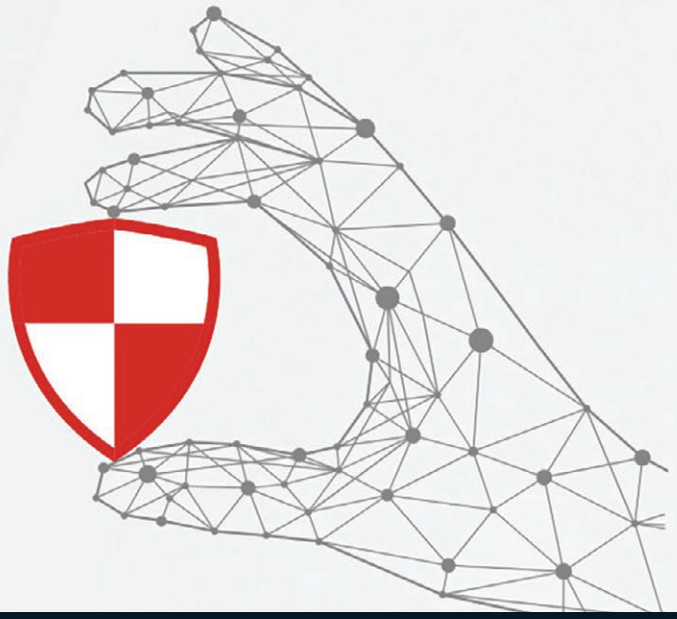
PROtaction [pratek[n]]

PROtACTION 2023

információbiztonsági konferencia

2023. május 4.



Az a jó az évenkénti PROtACTION-melléklet készítésében, hogy számvetésre kényszerít bennünket az elmúlt évről. Szerencsénkre sok hullámvölgyre nem hagyott lehetőséget a piac tavaly, egész évben ki sem látszottunk az érdekesebbnél érdekesebb feladatokból. Ismét sikerült 30 százalék feletti növekedést elérnünk, úgyhogy meglehetősen ki voltunk feszítve. Ezért idén januártól gőzerővel bővülünk, hogy az idei és az előttünk álló évek kihívásainak is meg tudjunk felelni.

Toltuk a kontentet is, ahogy a illik: több tucat cikk, konferencia előadás van a gallérunk mögött, és természetesen folytattuk gyümölcsöző együttműködésünket ennek a magazinnak a kiadójával podcast-területen. Idén ezeket a tartalmakat a saját oldalunkon elkezdjük utánközölni, hogy egy csokorban lehessen megtalálni, és akár archívumként, referenciaként szolgáljanak a megjelent anyagok. Nézzetek rá ti is! A menüpontot „Tudásközpontnak" hívják az oldalunkon. Ezen kívül idéntől négyre bővül a CLICO konferenciáinak a száma: túl vagyunk a „Conn@action" névre keresztelt, hálózatos és telekommunikációs technológiákkal foglalkozó alkalmunkon, most jön a security fókuszú esemény, ősszel folytatjuk a már két éve futó, a digitális identitásokra specializált napunkat, és hozunk majd októberre egy felhő és felhős technológiák biztonságával megtöltött dzsemborit is.

Figyeljétek majd a hírleveleinket!

Az idei lesz az ötödik élő PROtACTION konferenciánk, és mint mindig, most is hozunk új gyártót: tavaly ősszel kezdtünk el foglalkozni a Vectrával. A piacon már egy ideje jelenlévő cég friss energiákat szeretne bevonni a közép-európai piacon, így az egész CLICO-csoport Vectra-disztribútor lett. A kezdetek biztatóak, úgy néz ki, ez a sztori is sikerre van ítélve.

Az idei eseményen kipróbálunk valami újat: nem valamelyik gyártónk tartja a keynote-előadást, hanem felkértük az IDC-től *Bakk Józsefet,* hogy mutassa be szélesebb körben is azt a kutatást, amelyet tavaly ősszel készítettek a mi megbízásunkból. Ez a kutatás a legnagyobb cégek alatti, igen széles réteget öleli fel kiberbiztonsági beruházások és képességek szempontjából, néhány

FORRÁS: CLICO HUNGARY

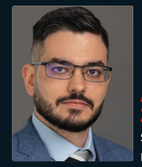
sokkoló megállapítással, és tudomásunk szerint ez az egyetlen, a kiberbiztonsági területen megvalósított reprezentatív felmérés.

Második keynote-előadónk *Bencsik Balázs,* kibervédelmi igazgató lesz az SZTFH-tól, aki a NIS2 néven ismert uniós jogszabálycsomag magyarországi vonatkozásáról fog beszélni. Húsba-pénztárcába vágó információk, senki ne hagyja ki!

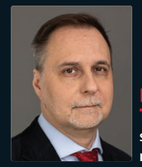
A délután folyamán pedig hozzuk a „formánkat": újabbnál újabb IT-biztonsági megoldások és eszközök bemutatói, ismertetői, demói fognak sorjázni. Lesz Palo Alto Networks, Forcepoint, SentinelOne, nCipher, Imperva, Radware, CyberArk, Recorded Future, Thales, Scirge, Nextsense, és Vectra előadás is.

Várunk benneteket május 4-én a Crown Plazaban, de előtte regisztráció: *www.protaction.hu*

May the 4th be with you,
Csinos Tamás
country manager



Almási Zsolt
senior rendszermérnök



Foki Tamás
senior rendszermérnök

Németh Mónika
senior rendszermérnök

Kamarás Bálint
security architect

Hogyan tovább SASE? Térhódítás, de hol és hogyan?

Ma már minden vállalat használ felhős szolgáltatásokat, azok is, amelyek kritikus infrastruktúrát kezelnek. Ezzel párhuzamosan a hatósági megfelelések egyre nehezebbé váltak. A biztonsági gyártók többsége is a felhőre helyezi a hangsúlyt a fejlesztési költségvetésében, a vállalatoknak viszont általában eszük ágában sincs teljes mértékig a felhőbe szerveződni, sok esetben inkább valamilyen hibrid eredmény születik.

Tapasztalataink alapján számtalan ilyen esetben lehet megoldás egy új generációs technológiai irány, csupán a piac ezt még nehezen ismeri fel.

FWaaS (Firewall as a Service, felhőben hosztolt tűzfal), ZTNA (Zero Trust Network Access, mondhatni újgenerációs VPN), SWG (Secure Web Gateway, azaz a lassan tényleg megboldoguló webproxy felhős kiadásban), CASB (Cloud Access Security Broker, ami vállalati webes szolgáltatások kontrollált elérését teszi biztonságossá), SD-WAN (Software-Defined Wide Area Network, mint okos felhordóhálózati technológia).

Ezeket hívószavakat már ismerjük, de az alábbi kérdésekbe már a legtöbbször beletörik a bicska: hogyan válasszunk, tervezzünk és implementáljunk egy integrációkra rendkívül érzékeny megoldást? Hogyan kezeljük azt, ha az ügyfél mindenféleképpen ragaszkodik a meglévő, sok esetben egyáltalán nem homogén módon kialakított infrastruktúrájához? Hogyan lehet felismerni egy SASE megoldás szükségét egy adott probléma megoldására?

A SASE áldásos tulajdonságai

Számtalan esetben tapasztaljuk azt is, hogy már egy „Proof of Material” ismeretében olyan előnyöket mutat fel ez a technológia, amelyek ritkán látott mosolyt csalnak az érintettek arcára, és nemcsak szakmai, hanem sokszor financiális szempontokból is.

A szakmai álláspontok talán triviálisak: egyszerűbb implementáció, mérsékelt üzemeltetési terheltség. A pénzügyi kérdések azonban már nem ilyen egyszerűek. Elsőre szinte hihetetlennek tűnhet, de sok esetben az ilyen projektek költsége adott időszakra bontva hatékonyabban optimalizálható. A szolgáltatók kiemelten érdekeltek jelenleg abban, hogy az általuk gigantikus erőforrásokat felemésztő megoldásokkal piacot nyerjenek. Aki ebben partner, az igen szimpatikus feltételekkel számolhat.

Gyakorlatiasabb irányból megvizsgálva a kérdést, létfontosságú tisztában lennünk egy szervezet méretével és szükségleteivel. Különbséget kell tudnunk tenni nemcsak egy bank és egy gyártósort üzemeltető nagyvállalat között, hanem számtalan más vertikumban, szabályozási környezetben, méretben létező cég között. Nincs két egyforma vállalat, két egyforma felhasználási mód, nincsenek kiforrott minták. Pontosan be kell határolni, hogy jelenleg hol tart a vállalati IT-kultúra a szervezeten belül. Mekkora az IT- és az IT-biztonsági érettség, és hova kívánunk eljutni egy, három vagy akár öt-tíz éven belül. Magas komplexitású, ebből fakadóan jól megtervezett, hatékony projektek lehetnek csak célravezetőek. Szinte tökéletes egyensúlyt szükséges teremteni a tervezettség és biztonsági fejlesztési ciklusok között. A speciális és gyakorlati tapasztalatból fakadó hozzáértés szintén elengedhetetlen.

Tűpontosan tisztázni kell a use case-eket

A SASE technológia implementálásához a különböző alapokkal és megközelítéssel rendelkező gyártók értelemszerűen különböző csomagokkal operálnak. A környezeti sajátosságoktól függően szükséges tervezni, választani és kivitelezni. A CLICO portfóliójában több, mint öt gyártó rendelkezik teljes vagy részleges SSE/SASE-megoldással, ezek közül most az általunk legjobbnak érzett három megoldást járjuk körbe a saját előnyeik és víziójuk mentén.

Kezdjük a **Palo Alto Networks** megoldásával. A SASE problémakörre a gyártótól megszokott kiterjedt, minden oldalról komplett megoldást nyújt. A Palo Alto Networks az általuk tökéletesített, új generációs tűzfal irányából indul, ezért egyértelmű, hogy a hálózatbiztonsági vonal nagyon hangsúlyos, és az ebből az irányból felmerülő ügyféligényeket a leghatékonyabban fedi. Ez a már régebben is elérhető **Prisma Access** nevű megoldásként található meg a portfóliójukban.

