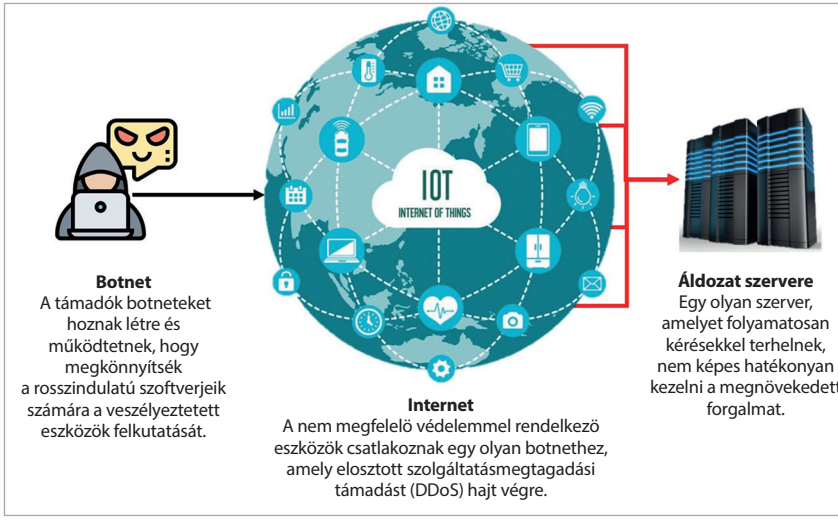
Az IoT-eszközök és -rendszerek jellemzői

Kétségtelen, hogy az átlagos háztartásokban egyre több IoT-eszköz található, és hasonló tendencia figyelhető meg az IoT ipari környezetben történő felhasználása terén is. Sajnos az IoT-eszközök nagy részét úgy építik, hogy a tervezés során kizárólag a költségek alacsonyan tartása a fő szempont, és ennek eredményeként sokuk rossz konfigurációjú és nyitott kialakítású, és ez azt is jelenti, hogy semmilyen biztonsági funkciójuk nincs, így többnyire nyitottak az internet irányába. Természetesen ezek a biztonsági problémák a hackerek figyelmét is felkeltették, hiszen nagyon könnyen támadható célpontokat jelentenek, amelyekkel akár komoly károkat is képesek okozni. Az IoT-eszközök jelentette biztonsági fenyegetés egyik legjelentősebb példája a Mirai botnet. A botnet olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást. Ezeket egész egyszerűen csak „botoknak" vagy zombi gépeknek hívjuk. Az ilyen számítógépeket többnyire valamilyen malware-rel fertőzik meg azért, hogy a távolból is irányítani lehessen őket. Egyes botnetek több százezer – esetenként több millió – számítógépből (vagy újabban okoseszközökből) állnak. A Mirai jelenlétét 2016 augusztusában leplezte le a MalwareMustDie biztonsági kutatási munkacsoport. Egyes feltételezések szerint a Mirai a qBot (más néven Qakbot) utódja. A Mirai malware eredete, valamint az elkövetők motivációja azonban továbbra is bizonytalan. A Mirai egy ELF (Executable and Linkable Format) többplatformos féregnek minősül, ezért ELF Linux/Mirai néven is ismert. Becslések szerint a forráskódjának 2016. szeptember 30-i nyilvánosságra kerülése után a Mirai botneteknek sikerült távolról majdnem félmillió IoT-eszköz felett átvenniük az irányítást, kialakítva ezzel egy hatalmas botnethálózatot. A mai napig a Mirai és változatai felelősek a legnagyobb és legkatasztrofálisabb elosztott túlterheléses támadásokért (Distributed Denial of Service, DDoS), többek között a Brian Krebs számítógépes biztonsági újságíró honlapja, a francia OVH webtárhely és a Dyn elleni támadásokért.[1] A Dyn internetes címtárszolgáltatásait érintő támadások eredményeképpen az Egyesült Államok keleti partján leállt a DNS-szoltáltatás, aminek következményeként több tízmillió IP-cím vált elérhetetlenné (olyan weboldalaké is, mint a Twitter, The Guardian, Netflix, Reddit, CNN). Ezenkívül számos másik, viszonylag kisebb méretű DDoS-támadást hajtottak végre a Mirai botnetek segítségével más célpontok, többek között lakossági IP-címek és játékszerverek ellen.[2] A Trend Micro cég elemzése alapján elmondható,

[1] Kambourakis–Kolias–Stavrou 2017: 267.

[2] Newman 2016.

hogy több százezer Mirai által megfertőzött IoT-eszköz vett részt a támadásban. A támadás mechanizmusát az 1. ábra szemlélteti.



1. ábra: A Mirai által fertőzött IoT-eszközökkel elkövetett támadás vázlata
Forrás: Trend Micro: *2017 Midyear Security Roundup: The Cost of Compromise (a szerző szerkesztése),* 2017.

A fenti mellett számos olyan eset történt, amely azt bizonyítja, hogy az IoT-eszközöknek és -rendszereknek komoly biztonsági réseik vannak[3], és ezzel nagy fenyegetést jelentenek mind a civil, mind az ipari, illetve a közigazgatási, az állami és a védelmi szektorra is.[4] Napjainkban már több milliárd olyan IoT-eszköz csatlakozik az internetre, amelynek gyakorlatilag semmilyen védelmi megoldása nincs. Ennek megfelelően a legnagyobb információ- és kiberbiztonsággal foglalkozó cégek és projektek már évekkel ezelőtt megkezdték az erre a veszélyre figyelmeztető dokumentumok kidolgozását. A Symantec Internet Security Threat Report tanulmánya szerint a legjelentősebb kihívások a következőkben foglalhatók össze:

– az IoT-eszközök nem megfelelő szoftvertesztelése és -frissítése, mind a gyártási, mind pedig a végfelhasználói üzemeltetési folyamatban;

[3] Trend Micro 2017: 286.
[4] Farkas 2020: 281–289.

- kitettség az alapértelmezett jelszavak kihasználását célzó brute-force támadásoknak;
- az IoT-eszközöket a számítógépes rendszerekbe behatolás eszközeként használó malware- és zsarolóprogram-támadások;
- a kriptovalutákat célzó botnetek, amelyek használata robbanásszerűen megnőtt, különösen az elmúlt világjárványos évben;
- adatbiztonság és adatvédelem (mobil, web, felhő);
- az adatbiztonság és adatvédelem elleni támadások;
- a mesterséges intelligencia elemeinek használata és kihasználása;
- távoli hozzáférés a hálózati architektúrán belüli erőforrásokhoz az IoT-eszközökön keresztül.[5]

Az Open Web Application Security Project (OWASP) – Internet of Things Project célja, hogy segítsen a gyártóknak, a fejlesztőknek és a rendszeres felhasználóknak jobban megérteni a tárgyak internetével kapcsolatos biztonsági kérdéseket. A projekt lehetővé teszi, hogy a bármilyen kontextusban tevékenykedő felhasználók a legjobb biztonsági döntéseket hozzák meg az IoT-technológiák építése, bevezetése vagy értékelése során. A projekt célja, hogy struktúrákat határozzon meg különböző alprojektekhez, amelyek az IoT-eszközökre is kiterjedhetnek. 2018-ban a projekt keretében közzétették az IoT sérülékenységével és biztonságával kapcsolatos tíz legfontosabb szempontot. Ez a kiadvány tartalmazza a legfontosabb és a legtöbbször előforduló sérülékenységeket egy adatbázisba rendezve, valamint bemutatja azokat a támadási felületeket, amelyek a leginkább kitettek ezeknek a veszélyeknek. A jelentést Kovács László magyarosította *A kibertér védelme* című könyvében. E könyv alapján a legfontosabb IoT-sérülékenységeket az 1. táblázat foglalja össze[6].

1. táblázat: IoT-sérülékenységek az OWASP alapján

Sérülékenység	Támadási felület	Összegzés
Felhasználónév-számlálás	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Valós felhasználónevek gyűjtésének képessége a hitelesítési mechanizmussal kölcsönhatása kihasználásával

[5] Symantec 2018.
[6] Kovács 2018: 93.

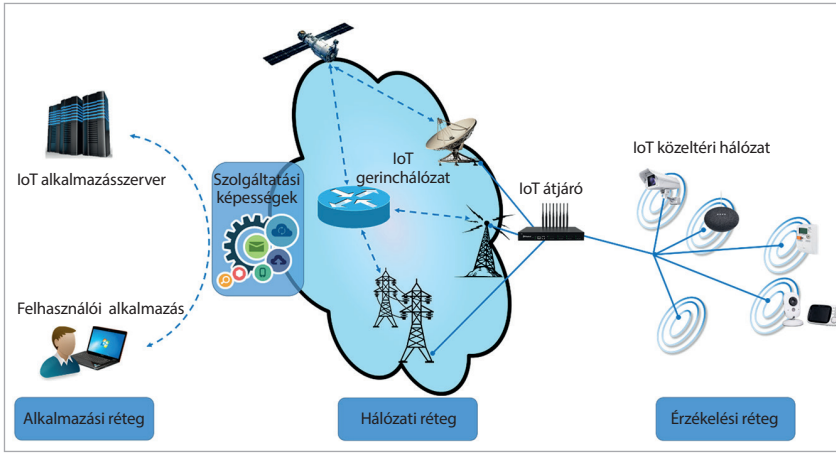
Sérülékenység	Támadási felület	Összegzés
Gyenge jelszavak	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	A fiók jelszavait például „1234” vagy „123456”-ra állíthatja. Előre programozott alapértel mezett jelszavak használata
Fiók kizárása	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Lehetőség a hitelesítési kísér letek tovább küldésére 3−5 bejelentkezési kísérlet után
Titkosítatlan szolgáltatások	Eszközhálózati szolgáltatások	A hálózati szolgáltatások nem megfelelően titkosítottak, így nem akadályozzák meg, hogy a támadók lehallgassák vagy manipulálják a hálózatot/adatokat.
Kétfaktoros hitelesítés	Felügyeleti interfész Cloud webes felület Mobilalkalmazás	Kétszeres hitelesítési mechanizmusok hiánya, például token- vagy ujjlenyomat-szkenner
Gyenge titkosítás	Eszközhálózati szolgáltatások	A titkosítás végrehajtása hely telenül van beállítva, vagy nem megfelelően frissül, például az SSL v2 használatával.
Frissítés titkosítás nélkül	Frissítési mechanizmus	A frissítéseket TLS-használata vagy a frissítési fájl titkosítása nélkül továbbítják.
Frissítés írható helyre	Frissítési mechanizmus	A frissítési fájlok tárolási helye bárhonnan írható, amely lehetővé teszi a firmware módosítását és elterjesztését az összes felhasználó számára.
DoS	Eszközhálózati szolgáltatások	A szolgáltatás megtámadható túlterheléses támadással.
A tárolóeszköz eltávolítása	Készülékfizikai interfészek	Az adathordozó fizikailag eltávolítható az eszközből.
Nincs kézi frissítési mechanizmus	Frissítési mechanizmus	Nincs lehetőség az eszköz fris sítésének kézi ellenőrzésére.
Hiányzó frissítési mechanizmus	Frissítési mechanizmus	Az eszköz frissítésére nincs lehetőség.
Firmware verzió megjelenítése és/vagy utolsó frissítés dátuma	Eszközfirmware	A jelenlegi firmware-verzió és/vagy az utolsó frissítési dátum nem jelenik meg.

