Kristálygömb: digitális transzformáció-digitális kockázatkezelés

CSINOS TAMÁS

FORRÁS: CLICO

Idén 5 éves a Clico magyarországi leányvállalata, és idén harmadszor rendezzük meg a PROtACTION biztonsággal foglalkozó konferenciánkat. Ahogy az eddigi alkalmakkor, most is az a célunk, hogy trendeket, új ötleteket, előremutató technológiákat mutassunk be, megpróbáljunk olyan problémahalmazokra reagálni, amelyek esetleg még a biztonsági szakemberek látókörébe nem kerültek, de a szervezeteknél már biztos van olyan műhely, akár csak egy-két kolléga, aki az üzleti oldalról érkezve kevésbé biztonságtudatosan hozna friss megoldásokat a vállalati IT-környezetbe.

A mi feladatunk művészi-professzionális szintre emelni ezt az egyensúlyozást: a lehető legkevésbé lenni kerékkötője a digitális átalakulás ezernyi fejlesztési irányának, de közben szilárd hátteret, sérülésmentes bizalmasságot, integritást és üzembiztonságot kínálni a szervezeteknek.

Mellékletünkben próbáltuk a legforróbb trendekre szánt megoldásokat, a legnagyobb kihívással járó biztonsági-folyamatszervezési kérdéseket körbejárni a magunk módján: értéknövelt disztribútor mivoltunkból fakadóan gyártó és technológiai fókusszal. A cikkek között van infrastruktúraközeli téma csakúgy, mint inkább biztonságirányítással kapcsolatos szöveg.

Jó tanulást, jó szórakozást!

Csinos Tamás

Forcepoint

Adat? Szivárgás!

Bár az adatszivárgást megakadályozó megoldások a más területeken megjelenő új technológiák miatt mostanában kicsit háttérbe szorultak, de a DLP nem halott, sőt, aktuálisabb, mint valaha! Ezt jelzik a rendszeresen feltűnő adatszivárgásokról szóló hírek, és az ilyen eseményekkel kapcsolatos hatósági eljárások is. Úgyhogy a DLP köszöni szépen, jól van, folyamatosan fejlődik az aktuális IT-trendeknek és változó környezeteknek megfelelően, és egyre több szervezet dönt úgy, hogy aktív védelmi megoldással próbálja a kockázatait csökkenteni ezen a területen.

FOKI TAMÁS SZENIOR RENDSZERMÉRNÖK

FORRÁS: CLICO

A Forcepoint DLP-csomagja eddig is az iparág egyik legfejlettebb megoldása volt, amely az utóbbi időben egyre több új funkcióval és integrációs lehetőségekkel bővült, ezekből mutatjuk be a legfontosabbakat.

Forcepoint DLP Cloud Application

Az adatok már nemcsak a szervezetek belső szerverein találhatók meg, hanem a felhős alkalmazásokban is – úgymint M/O365, Salesforce, G Suite, Onedrive, Dropbox és társaik –, ahonnan kellő védelem nélkül bárhonnan elérhetőek a vállalati perimeter-védelmi szolgáltatásokat megkerülve. A DLP-szabályok immár kiterjeszthetők a felhős szolgáltatásokra is, API integráció révén ugyanazok a DLP-szabályok érvényesíthetők a felhős szolgáltatásokban, mint on-prem, illetve az endpointokon, így ezen szolgáltatásokból is megakadályozhatók a nem kívánt adatszivárgások.

Címkéző rendszerek integrációja

A DLP-installációk másik jelentős problémája, hogy az érzékeny tartalmakat nehéz jól meghatározható szabályokkal védeni, és magas a téves riasztások száma. A DLP működését címkéző (tagging) rendszerek integrálásával lehet hatékonyabbá tenni. Egy címkéző megoldással nagyságrendekkel pontosabb lehet az érintett dokumentumok kezelése. A Forcepoint DLP nemcsak felhasználni tudja a dokumentumok tagging információt, de a discovery funkcióval és szabályok alapján történő automatikus tageléssel meggyorsíthatja és egyszerűsítheti a bevezetést is, mert így a már meglévő dokumentumokat automatikusan képes a megfelelő tagekkel ellátni.

Dynamic User Protection (DUP)

A riasztásoknál fontos lenne tudniuk az üzemeltetőknek, hogy mely felhasználók tevékenysége különösen gyanús, mert a hagyományos DLP-rendszerek nem tudnak két felhasználó által generált riasztás között különbséget tenni. Ennek kezelésére jelent meg az úgynevezett „Risk Adaptive Protection”.

A végpontokon a felhasználók tevékenységét automatikusan (User Activity Monitoring) elemzi egy felhő központú viselkedésanalitika-motor, amely nem igényel on-prem infrastruktúrát, bonyolult korrelációs szabályok beállítását, így gyorsan bevezethető és használatba vehető. Ez egy DUP agent révén a felhasználó összes tevékenységét követi, és egy analitikai motor segítségével előre definiált, a gyártó által karbantartott szabályok alapján keres gyanús viselkedésre utaló jeleket, majd ezeket az IoB-kat (Indicator of Behavior) felhasználva képes kiszámítani egy adott felhasználó kockázati szintjét.

Az így szerzett információkkal lehet súlyozni/finomítani a DLP-szabályokat, amelyek így sokkal pontosabbak lesznek, csökken egyrészt a riasztások száma (ezen belül is főleg a téves riasztásoké), másrészt az alkalmazás UAM- (User Activity Monitoring) megoldásként is megállja a helyét és a DLP-től függetlenül is segíti a rendszerfelügyeletet ellátó szakemberek munkáját.

Ezekkel a fejlesztésekkel a Forcepoint DLP lépést tart napjaink informatikai változásaival, és további funkciókkal pontosítja, illetve egyszerűsíti a biztonsági csapatok munkáját. ■

Amikor a cég biztonságát otthoni környezetben kell garantálni

Forcepoint

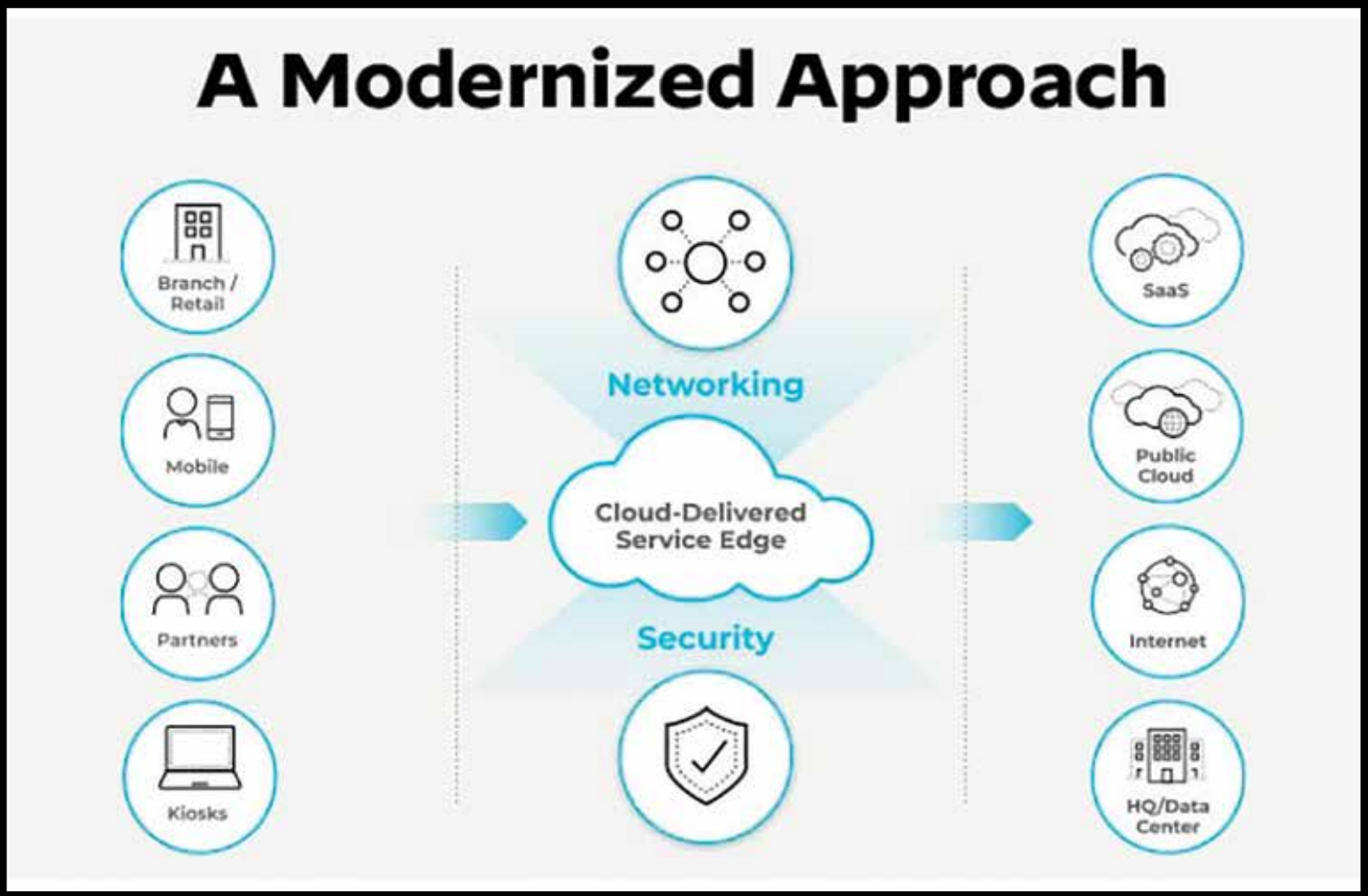
Az elmúlt évek egyik nagy dilemmája volt a vállalatok számára, hogy engedjék-e a távoli munkát vagy sem. Az elmúlt hónapok eseményei átléptek ezen a kérdésen, és már csak az a kérdés, milyen eszközökkel és hogyan valósítható meg az otthoni munkavégzés biztonsága, ezen kapcsolatok felügyelete és a szükséges erőforrások megléte.