A Prisma Access lényege, hogy egy jól használható, könnyen kezelhető FwaaS-t, tűzfal-szolgáltatást adjon az ügyfelek kezébe, ahol nem kell üzemeltetni magát az infrastruktúrát, elég csak szabályrendszert kezelni, és minden mást megold a szolgáltatás. A fiókirodák, távoli telephelyek, a „földi” adatközpont, de még az ügyfelek is a felhőn keresztül csatlakoznak, és onnan szabályozzuk, hogy ki, mit, és hogyan érhet el.

A teljes SASE megoldás része a **Prisma SD-WAN** is, amely egy fejlett, kifejezetten a jó felhasználói élmény biztosítására kihegyezett, saját, natívan integrálódó SD-WAN megoldás. Ez az alkotóelem nyújtja a SASE megoldásoktól elvárt hálózatkezelés funkciót és segít optimalizálni a hálózati kapcsolatokat. A Palo Alto Networks talán legnagyobb előnye az ADEM (Autonomous Digital Experience Management) névre keresztelt egyedülálló funkcionalitás, amelynek segítségével teljesen automatizáltan végez a rendszer folyamatos, mélyreható analízist a hálózaton közlekedő forgalmakon és folyamatosan a változó paraméterek figyelembevételével optimalizálja a kapcsolatokat. Ez például a különböző, alacsony késleltetést igénylő szolgáltatások (VoIP, Zoom, Teams, egyéb kollaborációs megoldások, gyártásvezérlők, ipari rendszerek) által generált speciális és számottevő sávszélességi igények esetén felmerülő teljesítményproblémák kezelésében kiemelkedő.

A fent említett két fő elem segítségével egy kifejezetten hatékony, mesterséges intelligenciával megtámogatott, mindenki számára jól kezelhető és könnyen igénybe vehető megoldást kínál a gyártó, amelyhez nem szükséges bonyolult „földi” infrastruktúrát fenntartani, ám mégis kiemelkedő védelmet nyújt az ügyfelek számára. Fontos megemlíteni, hogy a csomag egy ideje tartalmaz egy DLP-megoldást is, amely a megfelelési szempontok miatt elengedhetetlen lehet bizonyos iparágakban. A Palo Alto Networks érdeme továbbá, attól eltekintve, hogy a megoldás egyben nagyon hatékony platformot alkot, az elemei külön-külön is Gartner leader kategóriába sorolhatóak, mivel az elemzők számára is egyértelmű, hogy érdemes velük számolni. Egyedüli SASE gyártóként találhatóak meg a Gartner SSE, SD-WAN és NGFW Magic Quadrantban is.

A Forcepoint SASE megoldása a **Forcepoint ONE,** amelynek alapjait a 2021-ben felvásárolt Bitglass adja, és ennek meglévő funkcióit folyamatosan fejlesztik és integrálják a Forcepoint korábbi megoldásaival. A Forcepoint évek óta jelentős szereplő az SD-WAN és CASB kategóriákban, de a legnagyobb előnye mégsem ebben rejlik a versenytársaival szemben. A gyártó hagyományaiból fakadóan elsősorban nem a hálózatbiztonsági, hanem adatbiztonsági alapok irányából közelíti meg a SASE-problémakört. A Forcepoint ONE Secure Web Gateway (SWG-), CASB- és ZTNA-lábak szinte adták magukat, és ezek sziklaszilárd stratégiai bástyája mellé épült fel egy igen fejlett tűzfal és SD-WAN összetevőket tartalmazó (FlexEdge) teljes körű, minden elvárt funkciót magába foglaló, teljes komplexitású rendszer.

Az olyan szükséges kiegészítők, szolgáltatások sem kerülték el a gyártó figyelmét, mint a Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM), továbbá a manapság egyre fontosabb RBI (Remote Browser Isolation) és Content Disarm and Reconstruction (CDR) funkciók. Az RBI képes megvédeni a felhasználót a böngésző alapú támadásoktól úgy, hogy a tényleges böngésző munkamenet egy távoli felhős sandbox-környezetben fut, és a helyi gépen csak e folyamat „interaktív képe” jelenik meg. A CDR pedig az interneten keresztül érkező dokumentumok tartalmának teljes szétbontását képes elvégezni, majd minden potenciálisan kártékony kód nélkül, egy újragenerált verzióban már biztonságosan meg is nyitható. Mindezt értelemszerűen valós időben. Külön érdekesség, hogy nemcsak képként kapja meg a felhasználó a tartalmat, hanem az eredeti file formátumában, Office dokumentumok esetén szerkeszthetően is.

A Forcepoint ONE legnagyobb előnye a piacvezető Forcepoint Enterprise DLP-vel való integrálhatósága, amelynek révén a felhős környezetekre és a keresztül haladó forgalmakra is ki lehet terjeszteni védelmet, a földi DLP-ben megalkotott szabályrendszer szerint képes kutatni a felhőben tárolt érzékeny információk után, és szükség esetén blokkolni tudja az érzékeny információk szivárgását. Tapasztalataink szerint a versenytársak által ez az egyik leginkább lefedetlen terület, inkább csak „DLP Light” kezdeményeket építenek be a saját SASE-megoldásukba.

Összefoglalónkban a harmadik gyártónk a **Netskope.** Olvasóink többségének még nem feltétlenül cseng ismerősen a gyártó neve – csak egy éve kezdték meg európai menetelésüket –, de ennél jelentősebb a Netskope megoldásának jó néhány technológiai finomsága. Ráadásul a már említett gyártóktól eltérően a SASE a Netskope főprofilja, és ezen a piacon úttörő szerepe van.

A Netskope jelen pillanatban több mint 65 régió adatközpontjaiba telepített, saját maga által kezelt privátfelhő-szolgáltatást kínál ügyfeleinek, és minden adatközpontból egységesen biztosítja az összes elérhető szolgáltatási funkciót. Ez mindenképpen egy keresett és ritka privilégium, amellyel azoknál ügyfeleknél biztosan előnyt élveznek majd, akik nem szeretnének egyik nagy felhőszolgáltató felé sem elköteleződni, vagy nem szeretnék a hibrid, netán multicloud infrastrukturájukat a szükségesnél jobban kitenni, például egy Amazonos (Azure-os, Google-os, stb) kiesés esetén az Azure-os (Amazonos, Google-os, stb.) workloadok elérését elveszíteni.

Az Netskope SSE-irányból épített SASE-megoldását szintén megkülönbözteti a versenytársaktól, hogy a szolgáltatásokat egyetlen platformról biztosítja. Egyetlen konzolon tudunk minden funkciót használni, és az egyes modulok tökéletesen integráltak, ami lehetővé teszi, hogy a forgalmakon belüli különböző összefüggéseket könnyen észleljük.

A Netskope 2022. augusztusi Infiot-felvásárlásával egy addig hiányzó elem, egy Borderless SD-WAN megoldás is került a csomagba. A SASE biztonsági részét a Netskope Intelligent SSE biztosítja, amely tartalmazza az elvárt CASB-, FWaaS-, SWG-, ZTNA-, RBI-funkciókat. A Netskope-t mindezek mellett úgy tervezték meg, hogy nemcsak TCP és HTTP alapú forgalom kezelésére alkalmas, hanem API szinten vizsgálódik, így „megérti” a felhasználók szándékát, hogy milyen tevékenységet végeznek éppen, így több összefüggésben is biztonságot tud nyújtani. A Netskope SASE megoldás alapja a NextGen SWG, amely nem csak allow/block kontrollokat nyújt, hanem megérti az adatfolyamok a kontextusát. A Netskope CASB egyébként az iparág vezető felhőalapú CASB megoldása, több ezer felhőalkalmazás azonosítására és kezelésére, a különböző fenyegetések valós idejű észlelésére és orvosolására képes.

Négykilences rendelkezésre állás

Mindhárom gyártó esetében 99,99 százalékos vállalt rendelkezésre állással számolhatunk a platform tekintetében, és POP-ok (Cloud Point of Presence) vonatkozásában szintén a bőség zavarával szembesülünk, akárcsak a skálázható teljesítményt illetően. Ezeket megfejelve az ugyan gyártónként eltérő, de minden esetben könnyen átlátható és rugalmas előfizetési modellek között biztosan mindenki megtalálja a számára szimpatikusat.

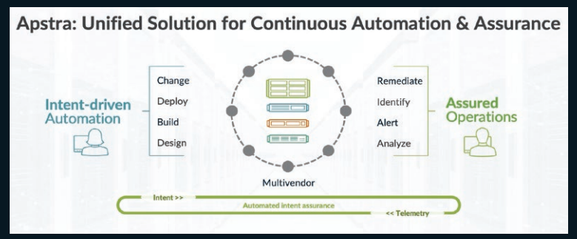
Összességében tehát kijelenthető, hogy mindegyik megoldás több mint megfelelő lehet a környezeti sajátosságok és a felhasználás céljának függvényében, az adott feladatra legalkalmasabb belépési pontot – gyártót, technológiát – pedig szakértőink segítségével már egyszerűbb lesz meghatározni. ■

Németh Mónika
senior rendszermérnök

Juniper Apstra, az adatközponton innen és „tool”

Az alábbi cikkben azoknak a kedves olvasóknak szeretnénk egy kis ízelítőt adni, akik adatközpontot üzemeltetnek, és szeretnék egyszerűbbé tenni ennek a feladatnak a mindennapos megpróbáltatásait, és persze mindenkinek, aki „csak” érdeklődik a téma iránt.

A **Juniper Apstra** egy olyan kulcsrakész, szoftveres, „intent-base” megoldás, amely lehetővé teszi, hogy több gyártótól származó eszközparkból felépített adatközpont esetében is automatizálható legyen az adatközponti hálózatok tervezése, építése, telepítése és üzemeltetése. Segítségével egyedülálló képet kaphatunk az adatközponti elemek közötti kapcsolatokról és kölcsönös függőségekről.