Sérülékenység	Támadási felület	Összegzés
Firmware és tároló extrakció	Szervizinterfész Labormérés OTA-frissítés lehallgatása Letöltés a gyártó weboldaláró eMMC-lehallgatás Az SPI Flash/eMMC chip törése és adapterben olvasása	A firmware sok hasznos információt tartalmaz, például a forráskódot és a futó szolgáltatások bináris kódjait, előre beállított jelszavakat, SSH-kulcsokat stb.
A készülékkód végrehajtási folyamatának manipulálása	Szervizinterfész Oldalsócsatorna-támadások	Különböző csatlakozásokon keresztül módosíthatjuk a készülék firmware-ének végrehajtását, és szinte az összes szoftveralapú biztonsági vezérlőt megkerülhetjük. Az oldalcsatornás támadások módosíthatják a végrehajtási folyamatot is, vagy információkat szerezhetnek meg az eszközről.
A konzol elérése	Soros interfészek	Soros interfészhez való csatlakozás esetén teljes konzol-hozzáférés szerezhető egy eszközhöz. Általában a biztonsági intézkedések magukban foglalják az egyéni rendszerindító eszközöket, amelyek megakadályozzák a támadó egyetlen felhasználói módba való belépését, de így azt is megkerülhetik.
Nem biztonságos külső gyártók	Szoftverek	Elavult Open SSL, SSH, webszerverek stb.

Forrás: OWASP: Internet of Things Top 10 (Kovács László szerkesztése), 2019.

Az IoT-környezet egy adott cél érdekében együttműködő, tudatos, intelligens rendszer, az érzékelési, az alkalmazási és a hálózati rétegeken lép kölcsönhatásba, ami egyfajta nyílt hálózatot alkot. Ezért kell lennie valamilyen biztonsági architektúrának, hogy megvédje az ezeket használó egyéneket, vállalatokat. E bárki által használt IoT-eszközök biztonsága rendkívül fontos, mivel sok ilyen eszközt rosszindulatú módon használnak fel. A szakemberek nagyon sok esetben eltérő véleményt fogalmaznak meg arról, hogy hol kell prioritásként kezelni a tárgyak internetét, de egy dolog közös bennük: a biztonság a legfontosabb. Arra már több korábbi kutatás is rámutatott, hogy néhány régi technika már nem hatásos az IoT-k esetében, mivel azok némileg különböznek a hagyományos hálózatoktól. Ennek megfelelően modern taktikákat és technikákat kell alkalmazni e széles körben elterjedt nyílt

architektúrák védelmére. Ezeknek a megoldásoknak az IoT-architektúra minden szintjén meg kell jelennie.[7] Az IoT-rétegek esetében több különböző elképzelés is van, a szerző ebben a kéziratban a háromrétegű IoT-architektúra elrendezését veszi figyelembe, amelynél a három réteg az alkalmazás, a hálózati és az érzékelési réteg. Az IoT-architektúra elvi felépítését a 2. ábra szemlélteti.



2. ábra: Az IoT-architektúra elvi felépítése
Forrás: a szerző szerkesztése

A képen látható IoT-architektúra egy olyan ígéretes technológiát képvisel, amelynek célja az emberek életminőségének javítása a mindennapi tevékenységeiket megkönnyítő új alkalmazások létrehozásával. Az IoT-rendszereknek számos közös jellemzőjük van:

- Nagy méretezhetőség: az IoT-eszközök száma milliárdos nagyságrendben növekszik. Ezt a nagy méretű eszközhálózatot úgy kell irányítani, hogy az eszközök kommunikálhassanak egymással. Ezenkívül ez a nagy méretű hálózat hatalmas mennyiségű adatot generál, ez pedig kritikus problémát jelent az adatok értelmezésével és elemzésével kapcsolatban.
- Intelligencia: a kifinomult szoftveres algoritmusok és a hardver kombinálása lehetővé teszi az IoT-eszközök intelligenssé válását. Ezek az intelligens képességek lehetővé teszik az IoT-eszközök számára, hogy

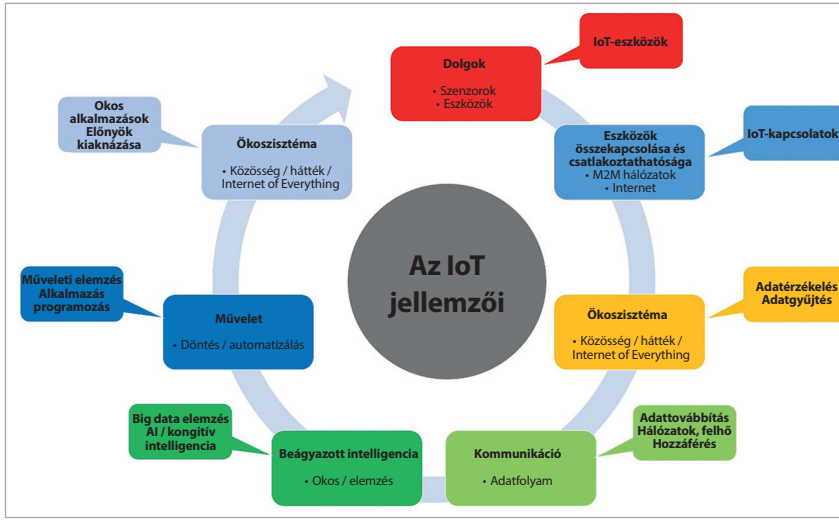
[7] Rizvi–Kurtz–Pfeffer–Rizvi 2018: 163–168.

különböző helyzetekben intelligens döntéseket hozzanak, és intelligens módon lépjenek kapcsolatba más kommunikáló eszközökkel.

- Érzékelés: az érzékelők az IoT-rendszer fő részei, alaprendeltetésük a környezet változásainak érzékelése és minden ezzel kapcsolatos adat gyűjtése és továbbítása. A szenzorok a különböző érzékelési technológiák segítségével érzékelik a közvetlen környezetükben végbe ment minden változást, ezzel növelik az emberi tudatosságot a fizikai világról.
- Csatlakoztathatóság: az IoT-rendszer egyik fő jellemzője, hogy képes összekapcsolni a különböző jellemzőjű eszközöket, és felhasználni az összegyűjtött információikat újszerű alkalmazások és szolgáltatások létrehozására. Ehhez jellemzően az úgynevezett gépek közötti kommunikációt alkalmazza (machine-to-machine, M2M).
- Komplex rendszer: az IoT-rendszer több milliárd, különböző hardver- és szoftverképességű objektumból áll, és ez jelentősen megnehezíti a menedzsmentfolyamatokat, különösen a memóriával, energiával és idővel kapcsolatos korlátok miatt.
- Heterogenitás: az IoT-rendszer több milliárd eszközt foglal magában, amelyek operációs rendszerek, platformok, kommunikációs protokollok szempontjából heterogének. Ezek a heterogén jellemzők bonyolult feladattá teszik a kezelési műveleteket az IoT-infrastruktúrákban.
- Dinamikus környezet: az IoT-rendszerek képesek összekapcsolni a környezetünk szinte minden tárgyát anélkül, hogy meg kellene határozni a kialakított hálózatok határait, ezáltal egy dinamikus rendszer alakítható ki. Emellett az IoT-eszközök a változó körülmények és helyzetek alapján dinamikusan működhetnek és módosíthatók.
- Önkonfiguráció: az általános infokommunikációs eszközöket jellemzően egy bizonyos művelet elvégzésére konfigurálják, ezzel ellentétben az IoT-eszközök képesek az önkonfigurálásra, ami lehetővé teszi számukra, hogy emberi beavatkozás nélkül működjenek. Az eszköz gyártójával együttműködve az IoT-eszközök a felhasználó közreműködése nélkül konfigurálhatják magukat a részükre megküldött szoftverfrissítéseknek megfelelően.
- Egyedi azonosíthatóság: az IoT-hálózaton belül minden IoT-objektumot egyedi azonosító, például IP-cím segítségével azonosítanak és ismernek fel. Ezenkívül ezeknak az eszközöknek olyan interfészeik vannak, amelyek lehetővé teszik a felhasználók számára, hogy összegyűjtsék a szükséges információkat az eszközökről, rögzítsék állapotukat és távolról kezeljék őket.

– Hatalmas mennyiségű adat: az IoT-eszközök száma milliárdos nagyságrendű, és ezek az eszközök az alaprendeltetésüknek megfelelően folyamatosan gyűjtik az információkat a környezetükből, így hatalmas mennyiségű adatot generálnak, amely az úgynevezett Big Data egyik forrása.
– Környezettel kapcsolatos tudatosság: egy-egy IoT-környezetben több érzékelő is megtalálható, amelyek érzékelik a környezetüket, összegyűjtik és tárolják a szükséges információkat, továbbá ezek az érzékelők a gyűjtött adatok alapján hozhatnak döntéseket, ami tudatossá teszi őket a környezetükben megjelenő információkkal kapcsolatban.
– Korlátozott energia: a legtöbb IoT-eszköz kicsi és könnyű, és erőforrásaik jellemzően korlátozottak, ezért úgy tervezték őket, hogy minimális energiafogyasztással működjenek.[8]

A fenti jellemzők szemléltetésére és könnyebb megértése céljából a 3. ábrán szemléltetjük a különböző szegmensek jellemzőit az IoT-rendszereknél.



3. ábra: Az IoT jellemzői
Forrás: a szerző szerkesztése

[8] Atlam–Wills 2019: 127.

Az egyre fejlettebb technológia megoldások lehetővé teszik, hogy az IoT-eszközökben beágyazott intelligencia legyen, amely azt jelenti, hogy a rendszerben megtalálható minden fizikai tárgynak beágyazott számítástechnikai és kommunikációs képességei vannak, hogy képesek legyenek érzékelni a környezetüket, az abban végbemenő változásokat, és az alkalmazott eszközök tudjanak kommunikálni egymással a szolgáltatások nyújtása érdekében. Ezeket az intelligens összeköttetéseket és az interoperabilitást nevezzük IoT-nek vagy gép-gép (M2M) kommunikációnak.

Maede Zolanvari és szerzőtársai vizsgálták meg az IoT-eszközök hálózati sérülékenységeit, és az információbiztonsági alapelveknek megfelelően azonosították be őket úgy, mint bizalmasság, sértetlenség és rendelkezésre állás. Mindezek mellett vizsgálták még a hitelesítés és a jogosultságkezelés kérdésköreit is, amelyek szintén kiemelt szerepet játszanak az információk megóvásában, illetéktelen kezekbe kerülésének megelőzésében. Kutatásuk során megállapították, hogy a bizalmasságra a legnagyobb fenyegetést a puffertúlcsordulás, a kódbefecskendezés és a hibás bemeneti érvényesítés jelentik. A sértetlenségre a legnagyobb hatással a felderítés van, míg a rendelkezésre állást a túlterheléses támadások fenyegetik a legjobban. A hitelesítés esetében a legnagyobb problémát az illetéktelen hozzáférés és a közbeékelődéses (man-in-the-middle, MiTM) támadások jelentik, míg a jogosultságkezelésnél a legfenyegetőbb támadások a könyvtárkeresztezés alapú jelszófeltörő támadások, valamint a hátsó kapuk. Az egyes támadási formák jellemzőit a 2. táblázat szemlélteti.

2. táblázat: Az IoT-rendszerek jellemző támadási vektorai

Támadási vektor	Jellemzők
Puffertúl-csordulás	A puffertúlcsordulásos támadások során a behatoló megpróbál nagy mennyiségű (a kijelölt méretnél nagyobb) adatot írni a pufferbe, ami a pluszbitek túlcsordulását és más pufferek felülírását, valamint azok értékének megváltoztatását okozza. Ez a támadás általában a rossz bemeneti típus- vagy méretérvényesítési mechanizmusok miatt következik be, és a rendszert megbízhatatlanná teszi, vagy akár össze is omolhat.