Ezzel a biztonsági csapatok feladata ugrásszerűen megnőtt, hiszen jóval nehezebb a szervezetek biztonságát az otthoni környezetekből származó kihívásokkal szemben is garantálni. Ilyen kihívás például az otthoni, alacsony szintű biztonságot nyújtó, olcsó wifi-routerek és saját eszközök használata, de az otthon lévő céges eszközök más családtag általi használata is. A tömeges home office-ra való áttérést kiváltó vírushelyzet miatt az évek során gondosan felépített céges biztonsági infrastruktúrák meghaladottá váltak. Ezért is lett napjaink mondása, hogy „A végpont az új periméter".
Másik probléma, hogy az eddig használt VPN-rendszerek kapacitása sok esetben szűkösnek bizonyult, mert hirtelen sokszorosára nőtt a távoli munkavégzés aránya. Természetesen ki lehet kényszeríteni, hogy az otthonról dolgozók teljes hálózati forgalma VPN-en keresztül menjen a központba, majd az ottani tűzfalakon, proxy-kon keresztül szűrve érje el a kívánt tartalmakat, de ez megnövekedett sávszélesség igényeket és nagyobb tűzfal-proxy-vpn teljesítményt igényel. Arról nem is beszélve, hogy egyre több szolgáltatás költözik publikus vagy privát felhőkbe, és így a forgalom egy része többször is megjárja a központi infrastruktúrát.

Ezekre az igényekre reagálnak a SASE (Secure Access Service Edge) és ZTNA (Zero Trust Network Access) megoldások. A SASE gyakorlatilag a felhőbe költözteti a hálózati és biztonsági infrastruktúra egy részét. A kliensforgalom közvetlenül a felhőszolgáltatásba érkezik. Ott történik a forgalom szűrése, a szabályok kikényszerítése, a rosszindulatú tevékenységek detektálása. Gyakorlatilag csak a megvásárolt licencektől függ, hogy milyen funkciót adunk hozzá a szabályainkhoz, illetve aktuálisan hány felhasználónk lehet az adott rendszerbe vonva. Ez kiegészíthető SD-WAN (software-defined WAN) funkcionalitással is, ahol a telephelyek forgalma is a SASE szolgáltatásba csatlakozik be, a végponti eszközök pedig gyakorlatilag csak a felhős kapcsolatot és a forgalom titkosítását és priorizálását végzik, minden más biztonsági szűrést, útválasztást a felhős erőforrások végeznek. A másik, szintén paradigmaváltó újdonság a VPN-megoldások evolúciója a ZTNA irányába.

Zero Trust Network Access

A ZTNA célja a hagyományos kliens VPN-kapcsolatok hiányosságainak kiküszöbölése és menedzsmentjük egyszerűsítése. Az alapszabály az, hogy a felhasználónak csak ahhoz az alkalmazáshoz legyen hozzáférése, amelyre ténylegesen szüksége van. A rendszer hozzáféréskéréskor ellenőrzi a felhasználó azonosságát és hozzájuk rendeli a szerepkör alapon definiált jogosultságokat, és a feltétlenül szükségesen kívül semmivel sem ad több hozzáférést, így valósítja meg a Zero Trust biztonsági modellt.



A ZTNA a VPN-ektől eltérően nem hálózati alapon ad hozzáférést, hanem előre definiált szerepköröket rendel az egyes felhasználókhoz, így csak a legszükségesebb erőforrásokhoz nyújt elérést. Amíg egy VPN kompromittálódása esetén akár egy teljes hálózati szegmens válik kiszolgáltatottá, addig a ZTNA esetén sokkal kisebb az elérhető komponens, és oda sem adunk teljes hálózati hozzáférést, csak bizonyos szolgáltatásokat teszünk elérhetővé. A tipikus ZTNA-megoldások felhőalapúak, nem kötik a VPN-ek korlátai, és sokkal rugalmasabban skálázhatóak. Ennek köszönhetően több beépített biztonsági szolgáltatatást nyújthatnak, például központi helyről folyamatos monitorozási lehetőséget, kockázat kiértékelési lehetőségeket, egy helyről konfigurálható és egyszerűen bővíthető további szolgáltatásokkal. A ZTNA tipikusan része a SD-WAN- és/vagy SASE-megoldásoknak.

SASE és ZTNA rendszerekre különböző gyártóinknak is van javaslata, például a Palo Alto Networks portfóliójában a Prisma Access megoldása ilyen. Használatával élvezhetjük a SASE és ZTNA előnyeit. A rendszer használatával megkapjuk a Palo Alto Networks tűzfalak képességeit, mint például L7 vizibilitást a forgalmakra, kifinomult policy lehetőségeket vagy az iparág vezető sandbox-megoldásához – a Wildfire-hez – való hozzáférést. A felhasználóink és a telephelyeken található eszközeink egyszerűen a legközelebbi adatközponthoz csatlakozhatnak és az elérhető sávszélesség gyakorlatilag csak az előfizetésünktől függ. A tűzfalakról ismert funkciókon kívül például DLP és Secure Web Gateway funkciók is elérhetőek, vagy akár vizsgálhatjuk adott alkalmazások elérésének a használati élményét is.

Forcepoint Dynamic Edge Protection

A Forcepoint Dynamic Edge Protection szolgáltatáscsomagja a gyártó SASE és ZTNA szolgáltatásait foglalja össze.

Van egy Cloud Security Gateway-nek (CSG) nevezett rész, amely a kliensek publikus internet irányba történő forgalmát és a publikus SaaS-szolgáltatásokat kezeli. Valamint egy Private Access (PA) csomag, amely a privát hálózatokba irányuló forgalmakat és a szervezetek saját alkalmazásainak elérését biztosítja.

A felhasználó szempontjából teljesen transzparens, a megszokott böngésző linkjeit használja otthon és az irodában, a Private Access elrejti előle a hálózati réteget, számára az egész olyan, mintha közvetlenül az alkalmazást érné el. Mindkettő tartalmaz különböző threat protection szolgáltatásokat és rugalmasan bővíthető további funkciókkal, mint például felhős DLP, CASB stb.

Talán ennyiből is kiderült, hogy ezekkel az új technológiákkal úgy tudunk reagálni a most zajló munkavégzési szokások változásaira, hogy egyrészt a „pay as you grow” elven rugalmasan megfelelhetünk a változó forgalmi igényeknek, másrészt a biztonsági szintet annak ellenére növelhetjük, hogy a felhasználók fizikailag kikerültek az eddig egyedül biztonságosnak gondolt belső hálózatokból. ■

A home office érájában a végpontvédelem az IT-biztonság új szuperhőse

paloalto NETWORKS

Egyre többször merül fel az a probléma, hogy a hagyományos desktop antivírus és cégen belüli egyéb IT-biztonsági védelmi vonalak már kevesek. Az elmúlt évben a járványhelyzet alatt ez hatványozottan beigazolódni látszik. A dolgozók legtöbbször az irodán kívülről végzik a munkájukat – a felépített céges biztonsági rendszerek védelme nélkül.

ALMÁSI ZSOLT RENDSZERMÉRNÖK, TANÚSÍTOTT PALO ALTO NETWORKS OKTATÓ

FORRÁS: CLICO

Ez új lehetőséget ad a támadóknak, akik egyre több és egyre fejlettebb módszerekkel célozzák meg a cégeket, illetve közvetlenül a dolgozókat. Sok esetben ezeket a támadásokat a korábbiakhoz képest jóval nehezebb kivédeni, és még nehezebb visszakövetni. Érdekes információ, hogy például a ransomware- („zsarolóvírus”) támadások számának folyamatos felfelé ívelése mellett megjelent ezeknek egy új generációja, amely ellen már nem elég egy sima mentés, amelyből egyszerűen vissza lehetett állni. Ezek a támadások az adatok erőszakos betitkosítása mellett egy plusz lépésben ki is viszik a támadóknak az érzékeny adatokat, majd ezek közzétételével (is) zsarolják a cégeket.

A home office és a mobil eszközök használata miatt egyre többször halljuk, hogy a végpont az új periméter (határ). Ahol megoldható, a járványügyi javaslatok miatt a kollégák egyre több időt töltenek a cégen (és a felépített biztonsági vonalakon) kívül. Különböző felmérések szerint a dolgozók a világjárvány után se szeretnék újra minden idejüket az irodában tölteni, ezért a helyzet valószínűleg nem fog teljesen visszarendeződni a korábban megszokott munkavégzésre a jövőben sem.

Kiterjesztett észlelés és válasz

Ezek a változások egyre inkább abba az irányba mutatnak, hogy az eddig használt központi védelmi rendszerek mellett szükség van egy, a sima antivírusnál nagyobb hatékonysággal rendelkező végpontvédelmi megoldásra is. Ezeknek az újgenerációs végpontvédelmi megoldásoknak a neve XDR lett (azaz „extended detection and response” a sima „endpoint detection and response”, EDR helyett), utalva arra, hogy már nemcsak a végponti, hanem más forrásokból jövő információkkal is képesek dolgozni.

Felmerülhet a kérdés, hogy mire képes egy XDR-megoldás, amire egy antivírus vagy más hasonló hagyományos végpontvédelmi eszköz nem. Az XDR-rendszerek különböző forrásokból képesek begyűjteni a megfelelő információkat, illetve megtalálni a köztük lévő összefüggéseket. Ilyen források lehetnek például a tűzfal és a hálózati logok vagy hálózati forgalomelemző rendszerek (NDR) által gyűjtött metaadatok. Az automatikus korreláció mellett fontos szerepük van abban, hogy a támadások kiindulópontját is felismerjék, és kiderüljön, hogyan jutott be a támadó a környezetbe, hogyan fertőzte meg az otthon lévő gépet, majd utána merre ment tovább. Ha valaki már próbált kézzel felderíteni ilyen támadást, és begyűjteni minden információt, ami ehhez szükséges, az

FORRÁS: BITDEFENDER.COM

gyorsan belátja, hogy egy ilyen megoldás óriási időmegtakarítást jelent, és nagyban megkönnyíti az IT-csapat életét.
Az ilyen megoldások most már egyre több vezető IT-biztonsági cég portfóliójában megtalálhatóak – mint például a Palo Alto Networks-nél is. Az ő megoldásuk a Cortex XDR, amely megfelelő licencek megléte esetén képes különböző, nemcsak Palo Alto Networks-tűzfal naplóbejegyzések, illetve például AD-logok elemzésére és a végpontokról gyűjtött infomációk korrelálására. A rendszer a hagyományos szignatúrák helyett a támadók által használt exploit technikák kivédésére fókuszál, ami jóval hatékonyabb és kevesebb frissítéssel jár. A Cortex XDR használatával pár kattintással kideríthetjük, honnan indult a támadás és megkezdhetjük a veszély elhárítását. Fontos, hogy a megoldás nagyon hatékonyan képes együttműködni a többi Palo Alto Networks platformelemmel.