Szándék alapú hálózatkialakítás

Mielőtt egy kicsit elmélyednénk a témában, nézzük meg, hogy mit is jelent maga az „intent-base” networking. A fogalom alatt egy szoftverrel támogatott automatizálási folyamatot értünk, amely magas szintű intelligenciát, analitikát és finomhangolást használ a hálózati működés és az üzemidő javítása érdekében. Gyakorlatilag az „intent-base” alatt azt a fajta megközelítést értjük, miszerint elegendő az Apstra számára azokat a dolgokat definiálnunk, hogy mit szeretnénk elérni, mire van „szándékunk” (intent), mire van szükségünk és ezen információk alapján a végső megoldást (konkrét eszköz, amely megfelel a követelményeinknek; az eszközökön beállítandó konfig) maga az Apstra fogja számunkra megadni.

Például tegyük fel, az az igény, hogy két hálózat között legyen biztonságos kommunikáció. Ebben az esetben az „intent” azt mondja ki nagyjából, hogy az „A hálózat” és a „B hálózat” között egy biztonságos tunnelre van szükség. Továbbá meghatározzuk, hogy melyik forgalom használhatja ezt a tunnelt, illetve a tunnel egyéb általános tulajdonságait is definiálnunk kell. De – és ez a lényeg – nem kell meghatároznia tunnel tényleges megvalósításának a módját, és azt sem, hogy milyen konkrét szolgáltatásokat és paramétereket kell bekapcsolni a tunnel működéséhez. Ehelyett egy intent-base hálózati rendszer az összes eszköz teljes konfigurációját képes a szándék leírása alapján automatikusan generálni. Ezután pedig folyamatos ellenőrzéseket tart fenn a hálózat tervezett és tényleges üzemi állapota között, hogy szükség esetén az eltérések javíthatók legyenek.

Építkezés moduláris elemekből

Az Apstra-ban az adatközpont modellezéséhez különböző, újra felhasználható építőelemeket használnak. Az első ilyen a **logical device.** Ez gyakorlatilag a célunk egyszerű leírása, például egy leaf switch. Ez teljes mértékben gyártófüggetlen, ténylegesen a lehető legegyszerűbb módja annak, ahogy az elvárásainkat le tudjuk írni. Például szükségünk van 8 db 25 GbE és 4 db 100GbE portra az eszközön, valamint megadhatjuk, hogy ezekhez a portokhoz mit szeretnék csatlakoztatni (a 25 GbE portokhoz szervereket, a 100GbE portokat pedig például a spine switchekhez). Tehát ez egy high-level leírás, semmi hardverspecifikus definíció, csak az alapvető elvárásaink.

A következő építő elem egy **rack**. Például megadhatom, hogy ebben a rackben 2 leaf switchet szeretnék használni, aztán meghatározhatom magukat a szervereket is, amelyek szintén logikai eszköz szinten lesznek modellezve.

A következő építőelem a **template.** Ez az a hely, ahol a különböző logikai eszközöket és rackeket össze tudom rakni egy feltételezett adatközponttá. Itt már a L2/L3 elvárásainkat is meg tudjuk adni, de például az adatközpontból kivezető linkeket is itt lehet definiálni. A template-et egyéb, az „élő” adatközpont tulajdonságaival felruházva tudjuk **a blueprintet** létrehozni, ahol már VLAN-ok, security zónák, VRF-ek, VxLAN-ok, VMware integráció stb. is megadható. Persze a rendszerből nem hiányozhatnak a konkrét hardverek sem, ahol megmondjunk, hogy konkrétan melyik switch modellt és azon melyik operációs rendszert szeretnénk használni. Természetesen az eszközök összekapcsolódnak azokkal az elvárásokkal, amelyeket az előményekben definiáltunk.

A **Juniper Apstra** megoldásával jelentős segítséget kaphatunk az adatközpontunk üzemeltetéséhez, egészen a tervezési fázistól kiindulva. A megoldás a nulladik lépéstől egészen az üzembe helyezésig támogatja a munkánkat, és utána még felügyeli is az adatközpont működését. Az már csak hab a tortán, hogy magának a konfigurációnak az elkészítését is automatizálhatjuk az Apstra segítségével, és ugyan a Juniper kínálatában is érhető el megoldás, de ahogy említettük, a támogatott eszközök nem korlátozódnak a Juniper adatközponti kínálatára. ■

Almási Zsolt
senior rendszermérnök

A fehérkalapos kémtevékenység

Már az elmúlt évben is nagy hangsúlyt fektettünk a CTI (Cyber Threat Intelligence) iránti igények felmérésére, illetve a CTI-megoldások bemutatására. Mostanra be is érett a gyümölcse: egyre több szervezet ismeri fel a kiberhírszerzésben rejlő lehetőségeket: tényleges védelmi funkciókat, a security analyst csapatok tehermentesítését.

Nagy segítség lehet a vállalatok számára egy jól használható, külső információforrás, amely segíti az IT-biztonsági rendszerek mindennapos, hatékonyabb használatát. Ha belegondolunk, hogy mekkora kapacitás kellene ahhoz, hogy folyamatosan figyeljük azt a ma már több mint egymillió forrást, amelyből például a **Recorded Future** dolgozik, rájöhetünk, hogy kézzel gyűjtve, vagy kevésbé professzionális, ingyenes feed-ek használatával sem jutunk olyan mennyiségű és minőségű információhoz, ami valódi segítséget jelenthet.

Ezek a platformok az IOC- (Indicators of Compromise, a támadási technikákat leíró adatsorok) listái, és a hozzájuk tartozó háttérinformációik miatt kerülnek a középpontba. Értékes tud lenni, ha nemcsak arra támaszkodunk, hogy a tűzfalgyártónk vagy végpontvédelmi megoldásunk milyen támadásokat vagy támadókat ismer, hanem az internet legmélyebb bugyraiból is tudunk információkat szerezni a támadók technológiáiról, és ezeket kontextusba is tudjuk helyezni.

Egy modern CTI-platform már nemcsak a védelmi rendszereinkhez szolgáltat extra információkat, hanem modulárisan, különböző célokra is tudjuk használni a kiterjedt képességeket. A Recorded Future esetén ilyen például az Attack Surface Management, azaz a támadási felületünket monitorozó képesség, amely folyamatosan kívülről vizsgálja az internetet, és rávilágít arra, hogy milyen sérülékenységek, illetve problémák vannak a hozzánk tartozó szerverek, szolgáltatások esetén. Ne várjuk meg azt, amíg egy támadó felfedi és kihasználja ezeket, hiszen mi magunk, proaktívan, a jelzések alapján kezelhetjük a felmerülő problémáinkat.

Leválasztott működés

Nemrég jelent meg a Recorded Future kínálatában egy újdonság, a sandboxolás lehetősége. A sandbox technológia korábban is egy fontos pillére volt a vállalati security elemzéseknek, viszont a Recorded Future esetén külső szolgáltatásként volt csak elérhető. Jelenleg a CTI-platfomon belül, bizonyos szolgáltatásokhoz akár ingyenesen elérhető a Recorded Future Hatching sandbox, amely hasznos információkkal lát el minket azzal kapcsolatban, hogy a fájlról futtatással, illetve statikus elemzéssel konkrétan mit sikerült észlelnie a rendszernek. Például adott esetben azt is megmutatja, hogy melyik malware-családhoz tartozik a bejutni próbáló kártevő. Ezeket kombinálva a rendszeren belül már megtalálható információkkal nagyon ütőképes eszközt kapunk a kezünkbe.

Szintén hasznos lehet, ha felhasználóink adataival kapcsolatosan is kapunk visszajelzéseket. Képzeljük el azt az ideális állapotot, amikor regisztrált felhasználóinknak, vagy céges, belső rendszer esetén a kollégáinknak, egy jól kialakított workflow segítségével tudjuk jelezni, hogy vélhetően kisziváro gtak a belépési adataik. Ezekhez a forrásokat a deep és darkweb különböző piactereiről, illetve egyéb forrásokból is közösen kezelve figyeli a rendszer, és riaszt, amikor szükséges.

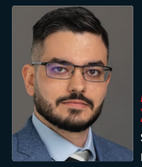
A beépülés fontossága

Sokat emlegetjük az integrációt, kicsit vizsgáljuk meg részletesebben: egy jól működő CTI-platform legfontosabb tulajdonsága, hogy a különféle rendszereinkkel is tudjuk integrálni, tud az adott rendszernek értelmezhető, értékes információt átadni. A különbségeket CTI és CTI között főleg akkor fogjuk megtapasztalni, ha az integrációk minőségét vizsgáljuk, illetve azt, hogy ezek egy vagy két irányú integrációk.

A Recorded Future esetén a legtöbb integráció könnyen kezelhető, és API-kulcsok megadásával működnek. Ezek segítségével tudunk többek között különálló rendszerekkel, mondjuk végpontvédelmi megoldásokkal is integrálódni (ilyen például a CLICO portfóliójában található **SentinelOne**), vagy lehetőségünk van dedikált információelosztó, ún. TIP- (Threat Intelligence Platform) megoldással integrálódni, például az open source MISP-el, amely utána szétosztja az egyes alrendszerek között az infókat. Ezek a komplexebb integrációk, amelyeket TIP- vagy SOAR- (Security Orchestration Automation and Response) irányban hozunk létre, képesek a folyamatainkat automatizálni, és a CTI-platformba közvetlenül nem bekötött rendszereinket is táplálni.

Itt is ChatGPT

Az integrációkon és a korábbi funkciókon felül még egy vadonatúj megoldással újított április közepén a Recorded Future: a nyelvi modell alapú generatív mesterséges intelligencia rendszerek felé is nyitott, elsőként az OpenAI üstökösét, a ChatGPT-t építették be. A platform a rendelkezésére álló óriási mennyiségű adatból és már elkészült elemzői riportokból teljesen önállóan képes (AI és GPT alapokon) saját szöveges riportokat is gyártani. Ezek a használatával tovább javítható a rendszer hatékonysága, és még több terhet képes levenni az elemzők válláról. Ugyan a riportkészítés a gyártó szerint, és a használt technológia természetéből fakadóan is igényelhet emberi felülvizsgálatot, de még így is hatalmas mértékben képes csökkenteni az elemzőktől elvárt munkamennyiséget. ■



Almási Zsolt
senior rendszermérnök

Identitásvédelemmel bővült a portfólió

Nem először írunk különféle XDR-technológiákról, és az ezt övező piaci trendekről, ugyanakkor évről-évre felbukkannak újdonságok, hiszen ebben a szegmensben sem pihennek a meghatározó gyártók fejlesztőcsapatai. Ugyanakkor az elmúlt időszakban nemcsak a fejlesztések határozták meg a SentinelOne körüli változások irányát, hanem egy figyelemre méltó felvásárlás is, amelynek köszönhetően a gyártó portfóliója tovább bővült az akvirált vállalat, az Attivo termékeivel.