Támadási vektor	Jellemzők
Kódbefecskendezés	A kódbefecskendezéses támadás során a behatoló rosszindulatú parancsokat próbál végrehajtani vagy rosszindulatú adatokat juttat a rendszerbe. Például egy SQL (Structured Query Language) injekciós támadásban SQL-lekérdezéseket küldenek az adatbázis-kiszolgáló irányítására vagy veszélyeztetésére. Ez a támadás kihasználja a rendszer sebezhetőségét a felhasználó által megadott bemeneti adatok érvényesítési technikáinak hiánya miatt. Ez a támadás lehetővé teszi a behatoló számára, hogy hozzáférjen érzékeny információkhoz, például felhasználónevekhez és jelszavakhoz, valamint megváltoztassa az adatokat (például engedélyezi a hozzáférést egy illetéktelen felhasználó számára, törli az adatokat stb.). A parancsbefecskendezéses támadás manipulálhatja a rendszerben lévő vezérlőparancsokat, és megzavarhatja a normál működést.
Hibás bemeneti érvényesítés	Ez a sebezhetőség a felhasználói bemenet érvényesítésére szolgáló megfelelő mechanizmusok hiányával függ össze. Ez egy általánosabb típusú sebezhetőség, amely más típusú kockázatokhoz vezethet. A támadó képes lehet rossz értékek bevitelére, ami instabillá teheti a rendszert. Ráadásul mivel ezeket a rendszereket determinisztikus jellegük miatt nem ellenőrzik rendszeresen, ez a támadás hosszú ideig észrevétlen maradhat.
Felderítés	A felderítő támadás során a behatoló kapcsolatba lép az IoT-hálózattal, hogy információkat gyűjtsön a rendszerről, például a csatlakoztatott eszközökről, biztonsági irányelvekről, IP-címekről, állomásinformációkról stb. A hálózat elemeinek azonosítása után a támadó feltérképezi a hálózati architektúrát, hogy azonosítsa a rendszer sebezhetőségeit. Végül a támadó ezeket az információkat felhasználhatja arra, hogy a rendszer működésének megszakítása érdekében exploitokat futtasson az arra fogékony eszközök ellen. A behatolók ezt a támadást szimatolási funkciókkal indíthatják. Lehallgatják, és megvizsgálják a folyamatban lévő hálózati forgalmat, hogy információt szerezzenek a hálózati elemekről és azok állapotáról.
Túlterheléses támadások	A támadó DoS-támadást hajt végre a célzott eszközök és rendszerek elárasztására. Ez a támadás megzavarja az IoT-rendszer rendelkezésre állását azáltal, hogy nagyszámú véletlenszerű csomagot küld a célzott csomópontnak nagy sebességgel, ezáltal a célpont nem lesz képes reagálni, aminek következményeképpen akár össze is omolhat az egész rendszer. Az IoT-rendszer elleni DoS-támadást általában a hálózathoz csatlakozó támadó hajtja végre, aki SYN- vagy HTTP-áradatot használ egy állomás ellen.
Illetéktelen hozzáférés	Ez a sebezhetőség az IoT-rendszerek gyenge hitelesítési mechanizmusainak köszönhető. Mivel ezek a rendszerek folyamatosan és önállóan működnek, a személyzet nem feltétlenül változtatja meg rendszeresen a felhasználóneveit és jelszavait. A könnyebb megjegyezhetőség érdekében akár alapértelmezett felhasználóneveket és jelszavakat is használhatnak. Az információ megszerzésére brute-force módszereket vagy a felhasználó billentyűleütéseinek naplózását lehet használni. Ezenkívül széles körben folytatnak adathalász támadásokat az üzemeltetők hitelesítő adatainak összegyűjtésére. Ha a támadó valahogyan rájön ezekre a hitelesítő adatokra, visszaélhet a hozzáféréssel, és más típusú támadásokat hajthat végre.

Támadási vektor	Jellemzők
Közbeékelődéses támadás	A közbeékelődéses támadás során a behatoló lehallgatja a kommunikációs kapcsolatokat, és megpróbálja kompromittálni a két csomópont közötti üzeneteket, miközben a csomópontok azt hiszik, hogy még mindig közvetlenül beszélnek egymással. A támadó továbbá eldobhatja vagy manipulálhatja az üzeneteket.
Könyvtárkeresztezés	Ebben a támadásban a behatoló megpróbál hozzáférni a korlátozott könyvtárakhoz vagy fájlokhoz, amelyekhez elvileg csak rendszergazdai hozzáféréssel lehet hozzáférni. Ez a sebezhetőség a felhasználó által megadott bemenetek rossz szűrési vagy érvényesítési mechanizmusainak köszönhető. A könyvtárak listázásának rossz ellenőrzése egy másik oka ezeknek a támadásoknak. Az ilyen típusú támadás során a támadó érzékeny fájlokat és információkat tud letölteni a rendszerből. Ez a támadás gyakran az IoT-rendszerek más biztonsági területeit is veszélyezteti, például a titkosságot, mivel a támadó hozzáférhet a rendszerben lévő privát fájlokhoz. A megfelelő bemenetérvényesítési módszerekkel megelőzhető ez a fajta támadás.
Hátsó kapuk	A hátsó kapus támadás során a támadó megpróbálja megkerülni a hitelesítési folyamatot, hogy bejusson a rendszerbe. A hátsó kapus hozzáférésen keresztül a támadó bejelentkezhet a rendszerbe, elérheti a rendszerben lévő összes adatot és fájlt, és parancsokat futtattathat le. A hátsó kapu telepítését az áldozat rendszerére akár egy bennfentes végezheti, de az IoT-k esetében nagyon sokszor előfordul, hogy a gyártó már a gyártási folyamat során elhelyezett valamilyen hátsó kaput az eszközön. A telepítést követően nagyon nehéz észlelni ezt a fajta támadást, és rendkívül veszélyes, mivel a támadónak teljes hozzáférést biztosít a rendszerhez.

Forrás: Zolanvari et. al. 2019 alapján a szerző szerkesztése

Az adatvédelmi és jogi kockázatok

A 2010-es évek vége előtt lényegesen kisebb figyelmet fordítottunk a személyes adataink védelmére. Ez nem csak állampolgári szinten volt így, hanem az államigazgatás és a munkáltató oldalán is, mivel a jogszabályok lényegesen szűkebb köre szabályozta a személyes adatok védelmét. Magyarországon kezdetben az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról foglalkozott a személyes adatok védelmével, azonban az új technológiák elterjedésével ez a 2010-es évek elejére elavulttá vált. Ennek következtében 2011. július 11-én az Országgyűlés elfogadta a 2011. évi CXII. törvényt az információs önrendelkezési jogról és az információszabadságról, amely onnantól kezdve egyedüli jogszabályként szabályozta a személyes adatok védelmét. Ennek kiküszöbölésére az Európai Unió és hazánk is komoly

szabályozói környezet kialakítására törekedett az elmúlt években. Ez szintén igaz az IoT-eszközök területére is, hiszen az IoT-szolgáltatások alkalmazása során számos olyan adat keletkezik, amely jellegéből adódóan érzékeny adatnak minősül (például személyes adat). A legnagyobb problémát az jelenti az ilyen eszközök alkalmazása során, hogy azok folyamatosan figyelik a környezetüket és gyűjtik az adatokat, ennek megfelelően rengeteg információjuk van például a viselőjükről. Alaprendeltetésből adódóan az így keletkezett adatoknak a tulajdonosa maga a felhasználó, azonban semmi nem garantálja, hogy az eszközök gondatlan hibái miatt ezek az adatok nem kerülnek harmadik fél kezébe.[9] Szintén kihasználhatók lehetnek az eszközökön alkalmazott gyenge szoftveres védelmek, amelyeket megkerülve a támadó könnyedén hozzáférhetnek olyan információkhoz, amelyek komolyan sértik a személyes szféránkat. Emellett komoly kihívást jelent a nem megfelelő felhasználói biztonságtudatosság, ami szintén hozzájárulhat a támadók sikereihez, hisz nagyon sokan még az alapvető biztonsági beállításokat sem kapcsolják be egy-egy általuk használt okoseszköz esetében.[10]

Az uniós szabályozás

Az Európai Bizottság SWD(2016) 110 final „A tárgyak internetének előmozdítása Európában" című dokumentuma alapján Európa jövőbeli digitális ipari ereje attól függ, hogy az ipar képes lesz-e megragadni a digitális innováció szélesebb körű elterjedéséből adódó lehetőségeket. Tekintettel Európa akkori erősségeire a vertikális piacokon, a Bizottság megállapítása szerint a tárgyak internetének fejlődése egyedülálló lehetőséget kínál Európa számára, mivel az új digitális értékláncok létrehozásához és megerősítéséhez vezethet Európában, ami befektetőket és innovátorokat vonz. Az összes ipari ágazat digitalizálása fontos az erős európai ipari bázis megtartásához, valamint az átalakuló értékláncok és üzleti modellek kezeléséhez. A digitalizáció és a tárgyak internetének használata például alapvető fontosságú az intelligens mezőgazdaság vagy az élelmiszerek nyomonkövethetőségének és biztonságának fejlesztése szempontjából. Az Európai Bizottság szerint az IoT elfogadásának legfőbb kihívása

[9] Bányász–Bóta–Zágon 2019: 23.
[10] Megyeri 2018: 67.

a felhasználók bizalma – magán-, üzleti vagy kormányzati használat esetén egyaránt. E tekintetben a következő kihívásokkal kell szembenézni:

- kontextusalapú biztonság és magánélet biztosítása, amely tükrözi a különféle fontossági szinteket (például vészhelyzeti válság, otthoni automatizálás);
- szükséges számítási kapacitás olyan kifinomult biztonsági védelmi megoldások megvalósításához, mint a megbízható számítástechnika vagy a kriptográfia a kiberfizikai rendszerekben és az IoT-hardverekben;
- mind a felhasználók, mind az eszközök megbízható azonosítása egy elosztott környezetben, ahol az irányítási struktúrák nem mindig egyértelműek;
- a profilozással kapcsolatos adatvédelmi szabályok betartása. Összefüggések és információkeresés, amelyek támogathatják az új típusú biztonsági mechanizmusokat, de engedélyezik a behatolási profilokat is;
- mind a felhasználói adatok, mind a protokoll metaadatainak anonimizálása kihívást jelent egy elosztott és mobil környezetben az adatgyűjtés és -feldolgozás során;
- több milliárd IoT-eszköz skálázhatósága, valamint a csatlakoztatott rendszerek, a kommunikációs technológiák és az erőforrás-korlátozások szélesebb heterogenitásának elsajátítása;
- biztonságos telepítési és konfigurációs módszerek az IoT számára, mivel a telepítőeszközök és -szoftverek lehetséges támadási felületet jelentenek a hardverobjektumokhoz és az alkalmazásokhoz;
- a kritikus infrastruktúrák és az IoT használata ott, ahol az új technológiák és eszközök az otthoni és a mindennapi életben új biztonsági vagy adatvédelmi problémákat vethetnek fel;
- a piaci érdekek összecsapása mint üzleti szempontból az IoT egyik vonzó képessége, lehetősége a bevétel növelése érdekében a különféle forrásokból származó adatok gyűjtése és korrelálása révén.[11]

Az EU-ban a 2018-tól alkalmazandó általános adatvédelmi rendelet (2016/679) kötelezővé teszi a „beépített és alapértelmezett adatvédelmet". Mivel ezeknek az elveknek az alkalmazására vonatkozó iránymutatások kialakítása még mindig folyamatban van, ezért nem teljesen világos, hogy elég nagy lesz-e a hatályuk ahhoz, hogy lefedje a tárgyak internetének tervezési biztonságával kapcsolatos

[11] European Commission: Advancing the Internet of Things in Europe. 29.

kihívásokat.[12] Ha a tervezési és alapértelmezett adatvédelemre vonatkozó iránymutatások nem terjednek ki a „tervezési biztonság" elvére, akkor hosszabb időt vehet igénybe, amíg az EU új jogszabályokat fogad el a tárgyak internetének tanúsítási rendszerére vonatkozóan, amint azt az Európai Bizottság jelezte.