Portfóliónk további elemei

A portfóliónkban található másik gyártó, a SentinelOne, amely Singularity néven fejleszti a platformját. Ez a megoldás ötvözi a hagyományosan EDR-rendszerek esetén megismert mély eszközkontrollt az új generációs malware- és vírusvédelemmel.

A SentinelOne végpontvédelem használata esetén a gyors felderítés és megelőzés mellett lehetőséget kapunk arra is, hogy támadás esetén az összes érintett fájlt visszaállítsuk eredeti állapotába vagy töröljük a fertőzött eszközről. Ezenkívül a Marketplace modulon belül folyamatosan bővülő integrációk sora várja az ügyfeleket.
Kínálatunkban megtalálható még a Fidelis Elevate platformja is, amely ha szeretnénk, egy teljesen saját rendszereken futó (on-prem) megoldás, szemben az eddig említett gyártók felhős hátterű kialakításával. Ez a platform ugyan kifelé kevésbé nyitott, de a gyártó saját végponti (EDR), hálózati (NDR) és megtévesztési Deception rendszere együtt dolgozva alkot egy XDR megoldást. A Fidelis Elevate automatikusan összefűzi a naplókat, és felismeri a különböző támadásokat és anomáliákat. A platformban megtalálhatók az XDR/EDR rendszerektől megszokott képességek is, úgymint élő fájlrendszer vagy futtatott folyamatok figyelése, illetve viselkedésalapú támadásfelismerés.
Ahogy a cikk végén felsorolt gyártók esetében is látszik, egyre több fejlett végpontvédelmi megoldás található a piacon. Ezek képességei ugyan nem teljesen egyeznek meg, de van pár dolog, amire ha odafigyelünk, már magas szintű védelmet érhetünk el. Ilyen például, hogy ha egy rendszer nem csak szignatúra alapján képes felismerni egy támadást, illetve képes segíteni nekünk kideríteni honnan indult a fertőzés, akkor már jóval többet tud segíteni az IT-biztonsági csapatunknak, mint egy hagyományos antivírus. ■

Csak ahhoz férjen hozzá a dolgozó, amihez engedélye van!

SailPoint CYBERARK

Egyre többször halljuk, hogy a jelszavakat el kell felejteni, és át kell térni valamilyen erős hitelesítési módszerre. Ezt igazolja az is, hogy napról napra több olyan adatszivárgás történik, ahol a támadók hozzáférési adatokat lopnak el, és ezzel óriási károkat okoznak a cégeknek. A hozzáférési adatokat érintő adatszivárgások és támadások számának évről évre történő növekedése mellett az így kiszivárgott jelszavak adatbázisa is folyamatosan nő, amit egy támadás esetén fel tudnak használni ellenünk.

Érdemes belegondolni abba, hogy egy átlagos felhasználónak hány helyen szükséges valamilyen jelszót megadni, ami sok esetben (a különböző javaslatok és céges előírások ellenére is) megegyezik valamelyik, a céges környezetben használt jelszóval. Vajon mi történik, ha egy támadó összerakja a begyűjtött morzsákat, és felhasználónk adataival belép a vállalati környezetünkbe?

Járvány előtt és után

Korábban, ameddig nem volt szükséges minden rendszert távolról elérni, egy ilyen támadásnak sokkal kisebb hatása lett volna. Egyszerűbb volt megbizonyosodni arról, hogy tényleg az adott kolléga jött be és ült le a gépe elé, amelyről eléri a belső előforrásokat, mint azt követni, hogy távolról ki szeretne hozzáférni a rendszerünkhöz. Részben ezért jelentek meg a különböző erős hitelesítési megoldások, például tokenek, smart cardok. Ennek egy továbbfejlesztett módja az, amikor a felhasználó már bármilyen jelszavas azonosítás nélkül is beléphet például a telefonján lévő biometrikus azonosítással (lásd: ujjlenyomat vagy arckép), esetleg push üzenettel.

Ezek az autentikációs módok az ellen is hatékonyan védenek, hogy a kiszolgáltatott végpontok fertőzés estén ne tudjanak az automatikusan mentett jelszavakkal kárt okozni. Gondoljunk csak bele, hogy egy otthoni munkavégzés esetén milyen IT-biztonsági hiányosságok lehetnek a használt hálózaton, illetve elég pár

perc, amíg egy gyanútlan családtag megnyit egy ártalmatlannak tűnő oldalt, amely a háttérben ellopja az összes belépési adatunkat. A home office munkavégzés ezért még kiszolgáltatottabbá teszi a vállalatokat. A távoli elérés biztosítása mellett legalább ennyire fontos a cégen belüli erőforrások, alkalmazások elérésének a kezelése. Sok esetben a támadások nagy részét meg lehetne előzni, ha minden felhasználó a „least privilege" elve mentén csak a szükséges dolgokhoz férne hozzá. Ha őszinték akarunk lenni, hány olyan esetről tudunk, amikor cégen belül egy kolléga pozíciót vált, és új eléréseket kell adnunk neki, ám a korábbiakat nem szüntetjük meg. Esetleg egy új dolgozó belépésekor mennyire lehetne megkönnyíteni mindenkinek az életét, ha a szükséges jogosultságokat egy központi felületen tudnánk kezelni és nyilvántartani? Majd az elérésbiztosítás utolsó életciklusában, amikor a dolgozónk elmegy, a hozzáférések megszüntetését egy automatizált folyamat tudná végrehajtani, ami nem hibázik és nem kézzel feljegyzett adatokból dolgozik.

Sailpoint IdentityIQ, IdentityNow a CyberArk Workforce Identity-vel kombinálva

Erre a problémára és az elérések kezelésének automatizálására nyújt tökéletes megoldást a Sailpoint IdentityIQ és IdentityNow megoldása, amely a céges hozzáférések teljes életciklusát végigköveti. Automatizált folyamatokkal segíti az adminisztrátorok munkáját belépéskor, pozícióváltáskor és a dolgozók cégtől távozásakor is. Ezeken kívül kialakíthatunk különböző munkafolyamatokat, amelyek kikényszerítik a jogosultságok időszakos felülvizsgálatát és tehermentesítik az adminisztrátorok munkáját jogosultság kérésekor.

Viszont ez önmagában nem nyújt megoldást a hagyományos, jelszóalapú hitelesítés problémájára, ezért érdemes mindenképp kiegészíteni egy erős hitelesítésre alkalmas rendszerrel. Az erre választott megoldás lehet például a CyberArk Workforce Identity (korábban Idaptive). Segítségével a mesterséges intelligencia bevonásával még egyszerűbbé és intelligensebbé lehet varázsolni az erőforrások elérését. A rendszer képes a felhasználói viselkedések elemzésére és intelligens döntések meghozására is. Segít az alkalmazások esetén létrehozni a megfelelő felhasználókat, illetve a jogosultságok kezelését is megoldja. Használatával elfelejthetjük a jelszavakat és könnyen használható SSO (Single Sign-On) megoldást biztosíthatunk a dolgozóinknak.

Ha a két gyártó identitáskezelő megoldásait kombináljuk, akkor a belső, illetve céges környezeteken kívüli legtöbb vállalati környezetben előforduló felhős vagy külső szolgáltatást is egyszerűen integrálhatjuk és jelentősen biztonságosabb módon használhatjuk. Segítségükkel annak az esélye, hogy valaki megszerezze a vállalati hozzáférési adatainkat, majd ezekkel kárt tegyen a céges infrastruktúrában – legyen az akár on-prem vagy felhős – nagy mértékben csökkenthető. Ezenkívül jobban bízhatunk abban, hogy valóban a dolgozónk használja az alkalmazásainkat és ő fér hozzá a rendszereinkhez – azokhoz, amelyekre a munkája elvégzéséhez szüksége van. ■

IT, OT, IoT – a biztonságosnak hitt környezet is potenciális veszélyforrássá válhat

ARMIS.

FORESCOUT

Évről évre egyre több IoT- és OT-eszköz jelenik meg a céges, illetve az otthoni hálózatokon. Egyre elterjedtebbek a különböző épület-automatizálási eszközök, okos szenzorok és egyéb megoldások, amelyek ugyan egyre kényelmesebbé teszik az életünket, ám sokan nem gondolnak a bennük rejlő biztonsági kockázatokra. Ez hatványozottan igaz azokban az esetekben, amikor például egy korábban (akár fizikailag megvalósított szeparáció miatt) biztonságosnak hitt környezetet – például víztisztító telepet, erőművet – az eszközgyártók felügyeleti megoldásai miatt össze kell kötni az internettel.

Ha megnézzük a sérülékenységekről szóló (be)jelentéseket, akár csak a múlt évre szűkítve, láthatjuk, hogy egy év alatt több száz olyan CVE-bejegyzés született, amely érinti az ICS-hálózatok komponenseit. Szintén fontos azt is tisztázni, hogy adott esetben például egy Windows-sérülékenység is érintheti ezeket a környezeteket, mivel – sokszor ugyan számunkra teljesen elfedve – egy régi, microsoftos gép a rendszer tagja. Ez azért veszélyes, mert az ilyen gépeket sokszor nem lehet, esetleg nem hagyják frissíteni, mert az leállással vagy akár a speciális program meghibásodásával járhat.

Érdemes azt is megemlíteni, hogy a frissítések és a javítófoltok (patch-ek) alkalmazása sokszor problémát jelenthet a célhardverek esetében is, mert ezeket telepítés után rendszerint hosszú ideig, akár évtizedekig tervezzük használni, és sok esetben a gyártók nem foglalkoznak a sérülékenységek javításával.

Nemcsak a védelem gyenge, de több a támadás is

Az előbb említett okok miatt sem szabad elfelejteni, hogy a korábban biztonságosnak hitt környezeteket egyre többször éri támadás. Ennek részben az is az oka, hogy az általában kevésbé védettek, mint egy tipikus IT-hálózat. Sok esetben a távoli elérést se egy viszonylag biztonságos VPN-nel vagy más fejlett technológia használatával oldják meg, hanem esetleg egy közös, állandó jelszóval használt távoliasztal-megoldással, amely rögtön a hálózat közepébe visz. Szintén sokszor látjuk azt, hogy ezekben a környezetek-

FORRÁS: SIMPLILEARN.COM

ben a hálózati vizibilitás a legtöbbször csak álom marad, és nincsenek ezt elősegítő megoldások telepítve.
A legtöbbször azt hisszük, hogy a vizibilitás csak az IoT-, illetve OT-környezetek esetén jelent problémát, de nem így van. A személyes beszélgetések során, illetve az általunk forgalmazott gyártók POC vagy demókörnyezetbe telepítésekor nagy érdekességek szoktak kiderülni. Például érdemes gyanakodni, ha az OT-hálózat megfigyelésekor gyanúsan sok az IT-irányú kérés, nem ismert eszközök találhatók a hálózaton, és jóval nagyobb számú felismert, védelem nélküli eszköz van jelen a környezetekben. A vizibilitással kapcsolatos problémák, főleg IT- és OT-hálózatok összekötése esetén, a környezetek akár 80-90 százalékát is érinthetik.