Az **Attivo** felvásárlásával a korábban is létező együttműködés magasabb szintre lépett: a **SentinelOne** platformon belül is elérhetővé váltak az Attivo funkciói. Ezekkel a funkciókkal a védelmi képességek kiterjedhetnek a különböző identitásokat tartalmazó környezetekre is. Ez alatt nemcsak azt kell érteni, hogy feltehetjük a S1 XDR agentet szerverekre is – ez már régóta elérhető –, hanem azt, hogy az új modullal olyan fejlettebb képességeket kapunk, amellyel az AD- (Active Directory) funkcionalitást is meg tudjuk védeni.

A modul többek között javaslatokat ad arra is, hogy miként tudjuk biztonságossá tenni a cégnél lévő felhasználók kezelését akár a „földön”, akár a felhőben. Ha ezeket a javaslatokat megfogadjuk, jelentősen csökkenthetjük a kockázatainkat, hiszen a legtöbb támadás alapvetően a magas jogosultságokkal rendelkező felhasználókra, és ezáltal az ő, praktikusan az AD-ban tárolt identitásuk kompromittálására fókuszál.

A domain controllerekre kihegyezett támadási felület felszámolásán kívül a rendszer képes riasztani olyan esetekben is, mikor a támadó már bejutott, és a megszerzett hozzáférési adatokkal próbál visszaélni vagy a rendszereinket kompromittálni. Fontos, hogy ezeket a támadásokat nemcsak a már SentinelOne menedzselt végpontok irányából képes észlelni, hanem korlátozás nélkül bárhonnan. Így a laterális mozgás észlelését, és az ilyen jellegű próbálkozásokat is hatékonyan ki tudjuk védeni.

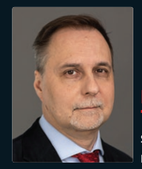
Az új képességek listája ezzel még nem ér véget, sőt talán az összes közül a legérdekesebb újdonság a deception-t, azaz a megtévesztést alkalmazó technológia integrálása a S1 XDR

platformba. Ezzel a támadókat becsapva, megtévesztve egy honeypot-hálózat irányába tudjuk csalni, így késleltetve, vagy adott esetben megakadályozva a támadást. Minden, a honeypot felé irányuló interakció hasznos információ a védekezésben, hiszen jogosan feltételezhetjük, hogy rosszindulatú támadás vagy felderítés miatt lépett valaki kapcsolatba a honeypottal.

Az új funkciók mind nagyon jól kiegészítik az évek óta a technológia élvonalába sorolt végpontvédelmi képességeket. Érdemes azt is megemlíteni, hogy nemcsak felvásárlással fejlődött a platform az elmúlt időszakban: több újítás között van az is, hogy már egy közös konzolról kezelhetjük a mobil és a hagyományos operációs rendszerű végpontjainkat is. A SentinelOne Marketplace-nek hívott felületén keresztül az elérhető 3rd party integrációk száma is folyamatosan növekszik, a nagy gyártók megoldásait már pár kattintással integrálhatjuk a megszokott, kiterjedt, natív API alapú integrációk mellett. ■

Kívánatos célpontnak tűnik

A honeypot – „mézesbödön”, csalétek – rendszerek valós adatokat nem tárolnak, ezért a „valódi” felhasználóknak nem kell kapcsolatba kerülniük ezekkel a hétköznapokban, viszont a működésüket tekintve teljes értékű elemnek, kiszolgálónak, magas jogosultságú végpontnak, vagy egyéb olyan fontos entitásnak látszanak, amiért a támadók szeretnék közelebbről is megismerni.



Foki Tamás
senior rendszermérnök

Vectra AI, az MI-vel támogatott NDR és a Sentinel One

A hagyományos biztonsági megoldások gyakran nem képesek lépést tartani a fejlett és folyamatosan változó fenyegetésekkel, amelyek kihasználják a hálózatok komplexitását és heterogenitását. Ebben a helyzetben egy új megközelítésre van szükség, amely képes automatizálni a fenyegetések észlelését és kezelését mesterséges intelligencia (AI) segítségével.

Egy ilyen megközelítést kínál a **Vectra,** amely egy piacvezető hálózati észlelési és válaszadási (NDR, network detection and response) platform. Olyan, AI alapú technológiát használ, amely képes tanulni a hálózati viselkedésből és felismerni az anomáliákat és támadási mintákat. A Vectra AI nemcsak észleli a fenyegetéseket, hanem rangsorolja őket az üzleti kockázat alapján, és javaslatokat tesz a válaszadásra. A Vectra fontos tulajdonsága, hogy a legkülönbözőbb (felhő, SaaS, adatközpont, IT, IoT) hálózatokon is képes működni, hogy teljes láthatóságot biztosítson a kibertérben. A Vectra az AI által vezérelt analitikának köszönhetően csökkenti a támadások észlelési idejét, és növeli az észlelések hatékonyságát, ahogy segít csökkenteni az emberi tényező hatását, és kevesebb emberi erőforrást, kevesebb manuális folyamatot igényel. Épp csak kávét nem főz.

Az operátorok munkáját nagyban segíti, hogy a Vectra alkalmazza a Mitre Att&ck® framework terminológiáját, amely egy olyan tudásbázis, amely a kibertámadók taktikáit és technikáit gyűjti össze valós megfigyelések alapján. A framework a teljes támadási életciklust lefedi, beleértve a felderítést, a behatolást, a hálózaton működő eszközök közötti laterális mozgást, a jogosultsági szintek emelkedését és a Command and Control kommunikációt, majd a megszerzett információk kiszivárogtatását.

Mivel gyakorlati szempontból, az ellenfél szemszögéből vizsgálja a folyamatokat, hogy azok milyen célokat akarnak elérni, és milyen konkrét módszereket használnak, ezért a Mitre Att&ck® frameworkot az IT-biztonsági rendszerek egyre gyakrabban alkalmazzák, ezzel egy közös incidensleíró nyelvet biztosítva számukra.

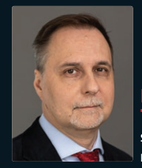
A Vectra több mint 90 százalékos lefedettséget biztosít a Mitre Att&ck® framework taktikái és technikái közül, támogatja a Mitre D3FEND keretrendszert is, amely az egyes támadásokkal szembeni megfelelő védekezési javaslatokat tartalmazza. A Vectra 12 olyan szabadalmat birtokol, amelyek a D3FEND keretrendszerben meghatározott ellenintézkedések alapját képezik.

Emellett képes integrálódni más biztonsági rendszerekkel, például tűzfalakkal, végpontvédelmi megoldásokkal vagy incidenskezelő platformokkal, hogy automatizálja a támadásokra adott válaszokat, és gyorsítsa az incidensek vizsgálatát. Ilyen integrációra példa **a Vectra és a SentinelOne XDR** platform együttműködése, hogy minél teljesebb körű láthatóságot, pontosabb észleléseket, az incidensek priorizálását és megfelelő reagálást biztosítsanak a hálózati hosztokon, a felhős munkafolyamatokon, identitásokon, és a végpontokon.

A Vectra által generált észlelések és kockázati pontszámok bekerülnek a SentinelOne rendszerébe, ahol összekapcsolódnak annak szintén mesterséges

intelligenciával segített viselkedésalapú észleléseivel, amelyek a támadások olyan jellemzőit és viselkedését tárják fel, amelyek csak a hoszt belsejében láthatók. Ezen túlmenően a SentinelOne végponti észlelései és telemetria adatai is bekerülnek a Vectra Cognito UI felületébe.

A két megoldás így kombinálja a hálózati folyamatoknak és a hosztok belső folyamatainak észleléseit és így együttesen magasabb védelmi szintet hoznak létre, és fejlett, automatizált, szabályvezérelt válaszadási képességekkel rendelkező rendszert kínálnak a fenyegetések gyors megszüntetésére, és ezzel nagyban segítik az incidensek felderítését és az azokra reagálást az IT/SOC csapatok számára. ■



Foki Tamás
senior rendszermérnök

Automatizálható incidenskezelés: XDR for beginners

Az XDR (eXtended Detection and Response) napjaink gyorsan fejlődő és rohamosan terjedő, több rétegű IT-biztonsági technológiája, amely több biztonsági rétegből származó adatokat és telemetriát gyűjt és korrelál, beleértve végpontvédelmi, hálózatvédelmi megoldásokat, alkalmazásokat.

Mivel az XDR megoldások több területet is lefednek, ezért egyre vonzóbbak az ügyfelek számára, akik így több, addig különálló megoldást tudnak konszolidálni egy terméken belül. Mint a legtöbb friss technológia esetén, itt sem beszélhetünk egységes termékkategóriáról, az egyes gyártók attól függően, hogy a piac melyik irányából érkeznek, más-más területen tapasztaltak, és ennek megfelelően mások az XDR megoldásaik erősségei.

Az amerikai **Rapid7**-nek is van saját XDR-megoldása, amelyet **InsightIDR**-nek hív, ez a gyártó a Gartner által is a piacvezetők közé sorolt SIEM-megoldásának evolúciójával lépett be ebbe a kategóriába. A gyártó a fejlett SIEM-rendszerét egészítette ki az évek során a hálózati szenzorral, hogy legyen telemetriája, deception funkcionalitással, fejlett viselkedés analitikai (UEBA és ABA) modulokkal, amelyek nemcsak a felhasználók viselkedését vizsgálva von le következtetéseket, hanem a naplókból a támadók viselkedésére utaló nyomokat keresve is.