Az Európai Parlament és a Tanács 2019-ben fogadta el a 2019/881 számú rendeletét az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). A jogszabály a 2. cikkében az infokommunikációs technológia (IKT) termékeit egy hálózat vagy információs rendszer elemeként vagy elemcsoportjaként azonosítja, az IKT-szolgáltatást pedig olyan szolgáltatásként határozza meg, amely teljes egészében vagy nagyrészt információk hálózati és információs rendszerek segítségével történő továbbításából, tárolásából, lekérdezéséből vagy feldolgozásából áll. A cikk az IoT fogalmát a bevezetésében határozza meg, amelyet követve megállapítható, hogy az IKT-termékek és -szolgáltatások valóban részei az IoT rendszerének, és az IoT eszközei az IKT termékek egy részhalmazát alkotják. Ezen túlmenően a kiberbiztonsági stratégia több preambulumbekezdése kifejezetten említi a tárgyak internetét. A második preambulumbekezdés különösen úgy véli, hogy a tervezésen alapuló biztonság elvének elégtelen alkalmazása akadályozza az IoT-elemek és -rendszerek megfelelő kiberbiztonsági képességének kialakítását: e tekintetben a tanúsítási rendszerek korlátozott alkalmazása hozzájárul az információs aszimmetriákhoz, amelyek a nagyban hozzájárulnak a fogyasztók IKT-termékek, -folyamatok és -szolgáltatások általános biztonságával kapcsolatos elégtelen ismereteinek fennállásához. Ami a biztonsági célkitűzéseket illeti, a jogszabály 51. cikke nem csupán a klasszikus számítógép- és információbiztonsági elveket, azaz a CIA-triász (confidentiality, integrity and availability – bizalmasság, sértetlenség, rendelkezésre állás) és a hitelesítés elvét tartalmazza, hanem a tanúsítási rendszerek céljait is kiterjeszti a kiberbiztonság olyan kiemelten fontos területeire, mint a sebezhetőségek kezelése, a digitális igazságügyi szakértői alapelvek, a katasztrófa utáni helyreállítás, a tervezési és alapértelmezett biztonság, valamint a szoftver- és hardverfrissítések. Ez a rendelkezés rendkívül fontos az összekapcsolt termékek biztonsági hiányosságainak kezelése szempontjából az egységes piacon, mivel alapvető szempontokat

[12] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), 78. pont.

határoz meg a magánszektor számára a (tárgyak internetére épülő) rendszerek robusztusságának garantálásához.[13]

Az Európai Bizottság 2020 decemberében kiadta „Az EU kiberbiztonsági stratégiája a digitális évtizedre" című dokumentumot, amely meghatározza és elmélyíti azt a nézetet, amivel elismeri, hogy a kiberbiztonság javítása alapvető fontosságú egyrészt az innováció, az összekapcsolhatóság és az automatizálás iránti bizalom eléréséhez. Mindezek mellett hozzájárul az ezekből származó előnyökhöz, másrészt az alapvető jogok és szabadságok védelméhez, beleértve a magánélethez és a személyes adatok védelméhez való jogot, valamint a szólás- és információszabadságot.[14]

A Bizottság mindezek mellett kiemelt figyelmet fordít a tárgyak internetére vonatkozó műszaki biztonsági szabványok kialakítására és alkalmazási köreire, mivel az interoperabilitás hiánya minden bizonnyal a legkényesebb akadály, amely még mindig akadályozhatja az IoT-rendszerek teljes megvalósulását. A Bizottság 2021-ben megfogalmazott terveiben kiemelt intézkedésként javasolta egyrészt a termékek kiberbiztonsági megfelelőségére vonatkozó európai szabvány kidolgozását, amely összhangban van az ISO 27000 család jelenlegi információbiztonsági megfelelőségi keretrendszerével és a GDPR-ral; másrészt javasolta, hogy a szabványt a hálózat- és információbiztonságról szóló (Network and Information Security) irányelvben meghatározott követelmények harmonizálására kell használni. Jelenleg az EU-n belül három kiemelt, az IoT-rendszereket érintő projekt van fejlesztés alatt:

- közös kritériumokon alapuló uniós kiberbiztonsági tanúsítási rendszer (EU Cybersecurity Certification Scheme on Common Criteria – EUCC);
- a felhőszolgáltatások uniós kiberbiztonsági tanúsítási rendszere (EU Cybersecurity Certification Scheme on Cloud Services – EUCS);
- és az 5G-re vonatkozó rendszer.[15]

A jelenleg hatályos uniós jogszabályi háttér kitér a nemzeti szabályozás kereteinek meghatározására is, amelyek alapján megköveteli, hogy a kormányok

[13] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), 51. cikk.

[14] Európai Bizottság: Közös Közlemény az Európai Parlamentnek és a Tanácsnak, Az EU kiberbiztonsági stratégiája a digitális évtizedre. 4.

[15] Chiara 2022: 122.

támogassák a tárgyak internetének biztonságos és megbízható fejlődését lehetővé tevő szélesebb körű intézményi megoldásokat. A biztonság vagy a beépített adatvédelem olyan széles körű területek, hogy a tárgyak internete szabályozásában nem lehet kizárólag felülről lefelé irányuló intézkedésekre támaszkodni. A kormányoknak alaposabban meg kellett vizsgálniuk a politikai eszköztárukat, és lényegesen markánsabb szabályozói környezetet kellett kialakítaniuk, amelyek képessé teszik a magán- és közintézmények intézményi kapacitását a gyorsan változó biztonsági és adatvédelmi kihívásokra való koordinációra és alkalmazkodó reagálásra. Ezért a kormányoknak figyelembe kell venniük szélesebb körű szervező és mozgósító szerepüket annak érdekében, hogy aktiválják a hálózatokat a nyilvános problémamegoldás érdekében. Ez azt jelenti, hogy olyan képzési programokat kell létrehozni, amelyek biztosítják a megfelelő felkészítést az adatminimalizálás, valamint az információ- és hálózatbiztonság terén. Ezeknek semmiképpen sem szabad csak a kormányzati megrendelések szolgáltatóit megcélozni, hanem a kis- és közepes méretű szervezetek részére is elérhetővé kell őket tenni, amelyek nem tudják könnyen fedezni a tárgyak internetének egyedi kockázataihoz szükséges kiberbiztonsági intézkedések bevezetésének és korszerűsítésének költségeit. Emellett a kormányok egyszerűsíthetik a magánvállalkozások és az összekapcsolt kiber- és fizikai infrastruktúrák biztonságával foglalkozó kormányzati szervek közötti információmegosztási mechanizmusokat. A kormányok pozitív hatású kezdeményezésekkel ösztönözhetik az információbiztonsági rendszerek szélesebb körű bevezetését a magánszektorban, ezek az intézkedések pedig lehetővé tehetik a biztosítási piac számára, hogy jobban felmérje a kitettséget és modellezze a kiberbiztonsági kockázatokat. Mindezek az intézkedések jelentős változásokra utalnak a kockázatkezelésben és a biztonsági kultúrák területén a magán- és a közszférában.[16]

Nemzeti szabályozás

Magyarország Alaptörvénye VI. cikk (2) bekezdése szerint „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez." Az alaptörvény szintén kimondja, hogy „Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme

[16] Brass et al. 2017: 13.

érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható." A garanciális elvek érvényesítése érdekében az alaptörvény rendelkezik arról, hogy fenti információs alapjogok érvényesülését független hatóság ellenőrzi (Nemzeti Adatvédelmi és Információszabadság Hatóság – NAIH).

Magyarországon az IoT-eszközöket érintő első jelentősebb szabályozás a kormány által 2012-ben elfogadott Magyarország Nemzeti Biztonsági Stratégiája volt, amely kimondta, hogy javítani kell az elektronikus közszolgáltatások információbiztonságát, a kritikus infrastruktúrát és a kibervédelmi képességeket, valamint kiemelt feladatként jelölte meg a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását. A stratégiát 2020-ban váltotta fel a 1163/2020. (IV. 21.) számú kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról, addig az első stratégia határozta meg azokat az elveket, amelyeket az IoT-rendszerek kialakítása esetében stratégiai szinten be kellett tartani. Az új biztonsági stratégia szintén komoly hangsúlyt fektet a kulcsfontosságú infokommunikációs rendszerek védelmére, valamint a felhasználók biztonságtudatosságának fokozására, amely a kiberincidensek megelőzésének egyik kulcseleme. Kiemelt problémaként azonosítja az információk tömeges rendelkezésre állását, amit megfelelő technológiai megoldásokkal tudnia kell kezelni a szakembereknek.[17]

A következő lépés ezen az úton a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013 (III. 21.) kormányhatározat volt, amely fő célkitűzései az incidensjelentési és reagálási képesség stabilizálása, a nemzetközi együttműködés fejlesztése, valamint a képzések, gyakorlatok, az alapszintű biztonság és az együttműködés fejlesztése. Ezek tulajdonképpen nagyon hasonlóak a NIS céljaihoz, de valamivel korábban megfogalmazva.[18] A stratégia követelményként rögzíti, hogy a magyar kibertér nyújtson biztonságos és megbízható környezetet:

- az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,
- a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,

[17] 1163/2020. (IV. 21.) kormányhatározat, 72. pont.

[18] Szádeczky 2020: 87.

- a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,
- az elektronikus közigazgatás számára, hozzájárulva az állami szolgáltatások innovatív és előremutató fejlesztéséhez.[19]

Ezek alapvetően garantálják mind a polgári, mind az ipari, valamint az állami rendszerekben alkalmazott IoT-rendszerek kialakításának alapelveit. Megerősítve az eddigi szabályozásokat 2013 áprilisában a magyar Országgyűlés elfogadta az állami és önkormányzati szervezetek elektronikus biztonságáról szóló 2013. évi L. törvényt. A törvény hatálya valamivel tágabb, mint az állami és önkormányzati szervezeteké, többek között kiterjed a nemzeti adatfeldolgozókra és a létfontosságú rendszerelemekre is, így az IoT-eszközök és -rendszerek szinte teljes körét érinti.[20] A törvény a nemzetközi legjobb gyakorlatokon és szabványokon (például ISO/IEC 27001:2013) alapul, bár közvetlenül nem hivatkozik rájuk. A törvény az információbiztonság területén a CIA-triászként (bizalmasság, sértetlenség és rendelkezésre állás) ismert alapvető elemekkel operál. A törvény megköveteli az információs rendszerek integritásának és rendelkezésre állásának zárt, teljes körű, következetes, az elektronikus rendszerre és elemeire vonatkozó kockázatokkal arányos módon történő biztosítását. Fontos, hogy a kockázatokkal arányos biztonsági ellenőrzés végrehajtása kifejezetten szerepeljen a biztonsági ellenőrzés végrehajtásában. Ez kikényszeríti a kockázatértékelés elvégzését és az azon alapuló döntéseket. Ez megváltoztatja a biztonsági intézkedések ad hoc végrehajtásának rossz gyakorlatát, és a biztonsági költségvetések minimalizálását szolgálja.[21] Ezek különösen fontosak egy IoT-eszközöket is tartalmazó rendszer kialakítása során.