Közel a segítség

Így, hogy remélhetőleg már sikerült minden olvasót megijeszteni, érdemes leszögezni, hogy legtöbbször van megoldás ezekre a problémákra. Az ilyen közös hálózati környezetek esetén erősen javasolt a hagyományos NAC megoldás helyett egy kifejezetten IoT- és OT-eszközök védelmét is ellátni képes megoldást bevezetni. Fontos, hogy akár már egy sima vizibilitást adó megoldás is óriási segítség lehet a környezetek biztonságossá tételében, de ennél még hasznosabb funkciók is elérhetővé válnak számunkra, ha egy professzionális megoldás mellett döntünk. Sok esetben ezek a rendszerek kiterjedt integrációk használatával elősegítik a hálózati szegmentációt, kikényszerítik a biztonsági megoldások frissítését, vagy ha a környezetünk tolerálja, akkor akár sérülékenységvizsgálat futtatását is lehetővé teszik minden frissen csatlakozott végpont esetén.
A Clico magyarországi portfóliójában több ilyen megoldás is található. Az egyik az Armis felhős megoldása, amely képes minimális helyi erőforrásigény mellett, a hálózati forgalom alapján felderíteni a céges rendszereket, és megfelelő vezeték nélküli hálózat esetén akár még a nem Ethernet alapú IoT-eszközökről is képet kaphatunk a hálózatunkban – és mindezt Agent telepítése nélkül.
A másik ilyen megoldásunk a Forescout platform. Ez a rendszer egyben nyújt új generációs NAC funkciókat az IT-eszközök számára, a viziblitást fontos kontrollfunkciókkal kiegészítve, és mindemellett a teljes IoT- és OT-környezetünk védelmét is képes ellátni. A Forescout használatával képet kaphatunk arról is, hogy milyen eszközök kommunikálnak a környezetünkben, ami kiemelten fontos egy ipari környezet esetén, mindezt Purdue-modell szerinti bontásban, így rögtön láthatjuk, ha valamelyik alsóbb szinten lévő eszközünk – valamelyik vezérlő – olyan irányba kommunikál, amerre nem lenne szabad. Az egységes megközelítés emellett lehetővé teszi, hogy kifinomult szabályrendszereket állítsunk fel, és az integrációk használatával akár aktívan beavatkozzunk az ipari környezetek esetében is. ■

THALES

Thales CipherTrust Data Security platform, mint komplex, szervezetszintű adatvédelmi megoldás

Az adatlopásokról, betörésekről szóló jelentések száma riasztó mértékben szaporodik, nap mint nap kapunk híreket a legkülönbözőbb ágazatokban bekövetkezett esetekről.

Evidens, hogy az érzékeny adatok biztonsága létfontosságú minden szervezet számára, és a saját üzleti érdekeken túl a szervezetek által kezelt adatvagyon védelmét globális és helyi adatvédelmi szabályozások is egyre kiterjedtebben kérik számon. Egy biztonsági incidens esetén a saját intellektuális tulajdon elvesztésén kívül a hatóságok által kiszabott pénzbüntetéssel is lehet számolni a nem megfelelően kezelt és védett személyes adatok miatt.

A felhős szolgáltatások használatának aránya és mértéke is növekszik, ami újabb kihívásokat jelent az adatvédelem és a szabályozási előírásoknak való megfelelőség számára, mert ebben a változó környezetben a bevált helyi védelmi rendszerek és a végpontokon használt hagyományos megoldások már kudarcot vallanak, vagyis a tárolt adatok védelmére más megoldást kell keresni.

Titkosítás: az első védelmi vonal

Itt jön képbe az adatok teljes körű titkosítása, mint végső védelmi vonal. Egyszerű belátni egy ilyen megoldás előnyeit: ha már minden más védelmi rendszer csődöt mondott és a támadó közvetlen hozzáférést szerez egy rendszerhez, akkor hiába másolja le az adatokat, ha azok titkosítva vannak, nem tud az érzékeny tartalomhoz hozzáférni.

A Thales és az általa nemrég felvásárolt Gemalto több terméke egyesül a CipherTrust Data Security Platformban, így egy közös menedzsment alatt vezethetjük be a szervezet érzékeny adatainak védelmét és egységes kezelését.

A platform egységesíti az adatok titkosítását, elősegíti a titkosítási kulcsok és a hozzáférések biztonságos kezelését, egyszerűsíti a adatbiztonságot, segít, hogy rövidebb idő alatt felkészüljünk egy-egy auditra, és biztonságosabbá teszi a felhős rendszerekbe migrálást.

Cél: az átlátható adatvagyon

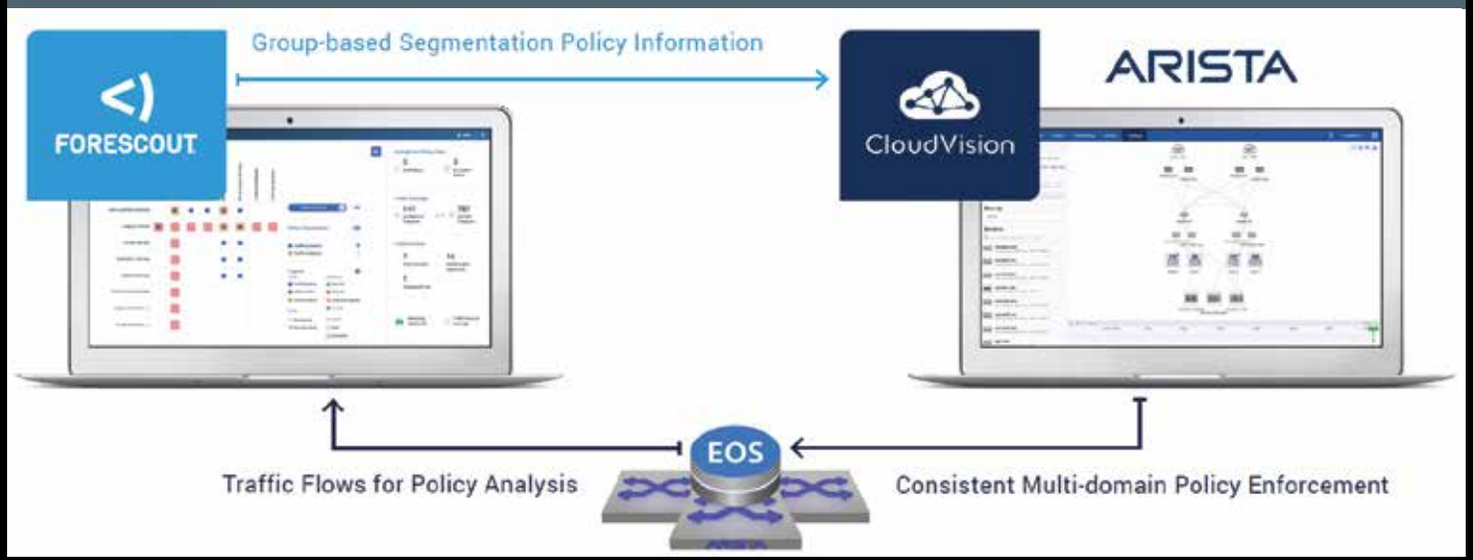
A CipherTrust része egy adatvagyont feltérképező és értékelő modul, amely strukturált (adatbázisok) és strukturálatlan adatokban (dokumentumok, ömlesztett fájlok, archivált tartalmak) is képes keresni. Felderíti az adatokat felhős megosztókon és helyi tárolókon is, majd a felfedezett adatokról kockázati elemzéseket készít. Számtalan előre definiált sablonja segítségével támogatja az egyes (GDPR, PCI DSS, HIPAA stb.) szabályozásoknak való megfelelést.

A már megismert és leltározott adatokat számtalan módon képes védeni illetéktelen felhasználás ellen: hozzáférések szabályozásával, alkalmazásszintű titkosítási réteggel, transzparens titkosítással fájlok, adatbázisok, konténerek, big data megoldások részére, de akár statikus/dinamikus adatmaszkolással is.

A központi felületről áttekinthető a szervezetnél található teljes adatvagyon elhelyezkedése, azok biztonsági állapota. Erről az egységes menedzsmentkonzolról szabályozható a hozzáférés és egységes titkosítási kulcsmenedzsmentet is kínál. A kulcsok kezelését FIPS 140-2 szintű fizikai védelemmel rendelkező HSM-ekkel valósítja meg. Természetesen gazdag riportlehetőségeket is biztosít a kezelt adatok típusairól és az azokhoz történő hozzáférésekről. Ez az egységes platform nemcsak a helyi, hanem a felhőszolgáltatásokban lévő adatok kezelését is ellátja, így ténylegesen egy helyről kezelhető és átlátható a teljes adatvagyon. ■

Zero Trust hálózatok kialakítása az Arista és a Forescout együttműködésével

ARISTA
FORESCOUT



Ha megnézzük a hálózatokkal és az IT-biztonsági megoldásokkal kapcsolatos mai trendeket, akkor legtöbbször azt láthatjuk, hogy a hálózati infrastruktúra és a védelmükre kifejlesztett megoldások egyre inkább együttműködnek egymással.

Legtöbbször a hagyományosan csak hálózati eszközgyártók felvásárolnak valamilyen IT-biztonsági megoldást, vagy másik utat választva technológiai partnerségre lépnek a biztonságos vállalati környezetek kialakítása érdekében. Ilyen például az Arista Networks és a Forescout között a Zero Trust hálózati koncepció kapcsán született partnerség. A koncepció hálózati oldalát az Arista Networks elismerten stabil és megbízható, a legnagyobb adatközpontokban is bizonyított switch-ei, illetve az Arista CloudVision központi management megoldása adja, a biztonsági, illetve szegmentációval kapcsolatos tudást pedig a Forescout újgenerációs NAC megoldása hozza a „házasságba".