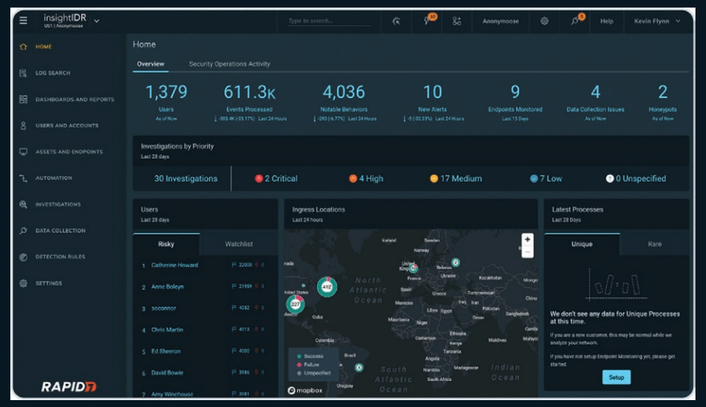
Az üzemeltető biztonsági csapatok munkáját és magát a megoldás bevezetését is nagyban segíti, hogy az InsightIDR több tucatnyi biztonsági megoldás log formátumát alapból ismeri, és ezek egyszerűen hozzáadhatók a rendszerhez, továbbá a bekötött eszközök naplóit több száz, a Rapid7 által előre megírt korrelációs szabály vizsgálja és anomália esetén riaszt. Ezeket a szabályokat a gyártó folyamatosan finomhangolja, és újakat ad hozzá, ezáltal biztosítja a lehető leghatékonyabb felismerést és reagálást a támadások esetén.

A rendszerbe bekötött alkalmazásokból érkező naplókat, a hálózati szenzor és a deception rendszer észleléseit egészítik ki a Rapid7 Insight Agentjéből érkező végponti információk is. Ezekből az adatokból nyerhető forensics információkat egy, a Mitre Att&ck® framework terminológiáját használó fejlett felületen gyűjtik össze, és ennek használatával teszik hatékonyabbá az SOC-csapatok elemzőinek az incidensek utáni analitikai munkáját. Így az InsightIDR, mivel SIEM-rendszerként a legkülönbözőbb források naplóit is megkapja, sokkal több információból képes dolgozni, mint más, csak egy-egy részterületre fókuszáló végpontvédelmi megoldás.

Miután az InsightIDR egy felhős környezetben futó SaaS, nincsenek bonyolult architektúratervezési feladatok, a gyártó pedig biztosítja a mindenkori szükséges számítási és tárolási kapacitásokat, így nincs infrastruktúra probléma a növekvő igények és újabb alkalmazások bevezetése esetén sem.

A Rapid7 a felhős szolgáltatásait egy egységes, Insight Platformnak hívott környezeten biztosítja, ahol az egyes ügyfelek adatai egyedi titkosítással, csak az ügyfél számára elérhető módon tárolódnak. Az előre megírt csatlakozók révén nagyon egyszerű az Insight Platformon nyújtott további szolgáltatások használatba vétele és összekötése a meglévő modulokkal. Így például a gyártó InsightConnect SOAR-megoldásával az InsightIDR egyszerűen bővíthető fejlett automatizálási képességekkel, vagy a ThreatCommand CTI technológiájával, de akár az InsightCloudSec multicloud és konténeres környezetek védelmét és felügyeletét ellátó CNAPP/CWPP/CIEM/CSPM funkcionalitással is.

A fentiek miatt megfontolandó az InsightIDR az olyan ügyfelek számára is, ahol csak kisebb biztonsági csapat van, korlátozottabb helyi erőforrásokkal, vagy esetleg tartanak a hosszas integrációs, telepítési és üzembeállítási folyamatoktól, de szeretnének fejlett SIEM- és XDR-szolgáltatásokkal rendelkező eszközt az incidensek kezelésére, azok kivizsgálásának gyorsítására és így a szervezet biztonsági szintjének növelésére.



RAPID7

Németh Mónika
senior rendszermérnök

Infinera XTM+800G, avagy száguldás fénysebességgel

Az Infinera a tavalyi megjelenésünk óta az egyik új gyártó, akinek a megoldásait képviselhetjük a Clico Magyarország portfóliójában. Az Infinera legfőképpen a távközlési szolgáltatói piac számára gyárt WDM (Wavelength Division Multiplexing) alapú optikai átviteli berendezéseket, valamint úttörő szerepet tölt be a PIC (Photonic Integrated Circuits, optikai integrált csipek) tervezésében és gyártásában.

Meglévő optikai infrastruktúránknak, akár bérelt, akár saját tulajdonú, véges a terhelhetősége, sávszélesség-bővítés nélkül a folyamatosan növekvő adatmennyiséggel egyre kevésbé hatékonyan fog megbirkózni. Mivel újabb optikai szálak elhelyezése nem megy egyik napról a másikra, érdemes azon elgondolkodni, hogy van-e esetleg lehetőség a meglévő szálak jobb kihasználására. Itt jönnek képbe az Infinera megoldásai, amelyek közül az **Infinera XTM** csomagkapcsolt transponder-sorozatot és a hozzá való 800G optikát mutatjuk most be.

Az Infinera XTM sorozatú csomagkapcsolt optikai hálózati platform nagy teljesítményű metro access, aggregation és core hálózatokat biztosít. Az XTM sorozat minden olyan képességgel rendelkezik, amely egy rugalmas és jövőálló metro network igényeinek megfelel. A Layer0 optikai hullámhossztól egészen a Layer2.5 MPLS-TP-ig nyújt támogatást az Ethernet, OTN, SDH/SONET, Fibre Channel és Intelligens WDM (iWDM®) technológiák használatával. Az XTM sorozat olyan kulcsfontosságú tulajdonságokkal rendelkezik, mint az alacsony fogyasztás, nagy portsűrűség és nagyfokú skálázhatóság.

Az XTM sorozat legújabb bővítésével már az XR optikák is használhatók a platformban. A 400 Gb/s támogatása mellett, az XTM sorozat mind a 600 Gb/s-os, mind a 800 Gb/s-os nagyobb sebességű DWDM támogatására is alkalmas az Infinera GX sorozatú transponderein keresztül.

Az Infinite Capacity Engine hatodik generációja (ICE6) az Infinera Advanced Coherent Optical Engines and Subsystems-től egy 1,6 Tb/s-os optikai engine, amely két, egyenként maximum 800 Gb/s sebességgel működő, egymástól függetlenül programozható hullámhosszt biztosít. Egy tipikus koherens optikai

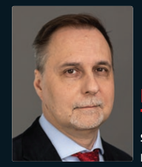
motor belsejében lévő kulcselemek közé tartozik a digitális ASIC/DSP, az analóg elektronika és fotonika, valamint rádiófrekvenciás (RF) összeköttetések. A digitális ASIC/DSP kulcsszerepet játszik az adó-vevő teljesítményében és a funkcionalitásában is.

Az Infinera ICE6 optikákban is a 7 nm-es CMOS-t használják, amellyel 30%-os teljesítménynövekedést és 60%-os áramfelvétel csökkenést érhetünk el. Ez az extra teljesítmény a nagyobb adatátviteli sebesség és a fejlett, processzorigényes szolgáltatások kulcsfontosságú eleme. Ezeknek köszönhetően az ICE6 ultramagas adatátviteli sebességet, magas modem SNR-t és innovatív funkciókat használ a teljesítmény és a spektrális hatékonyság korlátainak áttörése érdekében, beleértve a 800 G egyhullámhosszú teljesítmény több mint 1000 km-en keresztüli biztosítását. Az ICE6 lehetővé teszi a hálózatüzemeltetők számára, hogy megfeleljenek a gyors sávszélesség-növekedés által támasztott követelményeknek. Az Instant Bandwidth segítségével pedig az ICE6 kiterjeszti a szolgáltatók azon képességét, hogy gyorsan növeljék, áthelyezzék és visszavonják az átviteli kapacitást, ott és akkor, ahol szükség van rá.

Ismerjük meg az Infinera nevet!

Egy 2000-ben alapított, amerikai agytröszttől van szó, innovációi folyamatosan megújítják az optikaitranszport-piacot. Találmányaikat az összes versenytársuk rendelkezésére bocsájtják, így a nagy hálózati gyártók berendezéseiben szinte kivétel nélkül megtalálhatóak az Infinerától származó fejlesztések. Több mint 2000 bejegyzett szabadalmuk révén mindig a versenytársak előtt járnak sebességben és megbízhatóságban. Az Infinera mindent az Egyesült Államokban és Svédországban gyárt.
Komolyabb kereskedelmi tevékenységüket Európában a svéd Transmode 2015-ös felvásárlásával kezdték, ezt erősítette a 2018-as Coriant (korábban Siemens, később Nokia-Siemens cég) akvizíciója.

Infinera



Foki Tamás
senior rendszermérnök

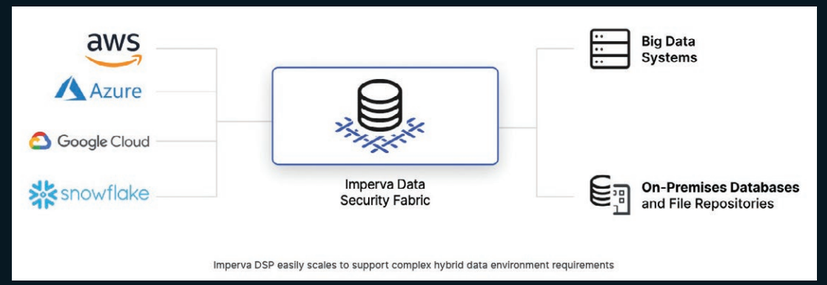
Imperva Data Security Fabric

A napjainkban zajló digitális transzformáció, azaz, hogy a szervezetek digitális eszközök és megoldások alkalmazásával növelik hatékonyságukat, számtalan új kihívást hoz az IT-rendszereket üzemeltetők számára, akik hajlamosak az adatbázisok védelméről megfeledkezni és csak a hagyományos végpont és hálózat védelmi megoldásokra koncentrálni. Pedig az adatbázisokban lévő adatok a szervezetek legértékesebb erőforrásai. Hogy védhetjük meg őket?

Az adatbázisokban tároljuk ügyfeleink, partnereink, termékeink, szolgáltatásaink értékes információit, amelyek nélkülözhetetlenek a hatékony működéséhez. Ha ezek az adatok sérülnek, elvesznek, illetéktelen kezekbe kerülnek, az súlyos károkat okozhat: a szervezet reputációjának, jövőbeni üzleti lehetőségeinek rontásával, és nem utolsó sorban számtalan jogi kötelezettség és a legkülönfélébb szabályozások is megsérülnek.