Az információs és kiberbiztonsági eljárásokat és intézkedéseket felölelő szabályozások mellett hazánkban a 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.) is rendelkezik olyan területekről, amelyek nagymértékben érinthetik az IoT-eszközöket és -rendszereket. Ezek a területek alapvetően az információs rendszer felhasználásával elkövetett csalások. Mivel az IoT-eszközök jellemzően kevésbé biztonságosak, így a fentebb is leírtaknak megfelelően a támadók által könnyen kihasználhatók valamilyen káros tevékenység végzése céljából. A támadók hozzáférhetnek általuk személyes adatokhoz, magánterületek kamerarendszereihez (azok által információkat gyűjthetnek az ottani személyekről, tárgyakról, dokumentumokról), továbbá az uralmuk alá vont eszközökkel káros tevékenységeket

[19] 1139/2013. (III. 21.) kormányhatározat, 8. pont.
[20] Kerti–Nyikes 2015: 330.
[21] 2013. évi L. törvény, 6. pont.

folytathatnak más eszközök, rendszerek ellen. A Btk. 375. § (1) pontjában megfogalmazottak szerint, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. További szabályozás, hogy aki az információs rendszer felhasználásával elkövetett csalással jelentős kárt okoz, vagy a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el, egy évtől öt évig terjedő szabadságvesztésre ítélhető. Amennyiben az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el, a szabadságvesztés mértéke két évtől nyolc évig terjed. Ha az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el, abban az esetben a büntetés öt évtől tíz évig terjedő szabadságvesztés. A tiltott adatszerzés bűncselekményére is kitér a Btk, amely akkor valósul meg, ha az elkövető személyes adatok, magántitkok vagy üzleti titkok jogosulatlan módon történő megszerzésére törekszik. Az ilyen adatok jogosulatlan megszerzése az alábbi technikák segítségével valósulhat meg:

- egy másik személy lakásának vagy más helyiségének, illetve a hozzá tartozó bekerített területnek a tulajdonos tudtán kívüli átkutatásával, valamint az ott folyó tevékenység technikai eszközökkel történő megfigyelésével és rögzítésével;
- más személy lezárt, közleményt tartalmazó postai küldeményének felnyitásával vagy megszerzésével és tartalmának technikai eszközökkel rögzítésével;
- elektronikus hírközlő hálózatra továbbított vagy ott tárolt adatok lehallgatásával és a lehallgatás technikai eszközökkel rögzítésével.[22]

IoT-eszközök és -rendszerek hardveres és szoftveres védelme

Az IoT-rendszerek esetében is, mint minden informatikai hálózatnál, a réteges biztonsági felépítés a leghatékonyabb, ezáltal több biztonsági eszköz és megoldás

[22] 2012. évi C. törvény, 422. §.

is alkalmazható az adatok megóvása érdekében. Az első védelmi vonalnak minden esetben egy jó tűzfalat, vagy a még jobb és hatékonyabb eredmény elérése érdekében egy olyan rendszert kell alkalmazni, amely hatékonyan magában foglal több biztonsági funkciót is. A legerősebb és legbiztonságosabb tűzfaltermékek kiválasztása során célszerű figyelembe venni a kormány és a különböző védelmi ügynökségek ajánlásait, javaslatait. Egy megfelelően biztonságos periméter védelmi eszköz az alábbi öt legszükségesebb biztonsági rendszert egyesíti egyetlen készülékbe:

- tűzfalat;
- víruskeresőt/kémprogramokat/spamszűrőket;
- virtuális magánhálózatot (VPN);
- alkalmazásszűrést;
- behatolásmegelőző/-érzékelő rendszereket.

A tűzfalak

A tűzfalak a külső perembiztonság alapvető eszközei, amelyek megvédik a belső hálózatot a külső fenyegetésektől. A tűzfal szelektálja, és ennek megfelelően engedélyezi vagy blokkolja a bejövő és kimenő forgalmat. A tűzfalak lehetnek önálló hálózati eszközök, amelyek a magánhálózatok belépési pontjain találhatóak, vagy a számítógépeken és egyéb hálózati végberendezéseken futó személyes tűzfalprogramok. Egy szervezet tűzfala védi a belső közösséget; míg a személyes tűzfalat az egyén igényeihez szabhatjuk. A tűzfalak elválaszthatják és elkülöníthetik a különféle hálózati zónákat, nevezetesen a nyilvános internetet, a magánhálózatokat és a demilitarizált zónákat (DMZ). A tűzfal feladata a (hálózati) biztonsági házirend betartatása hozzáférés-szabályozással a hálózati erőforrásokhoz. A tűzfal olyan biztonsági intézkedések integrált gyűjteménye, amelyek célja, hogy megakadályozza a hálózati számítógépes rendszerhez, valamint az IoT-eszközökhöz való jogosulatlan elektronikus hozzáférést. Ugyanez az elv működik az összes intelligens eszköz esetében. A tűzfal sikeres használata a megfelelő termék kiválasztásától függ. A tűzfalak csomagszűrése számos szabály alapján fogadja el vagy utasítja el a csomagokat, amelyek a csomagok forrás- és célportjaitól és egyéb diffúziós kritériumoktól függenek. A tárgyak internetén (IoT) található intelligens eszközök biztonsági szintje a tűzfalszoftver testre szabásától/beállításaitól függ.[23]

[23] Madakam–Date 2016: 29.

A demilitarizált zóna

A tűzfalak mögött elhelyezkedő felhasználók nagyon sok esetben szeretnének hozzáférni a nyílt internethez, hogy levelezéseiket tudják intézni vagy böngésszenek. Az IoT-k esetében azonban nagyon sok esetben fordított a helyzet. Az eszközök helyezkednek el egy védett belső hálózaton, azonban a felhasználók a külső nyílt internet irányából próbálnak hozzájuk hozzáférni. Mind a két esetben szükségszerű a demilitarizált zónák alkalmazása. A DMZ a kerületi hálózat, ahol az erőforrások nyilvános IP-címekkel rendelkeznek, tehát ezeket látják és hallják az interneten. Az olyan erőforrásokat, mint a web, az e-mail és a tartománynév-kiszolgáló, a DMZ-ben helyezik el, míg az ehhez a hálózathoz tartozó többi erőforrás teljesen el van rejtve egy tűzfal vagy forgalomirányító mögött. A DMZ-ben elhelyezett eszközök könnyebben támadhatók, mivel azokat a belső hálózattal ellentétben az esetek többségében csak egy tűzfal védi a külső nyílt internettől. DMZ-k esetében megkülönböztetünk egy és két tűzfalas rendszert. Az egy tűzfalas védelmi rendszert jellemzően a kisebb hálózatok engedhetik meg maguknak, amelyek kisebb adatforgalmat generálnak. A két tűzfalas konfigurációval jóval védettebb lesz a hálózat, a DMZ a belső és külső tűzfal között helyezkedik el.

Amennyiben a DMZ kialakításakor olyan tűzfalat alkalmazunk, amelynek három kapcsolata van – egy a külső hálózathoz (internet), egy a webszerverhez és egy a belső hálózat irányába, akkor a tűzfallal való összeköttetés (az egyes interfészek) során különféle tűzfalszabályok érvényesíthetők, különböző védelmi formákat biztosítva. A webszerver alkalmazása a DMZ-ben megakadályozza a külső hálózat felhasználói számára a közvetlen hozzáférést a belső hálózat többi számítógépéhez. Amennyiben a webszerver kompromittálódik a DMZ kialakításának jellegéből adódóan a belső hálózatnak továbbra is van bizonyos védelmi vonala, mivel a behatolóknak ismét át kell lépniük a tűzfalat, hogy belépjenek a belső hálózatba.

Ha a tűzfal csak két interfészt támogat (vagy csak egy házirendet), akkor több tűzfalat lehet használni ugyanazon DMZ hatás elérése érdekében. Az első tűzfalat a külső hálózat és a webszerver között kell elhelyezni, a második tűzfal a webszervert kapcsolja össze a belső hálózattal. Ennek a kialakításnak az alapján az első tűzfal házirendje kevésbé lesz korlátozó, mint a második. A gépek egymáshoz csoportosítása a hasonló tűzfalbiztonsági igények alapján egyre gyakoribb, és egyre jobban bevált gyakorlatnak tekinthető. A nagy hálózatokban lehetnek szerverfarmok vagy több kiszolgálóból álló csoportok, amelyek hasonló szolgáltatásokat nyújtanak.

A DMZ elsődleges előnye, hogy a nyilvános internetet használók részére hozzáférést biztosít bizonyos biztonságos szolgáltatásokhoz, miközben továbbra is puffert tart fenn a felhasználók és a magán belső hálózat között. Ennek a puffernek a biztonsági előnyei számos módon nyilvánulnak meg, ideértve:

- Hozzáférés-ellenőrzés: szinte minden modern hálózat, köztük az IoT-hálózatok esetében is szükséges, hogy a felhasználók számára hozzáférést biztosítsanak a hálózat peremén kívüli szolgáltatásokhoz a nyilvános interneten keresztül. A DMZ-hálózat hozzáférést nyújt ezekhez a szükséges szolgáltatásokhoz, ugyanakkor olyan szintű hálózati szegmentációt vezet be, amely növeli azon akadályok számát, amelyeken az illetéktelen felhasználóknak át kell jutniuk, mielőtt hozzáférhetnek a belső védett magánhálózathoz. Egyes esetekben a DMZ proxykiszolgálót is tartalmaz, amely központosítja a belső felhasználói internetes forgalom áramlását, és megkönnyíti a forgalom rögzítését és felügyeletét.
- Védi a rendszert a támadók hálózati felderítésétől: a DMZ által biztosított külső pufferzóna megakadályozza, hogy a támadó a hálózaton belül minél több potenciális célpontot azonosítson és esetleg megtámadjon. Még ha a DMZ-n belüli rendszert veszélyeztetik is, a magánhálózatot a belső tűzfal védi a támadóval szemben. Ugyanebből az okból kifolyólag megnehezíti a külső felderítést a magánhálózaton belül. Bár a DMZ-ben lévő szerverek nyilvánosan elérhetőek, a külső támadások kivédésére egy újabb védelmi réteggel is rendelkeznek, ami potenciálisan megnehezíti a támadói szándékok érvényesülését.
- IP-hamisítás elleni védelem: bizonyos esetekben a támadók megpróbálhatják megkerülni a hozzáférés-szabályozási korlátozásokat úgy, hogy a hálózaton engedélyezett IP-címet meghamisítva próbálnak hozzáférni a belső védett hálózathoz. A potenciális IP-hamisítók sikerének megakadályozása érdekében a DMZ egy másik szolgáltatás segítségével ellenőrzi az IP-cím jogszerűségét azáltal, hogy a hálózatba való belépés előtt ellenőrzi, hogy az az adott időpontban elérhető-e.