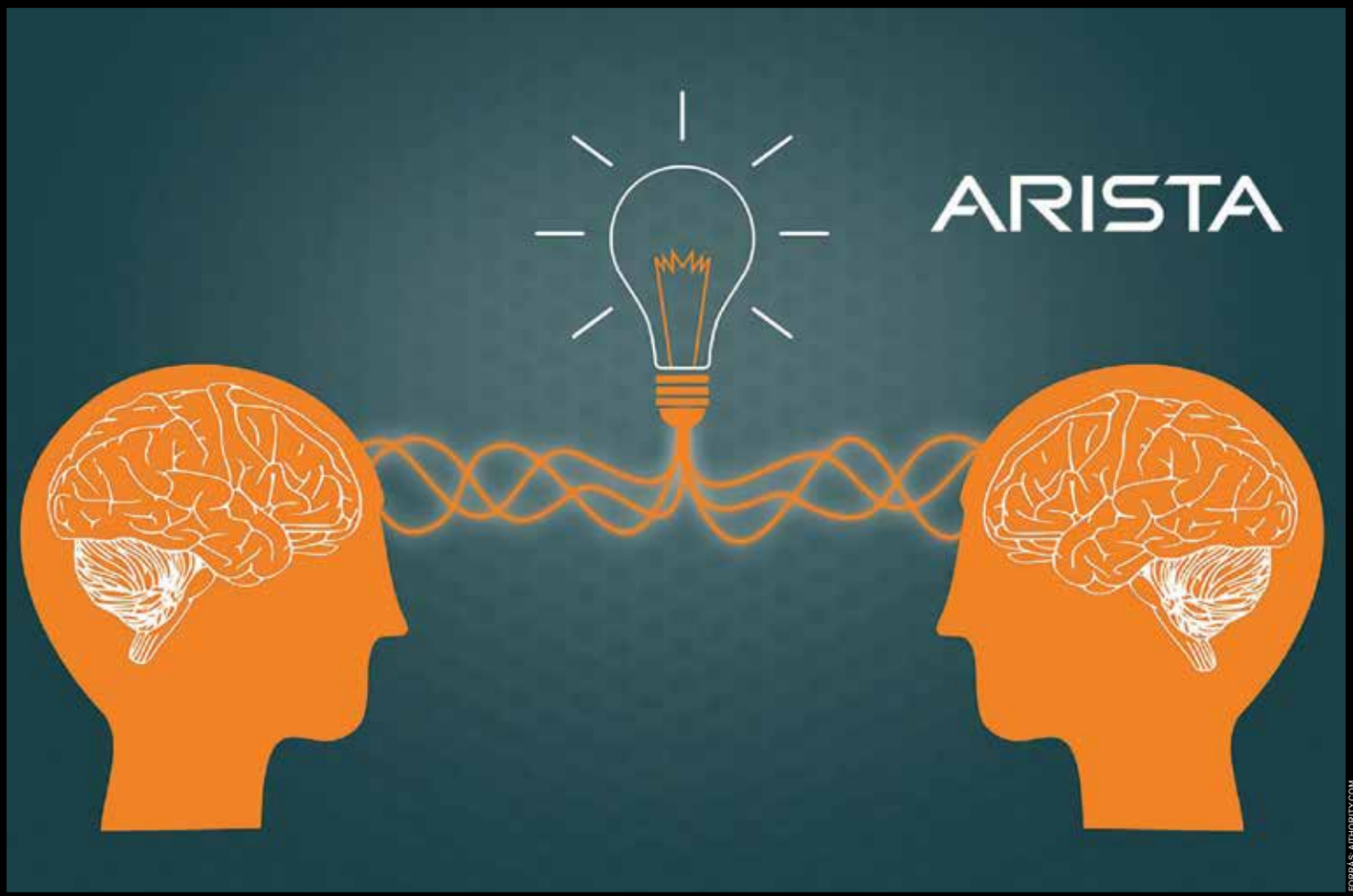
Az ilyen megoldások iránti igényt a vállalatok rohamos fejlődése és a digitális transzformáció hozza magával, mivel sok esetben a tradicionális hierarchikus kialakítás, illetve a hagyományos szegmentáció a gyors fejlődés és az eszközök kommunikációjának útjába áll. Ezért azt láthatjuk, hogy sokszor „lapos", horizontálisan növekedő hálózataink vannak, ami erősen csökkenti a hálózatunk biztonságát. Az ilyen hálózatok nem engedik meg, hogy bárhol dinamikusan szűrést vagy kontrollt alkalmazhassunk. Ez a probléma az üzemeltetők és a biztonsági felelősök rémálma.

Elmúltak az egyszerű „dot1x"-es idők, hiszen amit a 802.1x nyújt, az nem elég granuláris, és sokszor pontatlan, mivel csak alapinformációt közöl az eszközről, ha pedig az irodában használt okoseszközöket szeretnénk a hálózatra kapcsolni, sok esetben a fizikai, MAC címük alapján kell kivételeket tennünk.

Fontos észben tartanunk, hogy bármennyire is szeretnénk elkerülni, a kliensek folyamatosan mozgásban vannak a hálózaton. Szoftvereik ugyan a legtöbbször frissülnek, de előfordulhat, hogy mégsem, sőt mi több, a humán faktornak köszönhetően néha olyan dolgok is felkerülnek az eszközökre, melyek már konkrét veszélyt jelentenek – nemcsak az adott felhasználóra, hanem a hálózat többi kliensére is.

Arista MSS

Az Arista Macro-Segmentation Service (MSS) a hagyományos (vlan, vrf, port acl) szegmentációs megoldásokon felül képes új opciókat alkalmazni a kliensek házirend alapú kezelésére. A jól működő megoldásokban az eszközcsoportokat teljesen el kell különíteni egymástól, és más, szerepkörök szerinti házirendeket kell a kliensekre alkalmazni. Például egy beléptetőrendszer felületét el kell érnie egy arra jogosult személynek, hogy lássa, ki halad át éppen, a rendszernek pedig el kell érnie egy olyan adatbázist, ahol az áthaladó személy azonosítóját ellenőrizheti. Hagyományosan ezt meg lehetne oldani azzal, hogy közös hálózatba tesszük őket, viszont ez nem nyújt elég biztonságot, illetve felesleges támadási csatornákat nyit meg. Ha jobban megvizs-



FORRÁS: AITHORITY.COM

gáljuk a példát, akkor láthatjuk, hogy egy beléptetőkapu valószínűleg nem fog egy másik beléptető kapuval beszélni, még akkor se, ha egy hálózaton vannak, és általában véve igaz ez a biztonsági személyzet munkaállomásaira is.
Ilyenkor az MSS-megoldást használva, három csoportot létrehozva, a megfelelő irányokat megadva, az eszközök egymással nem beszélhetnek, de ha szükséges, az adatbázist elérik, a személyzet is látja őket, és egyéb erőforrásokhoz is hozzáfér, illetve az adatbázisszerver hozzáférése is korlátozható. Persze legtöbbször ezek a csoport telephelyek és „layer 3" rétegek felett ívelnek át, és telephelyváltások, IP-cím és VLAN újrakiosztások is lehetnek menet közben.

Forescout NAC

Erre a logikára építve az MSS-Group képes egy open API-t nyújtani harmadik fél számára – mint például a Forescout újgenerációs NAC megoldása –, ami lehetővé teszi, hogy a házirend- (policy) változásokat ott tudjuk követni, majd az onnan visszaérkező információk, tag-ek alapján képes beavatkozni a CloudVision. Ahogy változik a csoporttagsága egy eszköznek, vagy egy teljesen új eszköz lép a hálózatra, a Forescout frissíti az információkat a CloudVision-ben, ami jelzést és megerősítést küld vissza és beállítja a megfelelő házirendeket.
Az MSS-Group használatának további előnye, hogy a használt eszközöknek nem feltétlenül kell egy gyártótól származniuk, mivel nem egyedi Ethernet tageket használ és a kikényszerítést magukon az MSS-Group megoldást támogató eszközökön valósítja meg, ideális esetben már az „access layer"-ben.
Ezen az integráción kívül fontos megemlíteni, hogy az Arista CloudVision megoldása hálózatépítés esetén képes akár a legbonyolultabb adatközponti környezeteket is könnyebben kezelhetővé tenni. Segítségével a kompatibilis switch-einket monitorozni és konfigurálni is tudjuk, illetve a hálózatunkról egy teljes áttekintő képet is kaphatunk.

Nyíltság, integrálhatóság

Az Aristához hasonlóan a Forescout platformot is érdemes önállóan megvizsgálni. A platform számtalan kulcsrakész integráció használatával egy valós megoldást nyújt a vállalatok hozzáférési igényeinek a kezelésére.
A platform támogatja az IT-eszközökön kívül az IoT-, illetve az OT-hálózatok kezelését is, szükség szerint akár teljesen agent nélküli, passzív hálózati forgalomfigyelés használatával.
Mindez azt mutatja, hogy a két gyártó szerint a biztonságos(abb) jövő felé vezető út a nyílt gondolkodáson és integrálhatóságon keresztül vezet. Esetünkben ez főleg azt jelenti, hogy egy hálózat akkor képes jól működni, ha a hálózati elemek képesek több ponton, minél több esetben kétirányú információ cserével csatlakozni a használt biztonsági megoldásokkal. ■

Védett vonalak – titkosítás, és ami mögötte van

THALES

N CIPHER AN ENTRUST DATACARD COMPANY

ENTRUST

FORRÁS: PAYMENTEXPERT.COM

Ma már szinte egyértelműnek vesszük, hogy a legtöbb hálózati forgalmunk titkosítva halad az interneten, és nem lehet túl egyszerűen lehallgatni. Sokan nem gondolnak bele, hogy milyen protokollok, illetve technológiák kellenek ennek a technikai megvalósításához.

Napjaink legsűrűbben használt protokollja webes forgalmak esetén a Transport Layer Security (TLS). A TLS protokoll egy kriptográfiai protokoll, amely a titkosított web forgalomnak, a HTTPS-nek az alapja, és ez az a protokoll, amely megvédi a webes felhasználói forgalmat a hálózati támadásoktól, lehallgatástól. Eredetileg az SSL protokollt használták erre a célra, de az évek során számos gyengeségére derült fény. Az idő múlásával ezek elhárítására hozták létre a TLS protokollcsaládot, ironikus módon ezekben is sorra kerültek elő súlyos problémák, melyek miatt már a protokoll 1.3-as verziójánál tartunk.