Nem könnyíti az IT biztonságáért felelős csapatok munkáját, hogy az adatbázisok ma már sokféle környezetben működhetnek. A hagyományos, „földi” adatbázisok mellett egyre gyakoribbak a felhős környezetben használt adatbázisok, és az ilyen összetett, akár hibrid környezetekben is működő szervezetek számára további problémát jelent ezekre egységes szabályokat kikényszeríteni, egységes felületen kezelni ezeket.

A fentiekre kínál megoldást az **Imperva,** az iparágvezető biztonsági szolgáltató, amely termékeivel a kibertámadásoktól védi a webes alkalmazásokat, az adatbázisokat és a felhő infrastruktúrát, felismeri és blokkolja a rosszindulatú



Imperva DSP easily scales to support complex hybrid data environment requirements

forgalmat, megakadályozza az adatszivárgást, és segít a szabályozási előírásoknak való megfelelésben. Az Imperva több mint 6500 ügyfelet szolgál ki világszerte, köztük pénzügyi intézményeket, kormányzati szerveket és e-kereskedelmi vállalatokat.

Ez a platform képes felügyelni és ellenőrizni az összes adattevékenységet, legyen az hagyományos adatbázisokban, adattárházakban, felhőalapú tárolókban és big data platformokon. Integrálódik a meglévő adatforrásokkal és infrastruktúrával, valamint támogatja a legújabb technológiákat is, mint például a felhőalapú adattárházak, a NoSQL adatbázisok és a Kubernetes konténeres környezetek is.

– Az Imperva Data Security Fabric képes a legkülönbözőbb adatbázisokban lévő adatokat feltérképezni és osztályozni, valamint segít egységes képet adni a tárolt adatok helyéről és típusáról. Ezekkel a funkciókkal segít felismerni az adatbiztonsági kockázatokat, hogy a szervezetek időben észleljék és reagáljanak az adatsértésekre és a fenyegetésekre.

– Az Imperva Data Security Fabric nagy segítséget nyújt testreszabható adatvédelmi szabályok és házirendek meghatározásához és azok érvényesítéséhez. Finoman hangolható szabályok mentén képes észlelni és figyelmeztetni a gyanús viselkedésekre, az anomális tevékenységekre és a meghatározott házirendek megsértésére. Valós idejű blokkolást, maszkolást és titkosítást tud biztosítani és ezekkel megakadályozni az adatszivárgásokat, adatlopást és adatvesztést. Az összes, a rendszerbe bekötött adatbázissal kapcsolatos adatbiztonsági eseményeket egy egységes felületen képes megjeleníteni, és hatékony segítséget nyújt azok elemzéséhez.

– Az Imperva Data Security Fabric az egyik első onprem, hibrid és multi-cloud környezetben is egyaránt használható, valóban egységes, átfogó adatvédelmi megoldás, amely megvédi az adatokat a jogosulatlan hozzáférésektől, lopásoktól és visszaélésektől. Segít megfelelni az adatvédelmi előírásoknak, megelőzni az adatbiztonság sérülését és csökkenteni az adatvesztés kockázatát. Az Imperva Data Security lehetővé teszi, hogy átláthatóságot és ellenőrzést szerezzen adatai felett, bárhol is legyenek azok. Így az Imperva Data Security Fabric lehetővé teszi a vállalatok számára, hogy biztonságosan használják ki az adataikban rejlő értéket, miközben megvédik őket a belső és külső fenyegetésektől. ■ imperva

Almási Zsolt
senior rendszermérnök

Sok feladat ismétlődik a biztonsági központokban is

Az elmúlt években egyre gyakrabban találkozunk a „digitalizáció” és „automatizáció” kifejezésekkel az üzleti életben. Az automatizáció területe nagyon hangsúlyossá vált az informatikában, és ez a különféle IT-biztonsági rendszerek esetében sincs másképp. Évről évre látjuk az újabb és újabb bejelentéseket, amelyek azt ígérik, hogy meg fogják váltani a világot, és használatukkal könnyebb lesz az incidensek kezelése és a rendszerek üzemeltetése. Ezek az ígéretek általában egy-egy körülhatárolható problémahalmazra fókuszálnak, nem az IT-biztonsági csapatok munkájának egészét szeretnék megreformálni.

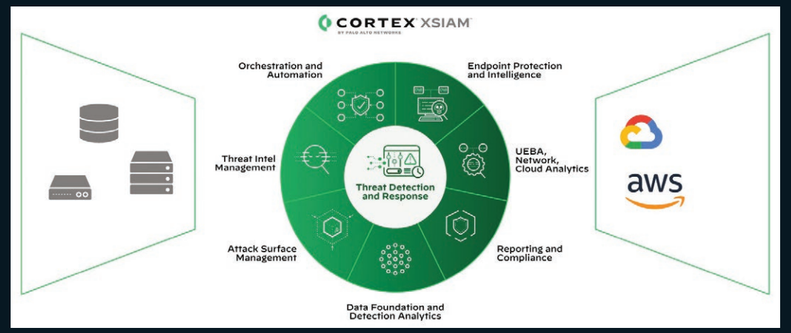
Az egyik ilyen aktuális megoldáshalmaz az XDR-ek családja, ahova kezdetben inkább végpontvédelmi problémák irányból közelítettek a gyártók, ám ma már egyre nehezebb meghatározni mi is egy XDR, illetve milyen feltételeknek kell megfelelnie egy ebbe a kategóriába tartozó megoldásnak. A legtöbb megoldás tartalmaz valamilyen végpontvédelmet, és hálózati, illetve egyéb kapcsolódó naplókat is képes a saját maga által generált bejegyzésekkel korrelálni, valamint segít megkeresni egy incidens kiindulópontját. Viszont ez nem mindig elég, és a reagálási képességek sem terjednek ki minden esetben a cégek által használt biztonsági termékek teljes arzenáljára.

Ha tovább haladunk az automatizáció irányába, akkor ígéretesebb megoldásnak tűnhet a SOAR-ok családja. Ezek már konkrét incidenseket kapnak a meglévő rendszerekből, és például a Palo Alto Networks XSOAR csomagja esetén közel 1000 különböző más megoldást integrálhatunk. Képesek a legkülönfélébb módokon beavatkozni, és sok helyről gyűjtött információkkal kibővíteni a kapott riasztásokat. Egy ilyen rendszer nagyobb mennyiségű riasztás esetén képes akár több kezdő analyst munkáját is kiváltani és nagyban megkönnyíti a SOC-csapat munkáját, akik így jobban fókuszálhatnak a bonyolultabb feladatokra. Sokszor ezekre a megoldásokra már úgy tekintünk, mint az automatizáció „csúcsára”, és azt gondolhatnánk innen már nincs tovább. Pedig van.

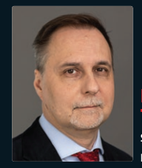
A **Palo Alto Networks** még egy lépéssel tovább ment: nemrég bejelentették az automatizált SOC víziójukat, amely a bejelentés óta már konkrét megoldásként, **XSIAM** néven érhető el a portfóliójukban. Ezt arra találták ki, hogy egy közös integrált platformként egyesítse az XDR és XSOAR, illetve a támadási felület figyelő – attack surface management, ASM – Xpanse nevű megoldását a gyártónak. Az XSIAM segítségével a SOC-csapatnak csak egy eszközön belül kell tevékenykednie, ahol az incidensek teljes életciklusát végig tudják követni. Nincs szükség a platformból „kinyúlni” egy külön ticketing rendszerbe vagy SIEM-be, és csak azok a riasztások kerülnek a szakemberek elé, amelyekkel mindenféleképpen foglalkozniuk kell.

Egy hagyományos SIEM-mel szemben (amely általában sok helyen jelenleg még a SOC központi eleme) az XSIAM az incidensek feldolgozását hatékonyan segíti azzal, hogy automatikusan a kezünk alá dolgozik, és már előre minden releváns információt korrelál és kibővít. Az XSIAM segít a SOC csapatoknak, hogy nagy mennyiségű riasztással is gyorsan tudjanak foglalkozni, illetve magába foglalja az adatok automatizált feldolgozását is. Az XSIAM további előnye, hogy a felhős felépítésének köszönhetően jóval egyszerűbb skálázni, mint egy saját SIEM-et, SOAR-t, illetve a hozzájuk kapcsolódó rendszereket.

Ezeket a képességeket és előnyöket átgondolva egyértelmű, hogy az XSIAM által beteljesített vízió jelentősen megkönnyíti a nagy



szervezetek számára a biztonsági incidensek kezelését. Ezen felül minden automatizáció, amely segít csökkenteni a céges rendszerek üzemeltetéséhez szükséges alkalmazottak számát, nagyban hozzájárul az általános IT-biztonsági szakemberhiány kezeléséhez. ■ paloalto NETWORKS



Foki Tamás
senior rendszer-mérnök

FIDO / passwordless technológiák

Korunk digitalizációs folyamatai miatt már senki sem kerülheti meg, hogy a legkülönbözőbb informatikai rendszerekhez legyen hozzáférése. A munkahelyen kívül a hivatalos ügyintézés, a vásárlás, és a szórakozás is egyre inkább digitális platformokon, nagyrészt felhős alkalmazásokon keresztül történik. Bár életünk elválaszthatatlan részei lettek ezek a hozzáférések, ennek ellenére a felhasználók még mindig nem kezelik kellő óvatossággal a jelszavaikat. Erre kínál egy egyszerű megoldást a FIDO.

A felhasználók gyakran könnyen kitalálható jelszavakat alkalmaznak, nagyon sok esetben pedig ugyanazt a jelszót használják több szolgáltatáshoz is, ami nagyon kiszolgáltatottá teszi őket. Egy phishing támadás vagy egy alkalmazás hibáját kihasználó jelszólopás esetén nemcsak az adott szolgáltatáshoz tartozó fiók válik elérhetővé, hanem más rendszerek is védtelenné válhatnak.