A DMZ minden esetben olyan szintű hálózati szegmentációt biztosít, amely olyan hálózati környezetet hoz létre, ahol az adatforgalom igény szerint szervezhető és kezelhető, és a nyilvános szolgáltatások a magánhálózattól biztonságos távolságból érhetők el. Összességében tehát elmondható, hogy a DMZ egy pufferzónaként működik, amely hozzájárul a megosztott szolgáltatások és adatok biztonságos elérhetőségéhez. Ez a zóna a biztonsági rendszerek egyszerű

szegmentálását is biztosítja a szervezeti vezérlőrendszerek számára. Az adatforgalom nem haladhat át ezen a zónán, és minden fontos, a zónához tartozó rendszernek ebből a zónából kell kiindulnia, és oda kell érkeznie.[24]

Forgalomirányítók

Az IoT-hálózatokban használt forgalomirányítók jellemzőinek összhangban kell lenniük a belső védett hálózat követelményeivel. A tesztelés után a szakemberek pontosan meg tudják határozni, hogy a forgalomirányítónak milyen tulajdonságokra van szüksége a kívánt védelmi szint eléréséhez. Az alapvető forgalomirányítási funkciók mellett a következő funkciók állnak rendelkezésre az eszközökön:

- biztonság (Security);
- a szolgáltatás minősége (Quality of Service, továbbiakban: QoS);
- IP-alapú hangátvitel (Voice over IP, továbbiakban: VoIP);
- hálózati címfordítás (Network Address Translation, továbbiakban: NAT);
- dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, továbbiakban: DHCP);
- virtuális magánhálózat (VPN).

Az IoT-hálózatok tervezésekor többszintű, hierarchikus címzési és elnevezési rendszert kell alkalmazni, hogy a hálózathoz hozzáadott új felhasználók vagy eszközök könnyen és egyszerűen nyomon követhetők legyenek. Fontos tervezési szempont, hogy a belső hálózattól szigorúan elkülönített demilitarizált zónában (DMZ) kell elhelyezni a külvilággal megosztott tartalmat tároló eszközöket. Ezzel a megoldással biztosítható, hogy a kívülről érkező támadások egy olyan alhálózatba érkezzenek, amely jól elkülönül a biztonságérzékeny területtől. A hálózati címfordítást arra használják, hogy a kialakított belső címzési sémát elrejtsék a külvilág elől. A belső IoT-eszközök privát IP-címeinek mások számára is látható nyilvános címre történő lefordításával megakadályozható, hogy a hálózati struktúrát kívülről felderítsék. A külső támadások mellett a belső forgalomszűrésre is szükség van, hogy kiszűrjük a bizonyos hálózati területekre belépő és onnan kilépő, nem engedélyezett csomagforgalmat. A felesleges forgalom kiszűrésével a hálózati sávszélesség javítható. Az összes hálózati eszközhöz

[24] Chopra 2020: 10.

való távoli hozzáférést úgy kell biztosítani, hogy azok megfelelő erősségű jelszavakkal védhetők legyenek az illetéktelen hozzáféréstől.[25]

Az IoT szoftveres biztonsága

Az előző fejezetben a szerző bemutatott számos hardveres védelmi lehetőséget az IoT-eszközök és -rendszerek számára, de ahhoz, hogy teljes körű védelmet biztosítsunk ezeknek az eszközöknek, szoftveres védelemre is szükség van. Mindenekelőtt az alapvető biztonsági beállításokat kell elvégezni a használt eszközök felhasználói szoftverében. Ez azt jelenti, hogy a telepítendő eszközök kezelőfelületére való bejelentkezéshez használt alapértelmezett felhasználónevet és jelszót minden esetben meg kell változtatni. Ezek minden eladott eszköz esetében azonosak, így egy támadónak nem nehéz kitalálnia, hogy milyen hitelesítő adatokkal férhet hozzá az eszközökhöz, és veheti át az irányítást felettük, vagy akár az egész rendszerünk felett. A felhasználónév és a jelszó kiválasztásakor fontos, hogy körültekintően járjunk el, és olyat válasszunk, amely nem azonosítható személyesen a felhasználóval (legyen az egy adott személy vagy egy szervezet), és nem lehet könnyen kitalálni, például egy közösségi médiaplatformon való kereséssel. Ajánlott továbbá elkerülni a túl egyértelmű, de mindenki számára könnyen megjegyezhető jelszavakat. Ezek nagyban megkönnyíthetik a jelszófeltörést, amellyel a támadó könnyedén hozzáférhet az eszközeinkhez, rendszereinkhez, adatainkhoz.[26] A következő módszerek segíthetnek a támadónak a jelszavak megszerzésében, így segítve az eszközhöz vagy alkalmazáshoz való hozzáférés megszerzését:

- Szótári támadás: szótári szavakat használó támadás, amely szisztematikusan kipróbálja a szótárban szereplő szavakat. A támadás esetében elmondható, hogy a támadó sikerének esélye nem sokat változik több szótári szó kombinálásával. A leetspeak (egy betű helyettesítése egy hasonló számmal) megoldást már számos jelszófeltörő használja, így ez nem növeli sokat a biztonságot. A szótári vagy személyes jelszó megváltoztatásának praktikus és megjegyezhető módja például az, ha a billentyűzeten az összes karaktert egy irányba toljuk el (például Password helyett Ősddeptf), ami számok és speciális karakterek hozzáadásával még nehezebben kitalálható.

[25] Meidan et al. 2020: 8.
[26] Bányász 2017: 117.

- Brute force támadás: az összes lehetséges alfanumerikus kombinációval történő támadás. E támadások elhárításához a felhasznált karakterek számának növelése jelentősen csökkentheti a támadó sikerének esélyeit, mivel növeli a jelszó megfejtéséhez szükséges időt. Ezért tanácsos nem egyszavas jelszavakkal védekezni, hanem inkább kifejezéseket és teljes mondatokat használni.
- Szivárványtábla-támadás: olyan dekódolási technika, amely egy előre kiszámított, hash-eket tartalmazó jelszólistát használ (egy egyirányú algoritmus, amely az adatokat egyedi karakterláncként ábrázolja), hogy a hashek keresésével következtetni lehessen a jelszavakra. Ismét, bár más általános klaszterezési módszert használ, a jelszavakat adathalászattal, social engineeringgel vagy rosszindulatú szoftverekkel is meg lehet szerezni.
- Maleware-es jelszófeltörés: erre példa lehet a keyloggerek használata (olyan program, amely rögzíti a felhasználó minden egyes billentyűlenyomását, lehetővé téve a bizalmas információkhoz és jelszavakhoz való hozzáférést), valamint a man-in-the-middle támadások, amelyek során a támadó a két kommunikáló fél közötti csatornába ékelődve észrevétlenül figyelheti és befolyásolhatja a forgalmat.[27]

A jelszavak kiválasztásakor tehát a legfontosabb, hogy megfelelő hosszúságúak és összetettek legyenek, lehetőleg ne tartalmazzanak konkrét szavakat, hanem inkább véletlenszerű karaktereket, és minden esetben tartalmazzanak számokat és speciális karaktereket. Sokak számára azonban komoly problémát jelenthet az összes jelszó megjegyzése, különösen akkor, ha betartják az alapvető jelszó protokollt, miszerint a jelszavakat néhány havonta meg kell változtatni. A probléma elkerülésére jó megoldás egy megfelelő jelszókezelő program használata, amely biztonságosan tárolja a több fiókhoz használt jelszavakat, amelyekhez csak egy fő jelszót kell megjegyezni ahhoz, hogy a többi fiókhoz hozzáférhessen. Ugyanakkor fel kell ismerni, hogy ez a módszer is problémás lehet: ha mindent egy programban tárolunk, elég azt az egy programot feltörni, és az összes fiók veszélybe kerül.

Napjainkban a felhasználók és az üzemeltetők egyre kifinomultabb támadókkal néznek szembe, és az IoT-eszközök számának exponenciális növekedése is hatalmas és egyre növekvő nyomást helyez rájuk. Ennek eredményeképpen az eszközök biztonsági tesztelésének, az eszközök nyomon követésének, fris-

[27] Szűcs 2019: 85.

sítésének, identitásának ellenőrzése egy pillanatra sem elhanyagolható. Több kutatás is bizonyítja, hogy az IoT-eszköznek egyedi azonosítója kell hogy legyen, ennek hiányában a felhasználó komoly kockázatnak van kitéve, megnő az identitáshamisítás és az eszközök feltörésének esélye.

Behatolásérzékelő és -megelőző rendszerek

A behatolásérzékelő rendszer (IDS, Intrusion Detection System) jelenti a kibertámadásokkal szembeni első védelmi vonalat, amely a hálózat egy taktikai pontján stratégiailag kijelölt eszköz vagy szoftver, amely az azon áthaladó forgalmat figyeli. Az IDS olyan hardveres vagy szoftveres megoldás, amely a hálózati forgalom zavarása nélkül válogatás nélkül figyeli a hálózaton áthaladó csomagokat.

A behatolásmegelőző rendszer (IPS) egy aktív eszköz, amely a hálózati forgalom szűrésével és vizsgálatával továbbítja vagy eldobja a csomagokat, amint azok belépnek a hálózatba. Telepítéskor kiemelt figyelmet kell arra fordítani, hogy minden ki- és bemenő forgalom áthaladjon az IPS-en. Ha az IPS rosszindulatú forgalmat észlel, képes az azonnali beavatkozásra a beállítások megváltoztatásával, ezzel blokkolva a rosszindulatú forgalmat. Ezzel egy időben riasztási üzenetet küld a hozzá csatlakoztatott felügyeleti állomásnak.

Az IDS és az IPS kombinált használata

A látszattal ellentétben az IDS és az IPS kompatibilis technológiák, és nem ritka, hogy mindkettőt párhuzamosan használják egy vállalati környezetben. Az IPS aktívan blokkolja a nem kívánt forgalmat, és tűzfalrendszernek tekinthető. Ezért úgy kell konfigurálni, hogy csak az ismert rosszindulatú forgalmat szűrje a csatlakozási problémák elkerülése érdekében. Ez lehetővé teszi az IDS számára, hogy felügyelje az IPS megfelelő működését, ugyanakkor riasztásokat küldjön a szürke zónának minősülő forgalomra. Ide tartozik minden olyan adat, amely nem egyértelműen rosszindulatú, de nem tekinthető hitelesnek sem. Amennyiben az IPS blokkolja az ilyen típusú forgalmat, fennáll annak a veszélye, hogy a jogszerű forgalmat is megszakítja. Rosszindulatú forgalom esetén azonban az IDS által küldött riasztás értékes információkkal szolgál a lehetséges problémákról és a támadás módjáról.[28]

[28] Zsótér 2021.

Az IDS és IPS rendszerek típusai

Az IPS és IDS megoldások típusai a hálózatban elfoglalt helyük és a rosszindulatú forgalom azonosítására használt módszer szerint csoportosíthatók. Az előbbiek hálózat- vagy állomásalapúak, míg az utóbbiak négyféle technikára oszthatók:

- szignatúraalapú;
- házirend- (policy-) alapú;
- anomáliaalapú;
- mézescsupor- („honeypot-”) alapú.

Az állomásalapú IPS (Host-based IPS – HIPS) minden egyes számítógép és hoszt tevékenységét külön-külön vizsgálja. Teljes hozzáférése van a végberendezések belső adataihoz, így a bejövő forgalmat az állomás tevékenységével összefüggésben vizsgálja. VPN-környezetben, ahol az adatok a hálózaton való áthaladás során titkosítottak, a HIPS az egyetlen megoldás a célállomáson a valódi forgalom vizsgálatára. Hátránya, hogy jellemzően egyetlen operációs rendszert támogat, és nem véd az alacsonyabb szintű támadások ellen, amelyek az OSI rétegmodell első és harmadik rétegét érintik. További hátránya, hogy a támadó a megfelelő felderítési folyamatok lefuttatása után tudni fogja, hogy az állomás létezik, és még azt is felfedezheti, hogy az állomás HIPS által védett.