A titkosított protokollok mellett ennek a titkosítási architektúrának másik fontos alkotóeleme a tanúsítványok használata. Amikor titkosított kommunikációról beszélünk, legtöbbször aszimmetrikus, avagy publikus kulcsalapú (PKI) kriptográfiát értünk alatta. Külön cikk témája lenne ennek az architektúrának az ismertetése, ebben a cikkben csak röviden foglalkozunk vele, most arra fókuszálunk, ahogyan a tanúsítványok kezelése a különböző biztonsági megoldásoknál előkerülhet. Tehát a tanúsítványok azt a publikus

kulcsot igazolják, melyek a titkosított forgalmak biztonságát, integritásukat illetéktelen hozzáférés ellen, valamint hitelességüket biztosítják.
Ha csak ennyi lenne a történet, akkor a világ összes szerverének (netán a klienseknek is) be kellene gyűjtenie és követnie minden „cert” lejáratát/visszavonását.
Ezt a problémát szüntetik meg a hierarchikus felépítésű „certificate authority-k” (CA-k) rendszere. Ezen „CA-k” szervezeteken belül is létezhetnek. Jól látható tehát, hogy ezen tanúsítványok biztonságának garantálása is létfontosságú a szervezetek számára, és ezért fontos, hogy ezek védelmére az őket használó többi biztonsági eszköz is fel legyen készítve. Erre hozunk az alábbiakban néhány példát.

Problémák a tanúsítvánnyal

Fontos, hogy modern tűzfalaink közbe tudjanak lépni olyan esetekben, amikor az internetes forgalomban felhasznált tanúsítvánnyal egyértelmű problémák vannak. Lejárt vagy ismeretlen kibocsátó esetén megállíthatjuk embereinket a szakadék szélén és blokkolhatjuk a forgalmat. Viszont abban az esetben, ha például csak egy régóta nem karbantartott oldalra akarnak tévedni, amely kizárólag már elavult titkosításokat támogat, lehet, hogy elég csupán figyelmeztetést adnunk. Ennél természetesen mélyebb szinten is bele tudnak szólni biztonsági megoldásaink az internetes forgalom kapcsolataiba.
Amikor a kliensek a világháló felé haladnak, egy úgynevezett „forward proxy” szerepet tölt be a tűzfal, amelynek ahhoz, hogy ki tudja szűrni az esetleg phishing oldalakat, felnőtt/tiltott tartalmakat és malware-eket, bele kell néznie a titkosított forgalomba. Itt máris előkerül a tanúsítványok kérdésköre, mivel a forgalmat ki kell titkosítani az átvizsgáláshoz, majd a kicsomagolt forgalmat vissza kell titkosítani, hogy tovább folytathassa útját biztonságosan az interneten a célállomás felé. A tűzfalainknak rendelkezniük kell az ezen forgalmakhoz való hozzáféréshez a titkosítási kulcsokkal, tanúsítványokkal, viszont nem feltétlen jó ötlet minden szerverünk kulcsát és tanúsítványát felmásolni az adott biztonsági megoldásra, illetve „CA” aláíró tanúsítványokat tennünk a tűzfalra és a proxyikra. Sokkal biztonságosabb, ha ezeket egy különálló biztonságos Hardware Security Module-ban, avagy HSM-ben tároljuk. Így a titkos kulcsokat a tűzfal felületéről nem lehet kinyerni, hiszen azok nem hagyják el a modulokat.

Keményebb a védelem hardveres titkosító modullal

Egy általános példa erre, ha megnézünk egy Palo Alto Networks-tűzfalat, amelyet egy Thales Luna HSM-mel vagy Entrust nChiper HSM-mel integrálunk. Ebben az esetben, ha a webes forgalmak esetén URL filteringgel szűrjük az irodai forgalmunkat, mivel a klienseink nagy része még TLS1.2-vel kommunikál a külvilág felé, nem feltétlen van szükség minden forgalom bontására, enélkül is láthatunk bizonyos paramétereket.
Azokban az estekben viszont, amikor a kommunikációhoz magasabb biztonsági szintű protokollt használnak, illetve amikor mindenképp szeretnénk mélyebb vizsgálatokat végezni a forgalomban, akkor használhatjuk a HSM-en tárolt aláíró tanúsítványt a forgalom ki- és betitkosításához, illetve a befelé jövő kapcsolatok esetén a szerver kapcsolatainak vizsgálatához. Mert a vissza irány is működik, amikor a világhálóra kitett szervereinket – például webszervereket – kell megvédenünk különféle támadásoktól, ismert expoitoktól, és itt még könnyebb dolgunk is van, mert elég, ha ezen szervereknek a kulcsához hozzáfér az adott megoldás.

Mélyebb vizsgálat magasabb biztonsági szintet ad

Szintén előfordulhat, hogy ha az általunk használt webszerverek esetén mélyebb vizsgálatoknak szeretnénk alávetni a forgalmat, hogy magasabb biztonsági szintet biztosítsunk ezen szervereknek, akkor lehetőség van úgynevezett WAF-ok (Web Application Firewall) használatára, amelyek nemcsak ismert exploitokra, hanem a protokoll alapos ismerete és feldolgozása által az adott webalkalmazás működéséből adódó speciálisabb támadásokra, rosszindulatú tevékenységekre is képesek szűrni. Ezek tradicionálisan „reverse proxy”-két működnek, tehát nem a klienseinket és az általuk kezdeményezett forgalmat, hanem szolgáltatásainkat védik a külvilág felől érkező kérésektől. Ebben az esetben is érdemes a webszerverünk hitelességét biztosító tanúsítványunkat egy biztonságos HSM-en tárolnunk és ezen keresztül felmutatnunk, mikor szükséges a forgalom számára. Ilyen integráció valósítható meg az Imperva piacvezető WAF megoldása és a már említett Thales Luna és Entrust nCipher HSM eszközök segítségével.
A fenti példákból is látszik, hogy habár azt már magától értetődőnek vesszük, hogy a forgalmunk titkosítva halad, és bizonyos megoldások képesek ebbe belenézni, ezzel még nem tekinthetjük a céges hálózatunkat biztonságosnak. Lehet, hogy a tűzfalunk és más biztonsági megoldásaink képesek az ilyen forgalmak bontására, de legalább ennyire fontos, hogy a kulcsaink védelmével is foglalkozzunk és ne csak azzal, hogy mi halad a kapcsolaton belül. ■

A forgalom biztonságos vizsgálata – de hogyan?

A TLS1.3-as verziójával a fejlesztők elmozdultak az autentikált titkosítások (AEAD) irányába, a régebbi, korábban a visszamenőleges kompatibilitás miatt megtartott, ám biztonsági szempontból elavult algoritmusokat elhagyva. Többek között eltávolították a statikus RSA és Diffie-Hellman készleteket, és megjelent a gyorsabb és biztonságosabb Elliptic Curve algoritmusok támogatása. A kommunikáló felek között immár a teljes kulcscsere-folyamatot titkosították, ezzel számos korábbi támadási mód lehetőségét is kizárták. Azzal, hogy lecsökkentették a használható kulcscsere-algoritmusokat és a paraméterkészletet, további általános teljesítménynövekedést értek el. Elsőre azt gondolhatnánk, hogy egy ilyen változásnak csak előnyei vannak, viszont ez nem így van, mert ez a jelentős biztonságiszint-növekedés új kihívásokat hozott a biztonsági szoftverek számára. Az eddig kiépített szűrési technikák arra a működésre alapoztak, amellyel viszonylag egyszerűen bonthatóak voltak a titkosított webes csatornák, és ezáltal például a céges tűzfalakon, proxy-kon vizsgálható volt a forgalom tartalma biztonsági szempontból. Ezzel az új típusú, jelentősen megerősített TLS 1.3-mal a védett forgalmak kezelésére új megoldásokat kell találnunk a forgalom biztonságos vizsgálatára.

Addig a miénk, amíg meg tudjuk védeni!

A digitális transzformáció egyik legjellemzőbb vonása a felhős szolgáltatások használatának robbanásszerű terjedése. Egyre többen veszik igénybe és egyre több dologra is használjak ezeket. Vadonatúj technológiák jönnek létre és terjednek el, lásd a hagyományos virtualizációt tovább gondoló konténeres megoldások, ezen konténeres rendszereket felügyelő management rendszerek, „infrastructure as a code", és serverless megoldások.

Ezek a megoldások legtöbbször felhőben futnak, a felhőben adminisztrálják őket, ezért egyre gyakoribb a fejlesztői rendszerek felhős működtetése is. Ezek a felhasználási formák újfajta kockázatokat, támadási felületeket hoznak magukkal, amikre sokszor csak új, eddig nem ismert biztonsági megoldásokkal tudnunk reagálni.
Ilyenek például a felhős szolgáltatások beállításait ellenőrző és szabályozásoknak való megfelelőséget biztosító megoldások. Azt látjuk, hogy az ismertebb sérülékenységmenedzsment-rendszerek is felkészültek az ilyen rendszerek elemzésére, például képesek egy adott konténeres image-ét még futtatás előtt a felhős repositoryban megvizsgálni és jelenteni róla. De megjelentek a felhős rendszerekre készült identity megoldások is. Nem szólva a DevOps folyamatokba beépülő megoldásokról, melyek az egyre többször elhangzó „shift left" filozófia betartatásában segítenek.