A jelszóhelyettesítő megoldások

Szerencsére ma már a technológia segít abban, hogy ne csak bonyolult, gyakran változtatott, megjegyezhetetlen jelszavakkal lehessen védekezni, hanem a multifaktoros azonosítás (MFA) révén felhasználóbarát módon adjunk lehetőséget a szolgáltatások biztonságos elérésére. A multifaktoros azonosítás során a felhasználónéven és jelszón kívül további fizikai faktorokat is bevonhatunk az azonosítási folyamatba, amelyek lehetnek biometrikus adatok *(ujjlenyomat, íriszmintázat – ilyen készülék látható a képen)*, fizikai eszközök (smartcardok, USB-tokenek) vagy email-címre, SMS-ben, esetleg mobileszközön futó dedikált alkalmazásba kiküldött egyszer használatos kódok.

Ezen technológiák elterjedését lassította, hogy minden gyártó egyedi megoldásokat használt, egy-egy alkalmazás alkalmassá tétele egy adott módszerrel való kompatibilitásra jelentős változtatásokat igényelhet. Erre a problémára reagálva jött létre a FIDO (Fast Identity Online), amely egységes, gyártófüggetlen, nyílt szabvány, és lehetővé teszi az online azonosítást és hitelesítést. A FIDO szabvány célja, hogy az egyszerű jelszavakat leváltsa a lehető legnagyobb biztonságot nyújtó és könnyű integrálhatóságú megoldásokkal, ugyanakkor szem előtt tartja az egyszerű használhatóságot is.

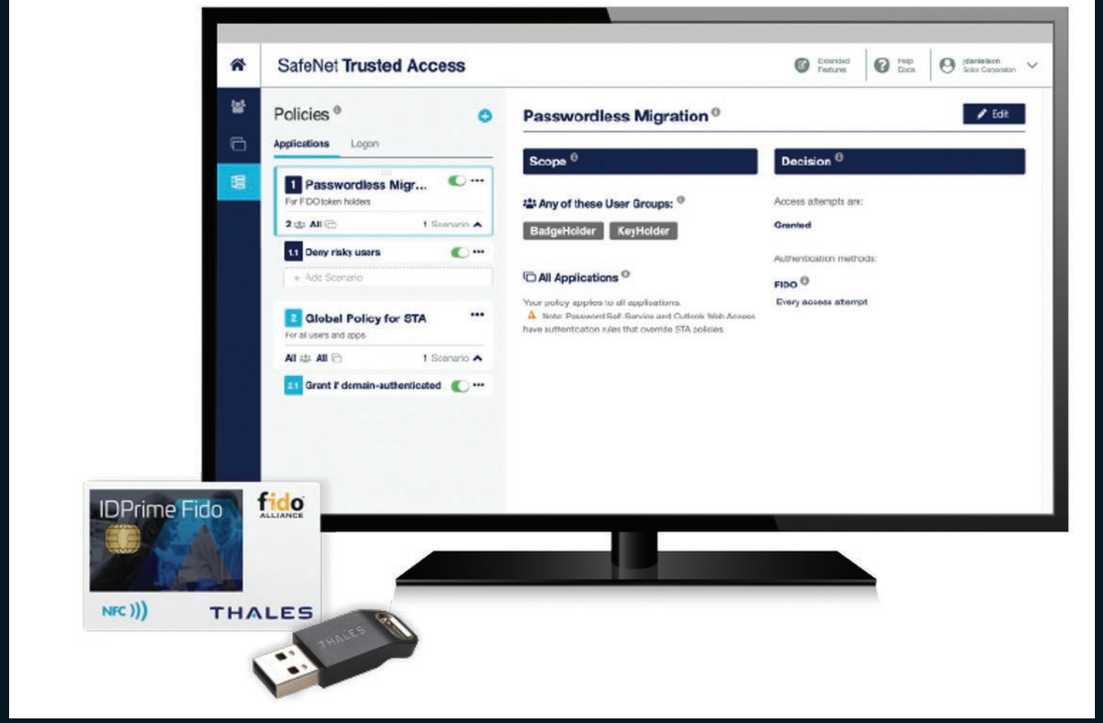
Mivel a FIDO Alliance-ban több mint 250 vállalkozás vesz részt, és már 600 feletti a „FIDO certified" megoldások száma, ezért elmondhatjuk, hogy az FIDO-protokollok és eszközök széles körben használhatók. Lehetővé teszik, hogy több megoldáshoz is párhuzamosan használjuk őket, ezért költségmegtakarítást jelentenek az ügyfelek részére más, gyártófüggő megoldásokhoz képest. A fejlesztőknek is előnyös a FIDO szabvány, mert csak egyfajta hitelesítési módra kell az alkalmazásukat felkészíteni, de az mégis számos gyártó széles termékválasztékával képes együttműködni.

Platformok, amelyen a FIDO-t lehet használni

- Microsoft Azure AD
- M365 access
- Asztali Windows login
- Privileged access management termékek,
- Remote access hozzáférések,
- Számos webes alkalmazás (belső vagy interneten elérhető publikus alkalmazások, beleértve a banki rendszereket is),
- Mobil operációs rendszerek, Android és IOS.

A Thales is FIDO-kompatibilis

A FIDO Alliance-nek fontos tagja a francia székhelyű nemzetközi nagyvállalat, a **Thales** is, amely a védelmi, légi és űripari, közlekedési és biztonsági piacokon tevékenykedik. HSM-jei, PKI-technológiái piacvezetőnek számítanak, de az azonosítás és hitelesítés terén is a legnagyobbak közé tartoznak, amit számos felvásárlással is erősítettek, ilyen a Safenet vagy Gemalto akvizíciója, és széles, FIDO-kompatibilis termékportfólióval rendelkezik: OTP-generáló fizikai tokenek, smartcardok, USB-s eToken-ek (USB-C és USB-A csatlakozóval is), contactless megoldások (NFC), de van SMS alapú szolgáltatás is FIDO-kompatibilis változatban, valamint egy egyedi, ún. gridToken megoldás, amelyben például egy weboldal betűkből álló négyzetet jelenít meg, ahonnan választva a felhasználó egy egyedi minta alapján írja be megfelelő sorrendben a karaktereket, mint második faktort.



Fontos, hogy a Thales FIDO-kompatibilis tokenjei opcionálisan kompatibilisek a gyartó PKI-megoldásaival is, valamint a legkülönbözőbb szabványú fizikai beléptető rendszerekkel is kombinálhatóak, és van még biometrikus, ujjlenyomat alapú tokenjük is.

A FIDO-szabvány miatt természetesen a gyártó FIDO-tokenjei más third-party IDP és CMS rendszerekhez is használhatók, például ilyen a Versasec, az AWS és a Microsoft, valamint ezek rendelhetők co-branded változatban is, illetve FIPS és Common Criteria tanúsítvánnyal rendelkező változatok is léteznek.

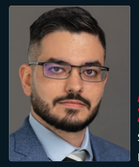
Hozzáférés-hitelesítő megoldás FIDO-val

A Thales továbbá rendelkezik egy – természetesen a FIDO szabvánnyal is kompatibilis – hozzáférés-kezelő és -hitelesítő szolgáltatási megoldással, az STA-val (SafeNet Trusted Access-el), amely lehetővé teszi a felhasználók számára, hogy biztonságosan és egyszerűen hozzáférjenek az alkalmazásokhoz és az adatokhoz bármilyen eszközről és helyről. A SafeNet Trusted Access biztonságos hozzáférést tesz lehetővé a felhőalapú alkalmazásokhoz, beleértve a SaaS és az egyéb webes alkalmazásokat, valamint a helyi erőforrásokhoz is.

A STA biztosítja a tokenek kiosztását és nyilvántartását a felhasználók számára, a felhasználók kezelését, ugyanakkor integrálható külső IdP szolgáltatóval, de az STA is képes idP szolgáltatást nyújtani, valamint ügyfél portált tesz elérhetővé az általa biztosított erőforrások közvetlen elérésére érdekében, és SAML alapokon böngésző alapú SSO szolgáltatást is biztosít webalkalmazások számára. Ezért rugalmasan illeszthető bármelyik szervezet informatikai rendszereihez.

Röviden összefoglalva: már nem csak a minden alkalmazáshoz egyedi, bonyolult és állandóan változó jelszavak használatának mindenáron kikényszerítése az út, amelyek ráadásul önmagukban még nem is jelentenek tökéletes védelmet, cserébe viszont biztosan tönkreteszik a felhasználói élményt, és szinte teljesíthetetlen követelményeket támasztanak.

Ezzel szemben egy FIDO alapú MFA-megoldással, amelyre tökéletes példa a Thales STA csomagja, az elérhető legnagyobb biztonságot garantálhatjuk az azonosítási és hitelesítési folyamatainknak, miközben felhasználóbarát szolgáltatást nyújtunk. ■ THALES



Almási Zsolt
senior rendszer-mérnök

Biztonsági mentés a 21. századi, felhős környezetekre: Rubrik

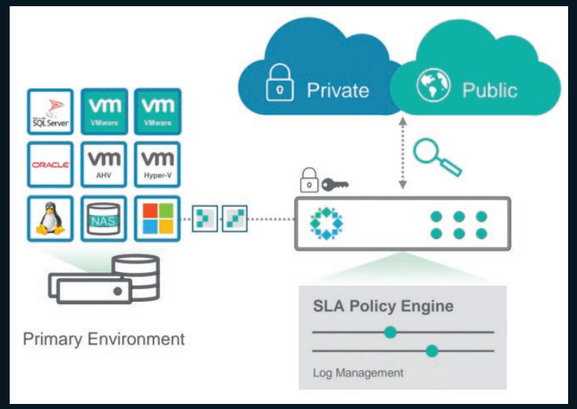
Egyre kevésbé ideális állapot, hogy egy hosszú évek óta üzemelő, hagyományos backup-megoldást használjunk csak azért, mert „nekünk évek óta ez van, és bevált”. Sokszor nem gondolják végig az IT-vezetők, hogy az elmúlt időszakban a védendő eszközök és rendszerek is teljesen megváltoztak. Sok új lehetőség feature jelent meg bennük, amelyeket a hagyományos backup-megoldások nem, vagy csak „toldozva-foltozva” támogatnak. Ami korábban elég volt, hogy egy virtuális infrastruktúrát tudtunk menteni, esetleg utána ezt még szalagos tároló használatával archiválni, ma már nagyon kevés.