A hálózatalapú IPS (Network-based IPS – NIPS) minden egyes, a hálózaton áthaladó csomagot elemez, így képes olyan rosszindulatú csomagok felderítésére, amelyek a tűzfal egyszerű szűrési szabályain is átjutnak. Az NIPS hálózatba telepítésekor ügyelni kell arra, hogy minden forgalom, de minimálisan a kritikus forgalmak vizsgálhatók legyenek. A NIPS képes az alacsony szintű támadások észlelésére, de az érzékelőn áthaladó titkosított forgalmat nem tudja ellenőrizni. A NIPS csak a hálózat szemszögéből, kontextus nélkül elemzi a támadásokat, így előfordulhat, hogy az egyébként ártalmatlan forgalmat támadásnak tekinti. E hiányosság miatt a NIPS következtetéseivel mindig óvatosan kell bánni.[29]

[29] Hussein–Falcarin–Sadiq 2021: 581.

Az állomás- és a hálózatalapú IPS összehasonlítása

Mivel a NIPS nem vizsgálja a forgalmat az állomás szintjén rosszindulatú tevékenységek szempontjából, kizárólag a csomagok jellemzői (szignatúra) alapján dönt a csomagok engedélyezéséről vagy blokkolásáról. Egy hálózati alapú IPS számára rendkívül nehéz, ha nem lehetetlen annak értékelése, hogy egy támadás sikeres volt-e. Az ilyen rendszerek csak a rosszindulatú tevékenység jelenlétét észlelik.

A HIPS ezzel szemben a helyi állomás vagy operációs rendszer ellenőrzését végzi. Lehet összetett, amely a tényleges rendszerhívásokat vizsgálja, vagy egyszerű, amely csak a rendszer naplózását és a naplófájlok elemzését teszi lehetővé a hosztokon. Egyes HIPS-ek megelőzik a támadásokat, mielőtt azok megtörténnének, míg mások csak akkor jeleznek, ha már megtörtént valami. Általánosságban elmondható, hogy a HIPS a puffertúlcsordulások, webkiszolgálók elleni támadások, hálózati felderítések, valamint elárasztásos, más néven szolgáltatás-megtagadásos (DoS) támadások detektálására alkalmas, és a HIPS az alkalmazások és állomások által használt erőforrásokat is óvja. A HIPS egyik fő előnye, hogy képes az operációsrendszer-folyamatok felügyeletére és a kritikus rendszererőforrások védelmére. A HIPS összesíti a viselkedéselemzést és a szignatúraalapú szűrést, egy csomagban egyesítve a vírusirtók, a hálózati és az alkalmazásszintű tűzfalak legjobb tulajdonságait.

Szignatúraalapú IDS és IPS

Az szignatúraalapú megközelítés viszonylag merev, de egyszerűen alkalmazható. A mintaillesztéshez előre meghatározott, rögzített bájtsorozatokat keres a csomagok fejlécében és adattartalmában. A legtöbb esetben csak akkor beszélhetünk mintaillesztésről, ha a gyanús csomag meghatározott szolgáltatásokhoz (még inkább meghatározott portokhoz) kapcsolódik. Ez a módszer csökkenti a vizsgálatból eredő hálózati terhelést, de sokkal nehezebben alkalmazható olyan rendszerekben, amelyek nem használnak jól ismert portokhoz kapcsolódó protokollokat.

Házirendalapú IDS és IPS

A házirendalapú szűrés során a házirend megsértése esetén az IDS és az IPS blokkolhatja a forgalmat vagy riasztást küldhet az eseményről. A riasztás szükségességét egy algoritmus alapján döntik el. A módszer azért is nagyon népszerű, mert olyan támadásokat is képes felismerni, amelyek még nem ismertek. A házirendalapú IDS és IPS esetében mindig világossá kell tenni, hogy pontosan mi a házirend célja és mire terjed ki. Ha a hálózati hozzáférést házirenddel kívánjuk szabályozni, akkor meg kell határozni a jogosultságokat, hogy mely hálózatok érhetik el egymást, és milyen protokollok használhatók.

Anomáliaalapú IDS és IPS

Az anomáliaalapú rendszerek általában a normálistól eltérő hálózati forgalmat keresik. Anomáliának tekintjük például egy bizonyos típusú forgalom szokatlan növekedését, a vizsgált hálózaton jellemzően nem előforduló forgalomtípus megjelenését, vagy akár egy ismert protokoll deformált üzenetét.

Kétféle anomáliaalapú IDS-t és IPS-t különböztetünk meg:

- Statisztikai alapú anomáliafelismerésről akkor beszélünk, amikor a rendszer megtanulja a vizsgált hálózat „profilját", azaz a rajta áthaladó forgalom mintázatát egy bizonyos idő alatt. Ezután a rendszer a forgalom statisztikai elemzésével megállapítja, hogy az eléggé eltér-e a szokásostól, és ha igen, riasztást küld.
- A nem statisztikai anomáliaérzékelés esetében az ismert, normális viselkedés előre meghatározott, a forgalmi mintától való bármilyen eltérés riasztást vált ki.

Mézescsupor-alapú rendszerek

A mézescsupor-alapú rendszereket gyakran használják arra, hogy segítsenek egy szervezetnek a belső IT-infrastruktúrája védelmében. Az ilyen típusú honeypot csökkenti az adott szervezet kockázatát azáltal, hogy az IT-környezetét a támadások azonosítása érdekében végrehajtja. Mivel a honeypotnak kevesebb funkciója van, a megvalósítás gyakran egyszerű. Elmondható, hogy a termelési honeypot a könnyű működtetés és az összegyűjtött információk mennyisége

közötti kompromisszummal jár. A honeypotnak szerver- vagy klienshoneypot szerepét kell betöltenie. A kiszolgáló-honeypot türelmesen vár, amíg a támadók kezdeményezik a kommunikációt, míg a klienshoneypotok szigorúan keresik a potenciális entitásokat, amelyek interakciót kérnek.[30]

A honeypot olyan rendszer, amely egy valós rendszer vagy protokoll szimulálásával rögzíti és azonosítja a rosszindulatú tevékenységeket. Célja, hogy megtámadják, de mivel ellenőrzött környezetben van, az esetleges támadásokat megfékezi. A támadó nem tudja, különösen a támadási folyamat elején, hogy a honeypot nem valódi rendszer vagy eszköz, és megpróbálja kihasználni azt az ismert sebezhetőségek alapján. A honeypot rögzíti a támadási stratégiákat, és tartalmazhatja a hálózati forgalmat, a hasznos terhelést, a rosszindulatú programok mintáit, a támadó által használt eszközkészletet stb.

Léteznek tipikusan az IoT-környezetre kialakított interaktív honeypotok, úgynevezett ThingPotok, amelyek egy teljes IoT-platformot szimulálnak, nem pedig egyetlen alkalmazási szintű kommunikációs protokollt. Jelenleg a következő IoT.honeypotok alkalmazása a legnépszerűbb:

- Telnet IoT.honeypot: ez egy olyan honeypot, amely egy Telnet-kiszolgálót valósít meg az IoT-malware elfogására.
- HoneyThing: ez egy olyan honeypot, amelyet a TR-069 (CPE[31] WAN[32] Management Protocol, CWMP) számára terveztek.
- IoTPOT: különböző IoT-eszközök Telnet-szolgáltatásait emuláló honeypot. Az IoTPOT egy alacsony interakciójú front-end responderből áll, amely együttműködik egy magas interakciójú virtuális backenddel, az IoTBOX-szal. Az IoTBOX különböző beágyazott rendszerek általánosan használt virtuális környezeteket működtet különböző CPU-architektúrákhoz.
- Dionaea: egy honeypot-keretrendszer, amely többek között egy üzenetküldő (például: MQTT[33]) modult valósít meg.
- ZigBee honeypot: egy ZigBee átjárót szimuláló honeypot.
- Többcélú IoT-honeypot: egy IoT-honeypot, amely a Telnetre, az SSH[34]-ra, HTTP-re és CWMP-re összpontosít.[35]

[30] Razali et al. 2018: 94.

[31] Customer Premise(s) Equipment: ügyfélnél működtetett eszközök.

[32] Wide Area Network: nagy kiterjedésű hálózat.

[33] Message Queue Telemetry Transport: az üzenetek sorba állításán alapuló telemetriai adattovábbítás.

[34] Secure Shell: egy protokoll, amely biztonságos, titkosított csatornát hoz létre egy helyi és egy távoli számítógép között.

[35] Wang– Santillan–Kuipers 2018: 1.

Virtuális magánhálózatok

Napjainkban az IoT-eszközök és -rendszerek elterjedése a hálózati biztonsági elemek fejlesztését és alkalmazását nagymértékben megnövelte. Számos gyártó kínál már olyan termékeket, amelyek ezeket a biztonsági megoldásokat más biztonsági funkciókkal kombinálják, hogy növeljék a használt eszközök és rendszerek biztonságát. Az egyik ilyen megoldás a virtuális magánhálózatok használata, amelyek ma már a gigabites biztonsági útvonalválasztókban is elérhetők, ahol az eszköz tűzfalfunkciókat, hálózati címfordítást és titkosítást is képes ellátni.

A virtuális magánhálózatok (VPN) fejlett titkosítási és alagútépítési technikákat használnak, hogy biztonságos, végponttól végpontig tartó hálózati kapcsolatokat tegyenek lehetővé olyan hálózatokon, amelyek alapvetően nem megbízhatóak. A biztonságos kapcsolat azt jelenti, hogy a küldő hitelesítése mellett az üzenet integritása és bizalmas jellege is ellenőrizhető. A VPN az adatokat kapszulázással, titkosítással vagy mindkettővel védi. A virtuális magánhálózatok általános jellemzői:

- virtuális: nincs valódi fizikai kapcsolat;
- az internet nyílt infrastruktúrájának kihasználása (az interneten keresztüli kapcsolatok);
- lehetőség az interneten keresztül történő információcserére földrajzilag egymástól távol eső vállalati telephelyek között;
- egyetlen, közös vállalati hálózat használatának lehetősége az összes telephelyen;
- viszonylag alacsony hálózati költségek, jelentősen olcsóbbak, mint a hagyományos megoldások, de a biztonság problémás lehet;
- léteznek olyan megoldások, amelyek a biztonsági követelményeknek is megfelelnek.

Az IoT-rendszerek esetében nagyon hasznos megoldás a szoftvervezérelt hálózati (software defined network, SDN) technológia. Az SDN hálózati egyszerűsítést és automatizálást biztosít, ezáltal például a VPN-szolgáltatásokat is hatékonyan lehet SDN-en keresztül biztosítani, amely az SD-VPN technológiát jelenti. Ennél a megoldásnál ahelyett, hogy a VPN-szolgáltatásokat előzetesen manuálisan hoznánk létre, az SD-VPN automatikusan hozza létre a VPN-szolgáltatásokat, amikor egy VPN-ügyfél csatlakozik, ami egy robusztus, gyorsan növekvő IoT-hálózat esetében nagyon hasznos tud lenni. Kezdetben az SD-VPN-végpontokon nincs VPN-szolgáltatás. Amikor az IoT-eszköz mint VPN-ügyfél csatlakozik

a saját VPN-hez, az ügyfél egyedi metaadatokkal (például MAC-cím, portszám stb.) fut, amelyek megkülönböztetik a többi VPN-klienstől és -szolgáltatástól. A metaadatok hozzárendelése a különböző VPN-ekhez, más szóval a különböző IoT-szolgáltatásokhoz, előre definiált, amelyek alapján az SDN-vezérlő meghatározza, hogy melyik VPN-példányt kell az ügyfélhez rendelni, és ezt az információt az SD-VPN-végpontra továbbítja, és ennek megfelelően létrejön egy VPN-példány a végponton.[36]

Titkosítás

A titkosítás vagy kriptográfia az egyik leggyakrabban használt technika a biztonság megteremtésére. A kriptográfia hatékony technikának és eszköznek tekinthető az adatok biztonságának garantálásához. A titkosítást jellemzően hash-funkciók alkalmazásával együtt használják a számítógépes jelszó biztonságossá tételére. A kriptográfiának számos aspektusa van, az információbiztonsághoz hasonlóan többek között például a bizalmasság, a sértetlenség és a hitelesítés. A kriptográfiában az adatokat olyan formában tároljuk és továbbítjuk, hogy a küldőn és a címzetteken kívül senki sem értheti meg, harmadik fél nem képes értelmezni vagy hozzáférni ezekhez az adatokhoz. A kriptográfiának két fő típusa van: szimmetrikus és aszimmetrikus kulcsú titkosítás.