Az egyik legújabb trend az Infrastructure as Code (IaC)

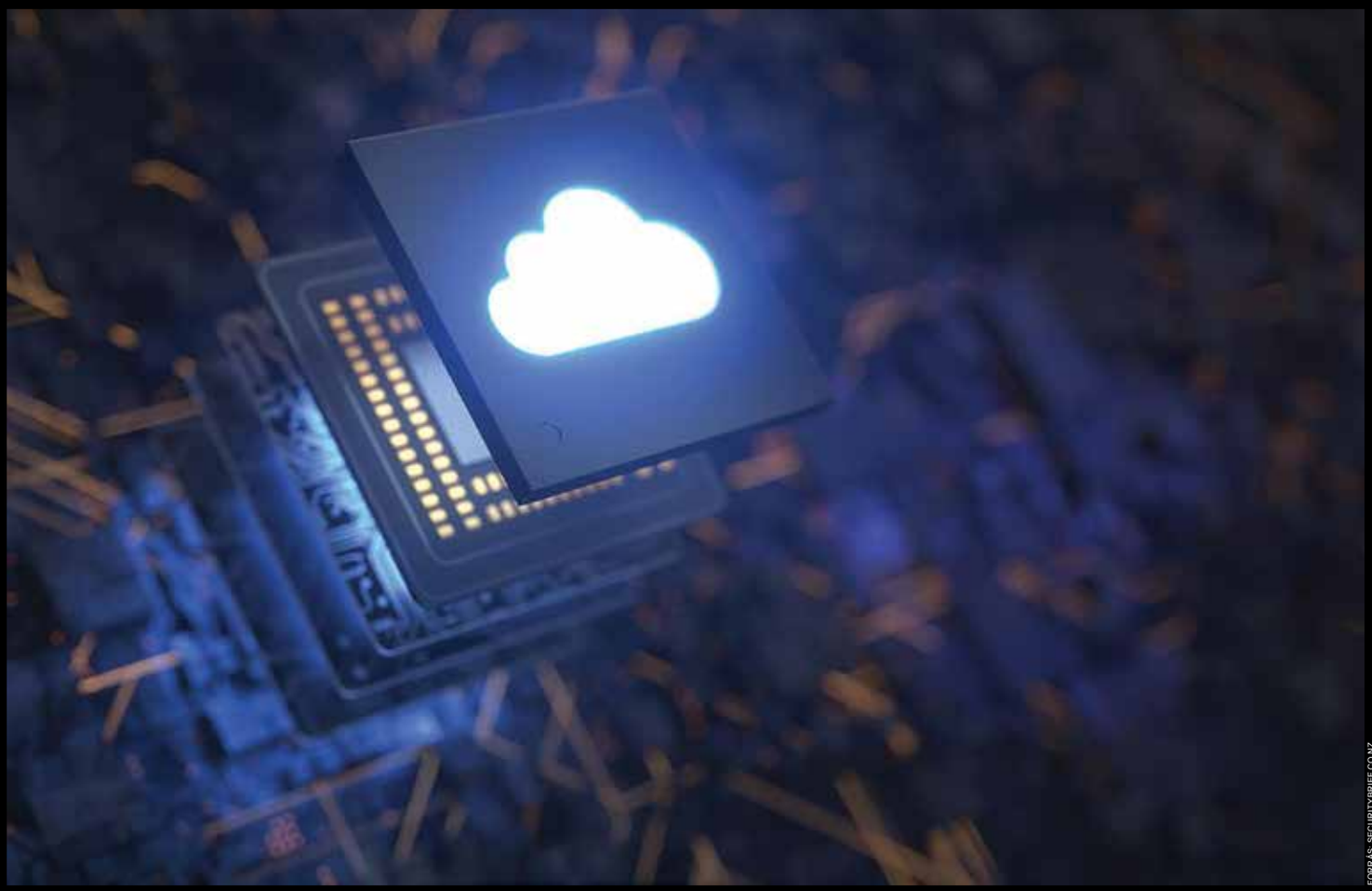
Ebben a működési modellben a felhős szolgáltatások (vm-ek, konténerek stb.) menedzselését, indítását és megállítását felhős DevOps környezetekben egyre többször már nem az üzemeltető csapat végzi, hanem a fejlesztőcsapat kezébe kerül az irányítás. Ők legtöbbször ezt scriptekkel és machine readable definiciós fájlokkal, automatizálva végzik. Ezzel ugyan kisebb lesz a terhelés a hagyományos infrastruktúra elemeit üzemeltető csapatokon (és sok esetben még a változások gyors lekövetésével sikerül a költségeket is csökkenteni), de újabb támadási felületet jelent a cég felhős környezetei esetében. Elég csak arra gondolni, amit már más folyamatok során megtapasztaltunk, mégpedig, hogy az alkalmazásfejlesztők általában nem a biztonsági szempontokat tartják szem előtt. Ezért fontos, hogy ebbe a folyamatba is képesek legyünk belelátni és automatizáltan kikényszeríteni még a telepítés előtt a legfontosabb elvárásainkat.

Rapid7 Divvycloud

A Clico által a piacon képviselt gyártók közül a Rapid7-nek van egy kimondottan a multi cloud környezetet használó szervezetek igényeit kielégítő megoldása, a Divvycloud. Ez képes felderíteni és osztályozni az adott szervezet által használt felhős erőforrásokat, compliance-vizsgálatokkal segíteni a különböző előírásoknak való megfelelést, vagy csak egyszerűen javaslatokat tenni a biztonságosabb és kockázatmentesebb beállításokra. Képes ellenőrizni a felhasználó jogosultságokat, jelszó házirendeket definiálni, segíti a szerepkköralapú felhasználó- és hozzáférés-kezelés-menedzsmentet (IAM funkcionalitás), multifaktoros autentikációt kikényszeríteni.
A hálózati támadások ellen képes API szinten integrálódni a szolgáltatók saját megoldásaival (például Amazon GuardDuty-val) vagy más partnercégekkel, és hatékonyan, valós időben, automatikusan beavatkozni fenyegetés esetén (például kriptovalutabányász-kód vagy káros botkommunikáció észlelése esetén), esetleg felismerni ismert rosszindulatú forrásoktól érkező API-forgalmakat.
Átfogó monitorozást és analitikát biztosít a használt erőforrásokról, így segítve a költséghatékony működést és erőforrás-menedzsmentet. Nemcsak a compute instance-okra terjed ki, hanem magába foglalja a felhős adatbázisokat, továbbá big data, cache, search összetevőket is. Jelenleg minden jelentősebb publikus felhőt támogat (Amazont, Azure-t, Google Cloudot, Alibaba Cloudot).

Valaki más számítógépe

Népszerű definíció a felhőre a „valaki más számítógépe" hasonlat. Ebben az írásban nem is a futtatókörnyezet-infrastruktúra tulajdonjoga szempontjából vizsgáljuk a „felhő" biztonsági vonatkozásait, hanem az IT-megközelítés szempontjából. Ha egy rendszer/alkalmazás „felhős" technológiákkal, de a „földön" fut, attól még a felhős környezetekre jellemző biztonsági megközelítéssel kell kezelnünk, legyen az Openshift, Tenzu vagy bármilyen, ma reggel megjelent friss technológia. A közös metszéspont sokkal inkább az lesz, hogy ezeknek az elemeknek a fejlesztése és üzemeltetése nem válik el élesen egymástól, sokkal inkább DevOps megközelítésű. Cikkünkkel az a célunk, hogy ezt megpróbáljuk a DevSecOps megközelítés felé tolni, miszerint hiába vagyunk roppant agilisak a fejlesztési és üzemeltetési területünkön a végletekig automatizálva azt, de az így teremtett vállalati érték addig a miénk, amíg meg tudjuk védeni, azaz szükségszerű a biztonsági szempontokat is beépíteni a folyamatainkba. Minél inkább a folyamat elején tesszük ezt, annál magasabb biztonsági szintet tudunk elérni, és annál súrlódásmentesebb lesz az összes érintett rendszer együttműködése.



FORRÁS: SECURITYBRIEF.CO.NZ

A Rapid7 további szolgáltatásokat is kínál, amelyekkel még tovább bővíthető a DivvyCloud, így az InsightVM sérülékenységmenedzsment-platformmal képes egyrészt a felhős compute instance-ok részletes vizsgálatára, felhős konténeres környezetekhez API-n keresztül kapcsolódva képes a repository-ban lévő konténer image-eket akár futtatás előtt is ellenőrizni, de természetesen helyi környezetek is vizsgálhatók vele. De kiegészíthető a Rapid7 további Insight Platform összetevőkkel is, mint például a web alkalmazások vizsgálatára alkalmas InsightAppSec-kel vagy a platform SOAR megoldásával, az InsightConnecttel, amellyel szélesebb körű automatizációs feladatok is megoldhatók.

Palo Alto Networks Prisma Cloud

A másik, Clico által képviselt gyártó, a Palo Alto Networks Prisma Cloud megoldását kicsit közelebbről megvizsgálva láthatjuk, hogy jól átgondolt, minden támadási vektorra kiterjedő „cloud native” biztonsági platformot alakítottak ki. A gyártó rövid idő leforgása alatt szinte számolatlan mennyiségű pénzt költött különböző cégek felvásárlására, melyek mély integrációjával és továbbfejlesztésével kialakította a Prisma Cloud platformot.

A megoldáscsomag magába foglalja a legtöbb ismert cloud security támadás elleni védelmet, például CSPM (Cloud Security Posture Management), CWP (Cloud Workload Protection), CIEM (Cloud Infrastructure Entitlement Management. Ezeken felül a közelmúltban belekerült a WebApp és API security, „identity based segmentation”, illetve a Bridgecrew felvásárlással már az „infrastructure as a code” környezetek biztosítását is képes megoldani. A biztonsági platform képes megvédeni a cégek virtuális gép alapú környezeteitől kezdve akár „serverless” alkalmazásokon át nagyjából bármit, ami privát, hibrid vagy publikus felhők esetén előfordulhat.

Ezenkívül a Palo Alto Networks CN sorozatú tűzfalával már akár Layer7 védelmet is ki tudunk kényszeríteni a konténerek közötti forgalmak esetében is anélkül, hogy ki kéne csatornáznunk ezt a Kubernetes környezetünkből. A Prisma Cloud funkcióit természetesen elérhetjük a legtöbb ismert felhős szolgáltató esetében, illetve érdemes fél szemünket a megoldáson tartani, mivel a platform képességeit folyamatosan (hetente!) bővítik újabb funkciókkal.

Egy jól működő felhős védelmi platformmal nagymértékben növelhetjük a cégünk és alkalmazásaink védelmét. Ahogy ebből a rövid cikkből is látszik, szerencsére erre a folyamatosan fejlődő területre is találunk már jó és átfogó IT-biztonsági megoldásokat. Viszont mivel a felhős környezetek nagyon gyorsan fejlődnek, érdemes nekünk is szemmel tartani a változásokat és követni a legújabb trendeket, illetve olyan gyártó mellett elkötelezni magunkat, amely agilisan és folyamatosan fejleszti a felhős védelmi mechanizmusait. ■

Ön dönt: vezet vagy hátradől – avagy az AI-Driven Enterprise

Juniper driven by Mist AI

Mára már természetes, hogy a mesterséges intelligencia által nyújtott pozitív hatásokból a vállalati informatikai hálózatok sem maradhattak ki. Cikkünkben a Juniper Mist AI-Driven Enterprise megoldásáról szeretnénk egy kis ízelítőt adni.

