informatikáról üzleti döntéshozóknak XXII. évfolyam 5. szám 2024. május 7. Ára: 3990 Ft www.itbusiness.hu

ITBUSINESS

A CLICO HUNGARY CSAPATA

FOTÓ: CLICO HUNGARY

NIS2, FELHŐ, BIZTONSÁGI PLATFORMOK

IT-BIZTONSÁG: SOK KÉRDÉSRE MÉG NINCS VÁLASZ

ITBUSINESS ROADMAP2024

01.09.
ITBUSINESS magazin

02.06.
ITBUSINESS magazin
E-Commerce melléklet

03.05.
ITBUSINESS magazin

04.02.
ITBUSINESS magazin

04.23.
Felsőoktatási és munkaerőpiaci különszám

05.07.
ITBUSINESS magazin
Informatikai jog melléklet

06.04.
ITBUSINESS magazin

08.06.
ITBUSINESS magazin
Agrárinformatika melléklet

09.03.
Az ICT-piac Nagykönyve

10.01.
ITBUSINESS magazin

11.05.
ITBUSINESS magazin
E-health melléklet

12.10.
ITBUSINESS ANNO-FUTURUM

03.05.
Software & Technology 2024

03.19.
NIS2

04.04.
Finance & Technology 2024

05.30-31.
ITEXEC 2024

09.10.
Data & Technology 2024

11.12.
Industry & Technology 2024

12.12.
CEO Summit 2024
By ITBUSINESS

További részletek:
www.itbusiness.hu

Szponzoráció:
sales@itbusiness.hu

FOTÓ: ITBUSINESS

Sziebig Andrea emlékére

Vezércikket írni nem mindig egyszerű – van, amikor szinte kifolyik a szöveg a billentyűzetből, máskor sokáig bámulja az ember a szövegszerkesztő fehér hátterén türelmesen villódzó kurzort. Az itt következő sorok azonban talán minden eddiginél nehezebben születtek meg.

Búcsúzni kell, örökre, mégpedig olyan valakitől, aki meghatározó szerepet játszott szakmai életemben, és akinek sorai közel húsz éven keresztül jelentek meg ezeken a hasábokon. Alig egy-két éve voltam újságíró, amikor először kollégám, majd főnököm lett a Computerworld-Számítástechnikánál. Már ott is megmutatta, hogy milyen komoly tényező ő és az általa vezetett lap a magyar IKT-szektorban, de megkerülhetetlen szereplővé az ITBUSINESS-szel vált.

ITBUSINESS és Sziebig Andrea – 2003-tól 2021-ig ez a két név összeforrott a hazai infokommunikciós médiában. A koncepciót ő találta ki, ő formálta kerek egésszé és ő győzte meg egy nyugati – a B2B-világban addig jelen sem lévő – kiadó külföldi igazgatóját, hogy érdemes kiadni az akkor még heti magazint.

A siker nem is maradt el. A piac megismerte, elfogadta és megszerette a lapot. Andrea ismert mindenkit, őt is ismerte mindenki, innen is eredt fantasztikus tájékozottsága, a piaci szereplőket, híreket és folyamatokat illetően. Mindenről tudott, ami az iparágban történt – sokszor olyan dolgokról is, amelyeket az érintettek legszívesebben titokban tartottak volna…

Számtalan olyan ötlettel állt elő, amelyek a maguk idejében még ismeretlenek voltak a hazai IKT-médiapiacon: konferenciák és üzleti reggelik, különszámok, tematikus kiadványok, díjak, és így tovább.

A sikert persze nem adták könnyen. Már jól futott az ITBUSINESS szekere, amikor a kiadó stratégiaváltása miatt az eladás réme fenyegette a magazint. Andrea a kapcsolatait mozgósítva befektetőket toborzott és saját (valamint néhány kolléga) tőkéjét is beletéve, kivásárolta a lapot és a továbbiakban saját vállalkozásban adta ki az ITBUSINESS-t.