A szimmetrikus kriptográfiai algoritmus ugyanazt a kulcsot használja az adatok titkosításához/visszafejtéséhez. A technikában a feladó egy kulcsot használ az adatok titkosításához és a címzettnek való átadásához, a címzett pedig ugyanannak a kulcsnak a használatával dekódolja az adatokat egyszerű szöveggé. A feladó és a címzett biztonságos kommunikációs csatornán cseréli ki a kulcsot a kommunikáció megkezdéséhez. Különböző szimmetrikus titkosításon alapuló algoritmusok léteznek, mint például a DES (Data Encryption Standard), az AES (Advanced Encryption Standard), a Block Cipher, a Caesar Cipher és a Stream Cipher.

Az aszimmetrikus titkosítást nyilvános kulcsú titkosításnak is nevezik. Az aszimmetrikus titkosításban két különböző kulcsot (nyilvános/magán) használnak az adatok titkosításához/visszafejtéséhez. Mind a feladó, mind a címzett a saját nyilvános és magánkulcsát használja. A nyilvános/magánkulcsoknak különböző céljuk van, a nyilvános kulcsot a titkosításhoz, a magánkulcsot pedig

[36] Shi–Wang–Lung 2018: 2.

a visszafejtéshez használják. A nyilvános kulcsot megosztják a többi szervezettel, így bárki, aki el akarja küldeni az adatokat, a nyilvános kulcsot használhatja a titkosításhoz, a címzett a magánkulcsot használja a dekódoláshoz. A magánkulcs minden egyes felhasználó számára egyedi, így azt semmilyen körülmények között nem oszthatja meg, mert azáltal a kommunikáció és az adatok nagyon könnyen kompromittálódhatnak. Az aszimmetrikus titkosításon különböző típusú algoritmusok alapulnak, mint például az ECC (Elliptikus görbe kriptográfia) és a Diffie-Hellman, valamint a Rivest–Shamir–Adleman (RSA) titkosítások.

Összegzés

A tárgyak internetének biztonságát vizsgálva egyértelműen megállapítható, hogy a rendszerek és hálózatok összetettsége miatt nem lehet tökéletes megoldást garantálni. Az elemzés során azonosított és megfogalmazott hardveres és szoftveres megoldások csak együttesen alkalmazva lehetnek hatékonyak. Az IoT-eszközök hardveres és szoftveres védelmét illetően számos megoldás áll rendelkezésre a biztonság növelésére. A VPN-kiszolgálók a lehető legbiztonságosabb kapcsolatok létrehozására használhatók, titkosított virtuális csatornát hozva létre a felhasználók és az IoT-céleszközök között. Egyetlen hálózatot sem lehet azonban csak hardverrel védeni; minden esetben olyan megoldásokra van szükség, amelyek támogatják a rendszereken futó alkalmazások és programok szoftveres átvizsgálását, valamint olyan kiegészítő biztonsági szolgáltatásokat nyújtanak, amelyek segítik az IoT-rendszerek védelmét. Általánosságban elmondható, hogy minden esetben alapvető követelmény, hogy megbízható gyártótól és beszállítótól származó berendezéseket használjunk. Fontos, hogy komoly figyelmet fordítsunk az eszközök szoftver- és firmware-frissítésének lehetőségére, mert ennek hiánya komoly támadási potenciált jelenthet. Amennyiben az alkalmazott IoT-eszközök sebezhetőségeit a gyártói támogatás hiánya miatt nem lehet kijavítani (a firmware nem frissíthető), az adatbetörésekhez, hálózati kommunikációs zavarokhoz vagy szolgáltatásmegtagadáshoz vezethet. Fontos továbbá, hogy olyan forgalomirányítókat telepítsünk, amelyek már képesek komplex feladatok kezelésére a megfelelő hálózati biztonsággal, szolgáltatásminőséggel, hálózati címfordítással és virtuális magánhálózatok kezelésével kapcsolatban. Fontos kiemelni a tűzfalak fontosságát is, amelyekkel a védett belső hálózatunk előtt demilitarizált zónákat hozhatunk létre, ami nagyban növelheti rendszereink

biztonságát. A különböző típusú tűzfalak segíthetnek megakadályozni az eszközökhöz való hozzáférést, a rendszerekbe való illetéktelen behatolást, vagy létrehozhatnak egy demilitarizált zónát, ami szintén növeli a védelem szintjét.

A szoftveres oldalon a legfontosabb a végpontok és a kommunikációs csatornák titkosítása. Alapvető fontosságú, hogy kiemelt figyelmet fordítsunk a felhasználók hitelesítésére, mielőtt belépnének a rendszerbe, ezért olyan eljárásokat kell bevezetni, amelyek többfaktoros hibrid hitelesítést alkalmaznak például a személyazonossággal való visszaélések elkerülése érdekében. Egy másik rendkívül fontos szempont a megfelelő kulcskezelő rendszer kialakítása, amely biztosítja a kulcsok megosztását és tárolását az IoT-eszközök, -átjárók és kommunikációs komponensek között. Még egy tűzfallal megfelelően körülvett belső hálózat esetén is mindig célszerű elkülönített hálózatokat létrehozni az IoT-összetevők kezelésére, és az összes többi kapcsolatot más alhálózatokba, esetleg virtuális alhálózatokba áthelyezni, hogy az egyes összetevők kompromittálódása a lehető legkisebb negatív hatással legyen a teljes hálózatra.

Mindezek akkor lesznek különösen fontosak, amennyiben megjelennek a mesterségesintelligencia-elemek is az IoT-környezetben. Ezek a megoldások számos olyan kihívást hoznak még a jövőben, amelyek komoly kihívások elé állítják a szakembereket.[37]

Felhasznált irodalom

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

2012. évi C. törvény a Büntető Törvénykönyvről

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

Atlam, Hany F. – Gary B. Wills (2019): IoT Security, Privacy, Safety and Ethics. *Digital Twin Technologies and Smart Cities. Internet of Things.* Cham: Springer, 123–150. Online: https://doi.org/10.1007/978-3-030-18732-3_8

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). (2016. április 27.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679

[37] Szűcs 2022: 227.

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). (2019. április 17.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Bányász Péter (2017): A közösségi média, mint az információs hadszíntér speciális tartománya. *Hadmérnök,* 12(2. különszám), 108–121.

Bányász Péter – Bóta Bettina – Zágon Csaba (2019): A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37.

Brass, Irina – Leonie Tanczer – Madeline Carr – Jason Blackstock (2017): Regulating IoT: enabling or disabling the capacity of the Internet of Things? *Risk & Regulation 33,* 12–15. Online: https://discovery.ucl.ac.uk/id/eprint/1544261/1/Brass_IoT%20Regulation_Risk%20and%20Regulation%20Magazine_Accepted%20Version.pdf

Chiara, Pier Giorgio (2022): The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology,* 36(2), 118-137. Online: https://doi.org/10.1080/13600869.2022.2060468

Chopra, Ashok (2020): Paradigm shift and challenges in IoT security. *Journal of Physics: Conference Series 1432,* 1–14. Online: https://doi.org/10.1088/1742-6596/1432/1/012083

Európai Bizottság: Közös Közlemény az Európai Parlamentnek és a Tanácsnak, Az EU kiberbiztonsági stratégiája a digitális évtizedre. (2020. december 16.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679

European Commission: Advancing the Internet of Things in Europe, SWD (2016) 110 final. (2016. április 19.) Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110

Farkas, Tibor (2020): Communication and Information Services: NATO Requirements, Part I. *Revista Academiei Fortelor Terestre / Land Forces Academy Review,* 25(4), 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor (2021): Communication and Information Services – NATO Requirements, Part II. Revista Academiei Fortelor Terestre / Land Forces Academy Review, 26(1), 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Hussein, Adil Yousef – Paolo Falcarin – Ahmed T. Sadiq (2021): Enhancement Performance of Random Forest Algorithm Via One Hot Encoding for IoT IDS. *Periodicals of Engineering and Natural Sciences (PEN),* 9(3), 579–591.

Kambourakis, Georgios – Constantinos Kolias – Angelos Stavrou (2017): The Mirai botnet and the IoT Zombie Armies. *MILCOM 2017 – 2017 IEEE Military*

Communications Conference (MILCOM), 267–272. Online: https://doi.org/10.1109/MILCOM.2017.8170867

Kerti András – Nyikes Zoltán (2015): Overview of Hungary Information Security, the Issues of the National Electronic Classified Material of Transmission. *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics,* Timisoara, Romania, 327–333. Online: https://doi.org/10.1109/SACI.2015.7208223

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

Madakam, Samoyya – Hema Date (2016): Security Mechanisms for Connectivity of Smart Devices in the Internet of Things. *Connectivity Frameworks for Smart Devices. Computer Communications and Networks.* Cham: Springer, 23–41. Online: https://doi.org/10.1007/978-3-319-33124-9_2

Megyeri Lajos (2018): Elektronikus információs rendszerek biztonsági menedzsmentje. *Műszaki Katonai Közlöny,* 28(2), 66–80. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/1579

Meidan, Yair – Vinay Sachidananda – Hongyi Peng – Racheli Sagron – Yuval Elovici – Asaf Shabtai (2020): A Novel Approach for Detecting Vulnerable IoT Devices Connected Behind a Home NAT. *Computers & Security, Volume 97,* 1–23. Online: https://doi.org/10.1016/j.cose.2020.101968

Newman, Lily Hay (2016): *What We Know About Friday's Massive East Coast Internet Outage* (2016. október 21.). Online: www.wired.com/2016/10/internet-outage-ddos-dns-dyn

OWASP (2019): *Internet of Things Top 10* (2019. november 1.). Online: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Razali, Mohamad Faiz – Muhammad Nazim Razali – Fawwaz Zamir Mansor – Gopinath Muruti – Norziana Jamil (2018): IoT Honeypot: A Review from Researcher's Perspective. *2018 IEEE Conference on Application, Information and Network Security (AINS),* Langkawi, Malaysia, 93–98. Online: https://doi.org/10.1109/AINS.2018.8631494

Rizvi, Syed – Andrew Kurtz – Joseph Pfeffer – Mohammad Rizvi (2018): Securing the Internet of Things (IoT): A Security Taxonomy for IoT. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 163–168. Online: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

Shi, Linda – Fei Wang – Chung-Horng Lung (2018): Improvement of security and scalability for IoT network using SD-VPN. *NOMS 2018 – 2018 IEEE/IFIP Network*