NÉMETH MÓNIKA, SZENIOR RENDSZERMÉRNÖK

A Juniper név valószínűleg sok mindenkinek ismerősen cseng, aki az informatikai hálózatok világában tevékenykedik – de ki az a Mist Systems? Róluk annyit kell tudni, hogy az ő nevükhöz fűződik az első AI-driven (mesterséges intelligencia által vezérelt) vezeték nélküli LAN fejlesztése. a mesterséges intelligencia segítségével sokkal kiszámíthatóbb, megbízhatóbb, mérhetőbb wifi-hálózatot lehet kiépíteni, ahol nagyon fontos mérőszám, hogy a hálózathoz csatlakozott felhasználóknak milyen felhasználói élményben van részük.

Vagyis jóval tovább megy annál, hogy a felhasználó sikeresen csatlakozott a letelepített AP-k valamelyikéhez, amit mi is láthatunk az AP menedzsmentfelületén, a felhasználói is látja a csatlakoztatott készülékén, de valami mégsem kerek, mert például nem tölt be semmilyen oldal vagy nem tud semmit letölteni, vagy kivárhatatlanul lassan működik az egész. De mi mindent megtettünk, hiszen van kapcsolata a vezeték nélküli hálózathoz!

A Mist megoldása ezt teljesen másként kezeli. Ráadásul emellett még olyan „extra” szolgáltatásokat is könnyedén kihasználhatunk, mint például épületen belüli navigálás (egyetemek, kórházak, konferencia központok, bevásárlóközpontok esetén), ahol a belső térben a telefonunkra telepített alkalmazáson keresztül, mint egy navigációs szoftverrel egyszerűen odatalálhatunk meghatározott helyszínekre. De akár célzott üzeneteket is küldhetünk az egyes felhasználóknak, akik egy adott hely közelében tartózkodnak (például egy plázában az adott bolt aktuális akciójáról kap értesítést a vásárló, ha éppen elhalad a bolt előtt), vagy épületen belül pontosan nyomon követhetünk nagyobb értékű, illetve „eltűnésre hajlamos” eszközöket. Továbbá egy, az éppen aktuális helyzethez kapcsolódó fejlesztésnek köszönhetően az eszközök jelezni tudják az operátoroknak, ha egy bizonyos területen belül (például a tárgyalóban) a felhasználók sűrűsége meghaladja az előre definiált limitet.

De ez csak a jéghegy csúcsa. a Juniper Networks 2019-ben felvásárolta a Mist Systems-t, így a „menyasszony” hozományaként az AI nyújtotta előnyök a teljes hálózatra kiterjesztve, a WLAN, LAN és SD-WAN területeket is lefedik, magasabb felhasználói és informatikai élményt nyújtva a hálózat egyes végpontjai között kommunikáló felhasználóknak és üzemeltetőknek.

Nézzük meg, hogyan!

Felhasználói minőségmutatók

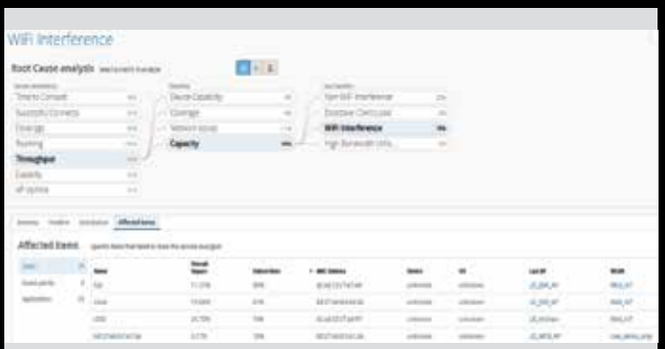
Az első fontos jellemző, amit a bevezetőben is említettem már, nem más, mint a felhasználói élmény megértése a felhasználóra jellemző minőségi mutatók megjelenítésével. *(1. ábra)*

A legtöbb hálózatos cégnél a hálózatmenedzselő rendszereket arra tervezték, hogy képesek legyenek a hálózati eszközök menedzselésére, de ezek a rendszerek nem értik valós időben, hogy mi történik a felhasználóval. a Mist megoldásában minden egyes felhasználó (vezetékes és vezeték nélküli is) valós időben nyomon követhető, hogy megértsük az egyedi felhasználói tapasztalatait.

1. ÁBRA: SLE MUTATÓK

A probléma jellemzői

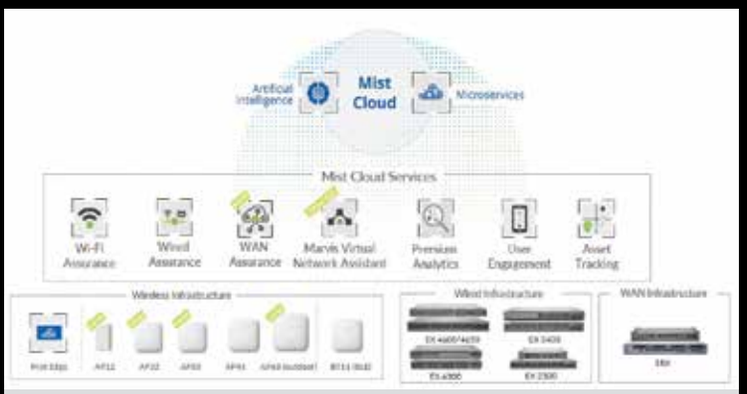
A második nagyon fontos tulajdonság, a megoldásban rejlő mesterséges intelligencia ereje. Ennek segítségével tudhatjuk meg, hogy melyik felhasználóval mi történt, ha valami gond van, akkor azt milyen probléma okozta. Láthatjuk azt is, hogy a teljes hálózatra jellemző az adott probléma, vagy csak egy adott részre. Kik az érintett felhasználók, van-e köztük valami összefüggés? Ezeknek az ismereteknek a birtokában már proaktív hibaelhárításra is képesek leszünk, akár azelőtt javíthatjuk a hálózaton előforduló különböző problémákat, mielőtt az ügyfélszolgálatot a hibával kapcsolatos tömeges telefonhívások árasztanák el. Ezenkívül az AI alapú hálózatok arra is képesek, hogy a hálózati anomáliák bekövetkezése előtti adatokat elmentsék, elősegítve így a hibaelhárítást. *(2. ábra)*



2. ÁBRA:ROOT CAUSE ANALYSIS

Üzletmenet-folytonosság

A harmadik dolog a microservice-eken alapuló felhős környezet, a Mist Cloud, amely az üzletmenet folytonosságát biztosítja. (3. ábra) A Mist Cloud alkotja a megoldás gerincét, és rengeteg előnyt nyújt a felhasználóknak. Például heti rendszerességgel kerülnek be új fejlesztések, javítások, melyek hálózati zavarok nélkül implementálódnak; a rendelkezésre álló szolgáltatások közül hardverbővítés nélkül állíthatjuk össze az üzleti igényeinknek megfelelő „csomagot”. Üzemeltetés szempontjából egy folyamatosan karbantartott, modern környezetet kapunk, üzleti szempontból pedig egy testre szabható, kiemelkedő minőségű megoldáshoz jutunk.



3. ÁBRA: MIST CLOUD

Természetes nyelvű kezelőfelület

A negyedik előnyös tulajdonság pedig az open architektúra és az open API-k. Ezekkel biztosítható az egyes folyamatok automatizálása és a 3rd party IT-partnerekkel történő együttműködés is.
A megoldás egy további nagyszerű dolgot is felvonultat, amely nagymértékben megkönnyíti a hálózati hibaelhárítást. Ő Marvis, „aki” – ha hihetünk az iparági pletykáknak – az angol „marvelous” (csodálatos) szóból kapta a nevét. Marvis egy „natural language” interfész, amelytől angol nyelven leírt, szabadszavas kereséssel kérdezhetünk. Marvis ugyanazt a folyamatot követi, amit egy élő hálózati mérnök is megtenne (csak sokkal gyorsabban, fáradtság nélkül), megkeresi és megmutatja, hogy milyen problémák vannak a hálózaton. Illetve különböző, az esetlegesen felmerülő hibák javítására szolgáló javaslatokat is képes tenni, amiket a hiba javítása érdekében el kell végezni. *(4. ábra)*

4. ÁBRA: MARVIS ACTIONS

Miért fontos mindez? Azért, mert a hálózatoknak folyamatosan alkalmazkodniuk kell a piac változásaihoz, minden pillanatban rendelkezésre kell állniuk, hiszen egy-egy leállás adott esetben több millió forintos bevételkiesést okozhat. Természetesen mindenkinek magának kell eldöntenie, hogy a jelenlegi munkáját milyen mértékben tudná támogatni egy mesterséges intelligencia alapú megoldás. A Mist megoldása rendelkezik ezen a területen a legnagyobb tapasztalattal, ők fejlesztették az első AI alapú megoldást a hálózati iparágban. Marvis az első „natural language” interfész, és azért az jelent valamit, hogy a többi gyártó is próbálja követni az irányukat és „születtek” már máshol is „Marvis hasonmások”.
Én már kipróbáltam, most Önön a sor! ■

CLICO

MAGYARORSZÁGI PORTFÓLIÓ:

ARISTA
ARMIS
CLOUDIAN
COMMSCOPE RUCKUS
cryptme
Cryptshare
CYBERARK
DIGI
ENTRUST
Fidelis Cybersecurity
Forcepoint
FORESCOUT
GREYCORTEX Security for Professionals
imperva
IronNet
JUNIPER driven by Mist AI
MICROSENS euromicron group
mobileiron
opengear A DIGI COMPANY
paloalto NETWORKS
Pulse Secure
radware
RAPID7
Recorded Future
rubrik
SailPoint
SentinelOne
THALES
tufin

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

human hungary

SURVIVOR

2021. 06. 08.

Platina szponzor:

TRAINING360 LSK HUNGÁRIA

Bronz szponzor:

Brightly never enough euJobs HR-Group






www.human-hungary.hu

TOP 25 / 2021

Nem mindenki **SIKERES**, aki sikert ér el,
de minden **SIKERESNEK** tűnő ember ért el sikert!

Az ITB üzenete az, hogy nem elegendő sikert elérni,
meg is kell élni, és át is kell adni azt!

Kik voltak az elmúlt egy év legsikeresebb menedzserei az ICT-világban?

Ezt mutatja meg a **TOP 25-ös lista – idén is**!

A díjakat 2021. szeptember 7-jén ünnepélyes keretek között,
az INSIDE ITB 2021 gálaesten adjuk át.