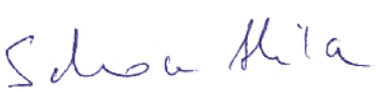
Más szempontból sem adták könnyen a sikert. Andrea számára az ITBUSINESS volt a legfontosabb, azért tűzön-vízen át harcolt, nehéz döntéseket hozott meg, súlyos konfliktusokat vállalt, akár régi barátokkal is. Mivel az ITBUSINESS volt szakmai életének főműve, ezért nehéz volt elképzelni, hogyan adja majd át a stafétabotot. Készült a váltásra, tervezgette a visszavonulást – de azt sem ő, sem a kollégák, sem a szakma nem sejtette, hogy arra kényszerűségből ennyire rapid módon kerül majd sor.

Andrea jó két éve visszavonult, azóta nélküle visszük tovább a kiadót és annak egyre szélesedő portfólióját. Az alapító-főszerkesztő örökségét azzal őrizhetjük a leghívebben, ha folytatjuk, amit ő csinált: az állandó fejlődést, az igazodást a változó piaci körülményekhez.

Isten veled, Andrea!

Következő számunkban hosszabb összeállítással emlékezünk meg Sziebig Andreáról.

SCHOPP ATTILA,
FŐSZERKESZTŐ



Ritter Dávid, ELTE

„A központi menedzsment részeként biztosított védelmi szolgáltatások főbb jellemzői közül talán az a legfontosabb, hogy az ELTE teljes informatikai környezete decentralizált. Ennek részben történeti okai vannak, de a több központú kialakítás miatt nincs olyan forgatókönyv, amely valamennyi, működés szempontjából fontos rendszer leállásával járna."

16. oldal

Jeránek Tamás, Siemens Zrt.

„Az ipari informatikai (IT) és operációs technológiai (OT) rendszerek integrációja kiemelt figyelmet igényel a gyártó- szektor szereplőtől. Az átjárhatóság és az együttműködés ma már nemcsak előny, hanem alapvető elvárás is. Ahhoz, hogy a vállalkozások versenyképesek maradjanak, érdemes bekapcsolódniuk egy szélesebb, ökoszisztémába."

28. oldal

Tobak Tamás, Waberer's International

„A mesterséges intelligencia fokozatosan épül be a napi működésbe, használata egyre inkább el fog mozdulni a klasszikus analitikus alkalmazási területek, az ügyfélszegmentálás, értékesítés és lemorzsolódás-előrejelzés felől az operatív munkafolyamatokba való beépülés irányába."

36. oldal

Hennelné Dr. Komor Ildikó, Komor Hennel Attorneys

„A védjegyoltalom nemcsak egyezőségre terjed ki, hanem az összetéveszthetőségig való hasonlóságra is, ami korántsem egyértelmű. Vannak alapelvek, amelyeket mindenképpen figyelembe kell venni. Számos, különféle paraméterezésű keresést kell lefuttatni, hogy minél nagyobb eséllyel találjuk meg a hasonlónak tekinthető védjegyeket."

48. oldal

ITBUSINESS

COVER STORY

ICT-MARKET

TECHNOLOGY

IPAR 4.0

ITEXEC

FINANCE & TECHNOLOGY

JOGI MELLÉKLET

CLICO MELLÉKLET

#719. ITBUSINESS 2024. május

SZERKESZTŐSÉG
Főszerkesztő
Schopp Attila

Vezető szerkesztő
Kenczler Mihály

Szerkesztők
Justin Viktor, Trautmann Balázs, Vass Enikő

Online szerkesztő
Gróf József

Tervezőszerkesztő
Papp Gyula

Fotó
Vogt Gergely

Kapcsolat
editorial@itbusiness.hu – online@itbusiness.hu

Sales igazgató
Bakos Gergely – sales@itbusiness.hu

Üzletfejlesztési igazgató
Tarnavölgyi Gáspár

Üzletfejlesztési és rendezvényszervezési munkatárs
Csányi Katalin

Event manager
Ordasi Ágnes – rendezveny@itbusiness.hu

Sales
sales@itbusiness.hu

KIADÓ
Kiadja az IT-Business Publishing Kft.
A kiadásért felel: Nagy László ügyvezető