A hagyományos backup-megoldások esetén sokszor nem lehet felhős szolgáltatásokat, megoldásokat kezelni, ami azt jelenti, ha a cég bizonyos infrastruktúraelemeket a felhőben szeretne futtatni, vagy felhős megoldást használna, ha nincs szerencséjük, akkor ezek az elemek egyáltalán nem lesznek menthetők a korábbi megoldásunkkal. Kicsit jobb a helyzet akkor, ha egy külön felületen, más mentési rendszerrel, más szabályokkal talán meg tudjuk oldani. Viszont mennyivel jobb lenne, ha ezeket egy egyszerűen használható, halandó emberek számára is érthető módon működő rendszerrel tudnánk megvédeni!

Ilyen megoldást kínál például a **Rubrik.** Az vállalat backup-eszköze egy jól használható GUI segítségével, SLA-k definiálásával, könnyen kezelhető módon képes megvédeni adatainkat, legyenek akár on-prem virtualizációs környezetben, akár felhős infrastruktúrában.

A Rubrik ezek mellett leveszi annak a terhét az infrastruktúra csapat válláról, hogy folyamatosan számolni kelljen a backuphoz használt szerver terhelésével, illetve az alatta lévő tároló teljesítményével. A rendszer hiperkonvergens mivolta miatt a Rubrik esetében egy újabb doboz („brick”, azaz tégla) megvásárlásával megkapjuk a szükséges tárterületet és az ehhez kellő számítási kapacitást, illetve a gyors működéshez elengedhetetlen beépített SSD-ket is.

A Rubrik megoldásától az egyszerűségen felül kiemelkedő képességeket is kapunk a jól átgondolt felépítésnek köszönhetően.

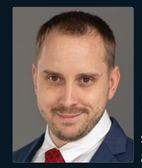


Ilyen például, hogy bármikor elindíthatunk egy sérült VM-et vagy visszaállíthatunk egy fájlt anélkül, hogy meg kéne várnunk amíg az adat visszajut a megfelelő tárhelyre. Ilyenkor a beépített diskek és SSD-k használatával ki tudjuk ajánlani az infrastruktúra felé a szükséges adatokat, és kiesés nélkül tudunk tovább dolgozni, amíg visszaállítjuk a szükséges állapotot.

A „hagyományos” infrastruktúrafeladatokon felül érdemes megemlíteni, hogy a rendszerhez elérhető egy felhős, központi menedzsmentkonzol, amelyet – többek között – a biztonsági funkciókra optimalizáltak. Elsőre ez ugyan idegen funkciónak tűnhet, de gondoljunk csak bele mennyire hasznos, ha a mentett fájlok esetén már a változás bekövetkezésekor tud jelezni a rendszer, hogy bizonyos adatok titkosítottá váltak (például ransomware-támadás miatt) vagy megsérültek. Illetve használatával jelentősen egyszerűbb lesz az üzemeltetők élete, mivel a támadás bekövetkezésekor a rendszer segít megtalálni a még sértetlen állapotot a hatékony visszaállítás érdekében. A megoldás már az alapjaitól kezdve a biztonságra törekszik, például a kívülről sérthetetlen tárhelyel, illetve MFA alkalmazásával a belépéskor, így ideális választás lehet minden olyan cég számára, ahol az IT-biztonságot nem veszik félvállról. ■

A Rubrik eredete

A Rubrik alapítói és technológiai vezetői korábban több nagy backup-megoldással, illetve adatokkal foglakozó cégtől érkeztek. Mivel szakmai előéletük során sok hasonló megoldást láttak/fejlesztettek, ezért megpróbáltak minden olyan hiányosságot kijavítani, amelyet máshol tapasztaltak. Jó példa erre a Google-hez hasonló indexelő és kereső motor is, amellyel nagyon egyszerűen, akár fájlra keresve tudunk visszaállítani adatokat a biztosított környezetek esetén.



Kamarás Bálint
security architect

Nyakunkon az új irányelvek

A Network and Information Security (NIS) Directive 2, a hálózati és információs rendszerek biztonságáról szóló irányelv az egyik legújabb európai szintű jogszabály-frissítés. Az irányelv az EU kiberbiztonsági stratégiájának része, és számos jelentéstételi és kockázatkezelési intézkedést vezet be a kiberbiztonsággal kapcsolatban.

A NISD 2016-os első verziója már 2016 óta minden az Európai Unióban, hálózat- és információbiztonsági munkakörhöz köthető szakmabeli életének részét képezi, a tagállamoknak pedig 2024. október 17-ig kell elfogadniuk és kihirdetniük azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy az új NIS2 irányelvnek megfeleljenek.

Rengeteg témát érint a NIS2: az érintettek körének bővülésén túl sokkal részletesebb lett az előző verzióhoz képest. Fontos kiemelni, hogy azon szervezetek számára is komoly feladatokat jelenthet, akik úgy gondolják, nem lehet problémájuk a minősítéssel, hiszen élenjárók az említett témákban. A CSIRT, azaz a Computer Security Incident Response Team (számítógép-biztonsági incidenskezelő csoport) működésének taglalása mellett például az üzletmenet-folytonossági kérdésekben és a katasztrófa-helyreállítás tervezésében is szintet lép. Kézzel fogható konkrétumok terén kiemelendő a tartalékrendszerek menedzselésének területe, a kiberbiztonsági gyakorlatok és a több faktoros hitelesítés témaköre is. Fontos célkitűzés a kkv-k felkészültségi szintjének növelése is.

A jogalkotó fő célja mind a köz-, mind a magánszektorban az incidensekre való reagálási képesség javítása. Az érintett területek a fontos és alapvető ágazatokban: postai és futárszolgálatok, elektronikai-, és járműgyártás, kutatóhelyek, hulladékgazdálkodás, élelmiszer előállítás és forgalmazás, digitális szolgáltatások (online piacterek, keresőmotorok, közösségimédia-szolgáltatási platformok), vegyipari gyártás és forgalmazás, a komplett energiaszektor (villamos, távfűtés és -hűtés, olaj, gáz, hidrogén), természetesen a banki és pénzügyi szolgáltatások, vízellátás, digitális infrastruktúrák (hírközlés, internet kicserélő pontok, bizalmi szolgáltatók, domainnyilvántartók, publikus DNS-szolgáltatások), űripar, szállítási szolgáltatások, egészségügy, közigazgatás, gyógyszeripar, valamint a menedzselt biztonsági szolgáltatások. Végül de nem utolsósorban, ami talán kiemelt figyelmet igényel: a felhő és adatközpont szolgáltatók.

Előírás, hogy a védekezés folyamatos legyen, amelyet monitorozással, értékeléssel és frissítéssel kell fenntartani. Ennek érdekében a vállalatoknak kockázatbecsléseket kell végezniük, védekezési terveket kell készíteniük, és olyan üzemeltetési folyamatokat kell kialakítaniuk, amelyek segítenek megfelelni a biztonsági követelményeknek.

Az érintettek köre igencsak széles, az előzetes felmérések kissé ellentmondásosak, de több ezer olyan vállalatra vonatkozik majd a rendelet, akiknek még komoly lépéseket kell tenni a sikeres megfelelésig: alap- vagy magas szintű kiberbiztonsági tanúsításon kell megfelelniük önértékeléses, vagy akkreditált auditor által végzett tanúsítás során. Bár a NIS2, gyakorlati tapasztalatok híján, még a „szürke zónában” van, mégis „jobb félni, mint megijedni.”

Végül, de nem utolsósorban: a bírság. Alapvető szervezetek esetében legalább 10 000, fontos szervezetek esetében pedig legalább 70 000 EUR lehet a bírság maximálisan pedig a vállalkozás előző pénzügyi évi globális éves forgalma 2, illetve 1,4 százaléka (alapvető, illetve fontos szervezetek), ha megsértik a kiberbiztonsági kockázatkezelési intézkedéseket vagy a jelentésbeli kötelezettségeiket. De ha ugyanazért GDPR alapján közigazgatási bírságot is kiszabnak egy vállalatra, az illetékes hatóságok nem szabhatnak ki a NIS2 irányelv szerinti bírságot. ■

A Digital Operational Resilience Act (DORA)

Az EB előkészítés alatt lévő, a kibertámadások elleni védekezés összehangolására definiált, 2025 januárjától érvényes törvényi szabályozás a pénzügyi kibertérben hivatott rendet tenni. Főbb feladatai a digitális reziliencára vonatkozó stratégia megalkotása, valamint annak tesztelésére szolgáló program kialakítása. Szintén feladat a rendszeres (havi) vezetői jelentés a harmadik félnek minősülő információs, kommunikációs technológiai szolgáltatók kapcsán, valamint a harmadik félnek minősülő szolgáltatókkal kötött megállapodások kulcsfontosságú vagy lényeges funkcióira vonatkozó tervek elkészítése, a pontos és széles körű, nem csak a kiszervezések és a felhőszolgáltatások értelmében vett nyilvántartások és kockázatok elemzése, átfogó kommunikációs eljárásrend kialakítása. Gyakorlatban ültetve mindez a már jól ismert hatóságok ajánlásain túl elvégzett elemzések során feltárt eltérések megszüntetésére, precíz, roadmapbe ültetett részletes tervek készítését és végrehajtását foglalja magába.

CLICO

MAGYARORSZÁGI PORTFÓLIÓ:

ARISTA | ARMIS | COMMSCOPE® RUCKUS®

cryptme | Cryptshare® | CYBERARK®

DIGI | Fidelis Cybersecurity | Forcepoint

FORESCOUT | GREYCORTEX Security for Professionals | imperva

Infinera | IronNet | ivanti

JUNIPER driven by Mist AI | MICROSENS euromicron group | CIPHER AN ENTRUST DATACARD COMPANY

opengear A DIGI COMPANY | paloalto® NETWORKS | radware

RAPID7 | Recorded Future® | rubrik

SailPoint | SCIRGE | SentinelOne™

THALES | tufin | VECTRA®

CLICO HUNGARY KFT. • 1134 BUDAPEST, DÉVAI UTCA 26-28. • EMAIL: INFO@CLICO.HU • WEB: WWW.CLICO.HU