ISSN 1589-3464

Előfizetéses terjesztés
Előfizethető a kiadó ügyfélszolgálatán,
elofizetes@itbusiness.hu

Előfizetési díjak
Egyéves (12 lapszám): 29 900 Ft + áfa
Továbbá előfizetésben terjeszti a Magyar Posta Zrt.
hirlapelofizetes@posta.hu

Digitális előfizetés
ugyfelszolgalat@dimag.hu

Nyomda
Fesztnet Kft. – Wingmix nyomda
www.wingmix.hu

1139 Budapest,
Frangepán utca 7.

24005
9 771589 346407

ITBUSINESS

NIS2, FELHŐ, BIZTONSÁGI PLATFORMOK

IT-biztonság: sok kérdésre még nincs válasz

Kapkodhatja a fejét, aki manapság lépést akar tartani az információbiztonság aktuális kérdéseivel és feladataival. A nagyobb cégek feje felett sötét fellegként lebeg a NIS2 szabályozás és annak előírásai az egyre közelgő határidőkkel. Eközben a felhőszolgáltatások felé nyitó – egyre nagyobb számú – vállalkozásnak fel kell(ene) készülnie az új infrastruktúra jelentette biztonsági kihívásokra. És ha ez nem lenne elég, az IT-biztonsági eszközök technológiájában is komoly átrendeződésnek lehetünk tanúi.

CSINOS TAMÁS, CLICO HUNGARY

FOTÓRÁS: CLICO HUNGARY

Június 30. az első határidő a NIS2 uniós kiberbiztonsági irányelv, illetve azt a hazai jogrendbe átültető 2023. évi XXIII. törvény (a „kibertantv.") előírásainak való megfelelésre – addig kell nyilvántartásba vétetniük magukat az érintett vállalkozásoknak és szervezeteknek, és addig kell a három védelmi osztály valamelyikébe sorolniuk információs rendszereiket. A törvény ugyan már tavaly májusban megjelent, de az érdemi felkészülés igazából január elején kezdődött – azóta eltelt négy hónap, a rendelkezésre álló időszak kétharmada.

Hiányzó szabályozás

„Ehhez képest minden szereplő erős késésben van", állítja határozottan *Csinos Tamás,* a biztonsági megoldásokat forgalmazó Clico Hungary country managere. Ehhez azonban rögtön hozzáteszi: a rendelet végrehajtásával megbízott hatóságok (a Szabályozott Tevékenységek Felügyeleti Hatósága, és a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet), valamint azok szakemberei minden elismerést megérdemelnek az eddig végzett felvilágosító munkájukért. Maguk is szerveznek rendezvényeket, minden eseményre elmennek, ahova hívják őket, de a nyomtatott és elektronikus sajtóban, és saját podcastokban is terjesztik az információt a NIS2-ről.

Ami viszont erősen hiányzik mind az érintettek, mind a felkészülésben potenciálisan segíteni tudó piaci szereplők számára, az a végrehajtási rendelet véglegesítése és nyilvánosságra hozatala. A legfontosabb az a kontroll-lista lenne, amely azt szabályozza, hogy az egyes biztonsági osztályokba sorolt információs rendszereknek milyen feltételeknek kell megfelelniük.

„Január elején kiadták társadalmi egyeztetésre a kontroll-listát, de annak minőségével is akadtak gondok. Nyilvánvaló, és egyáltalán nem is baj, hogy a lista az amerikai NIST SP 800-53 szabvány alapján készült. Az viszont már baj, hogy a magyar lista mintha az eredeti angol dokumentum géppel, rosszul lefordított verziója lenne. Amikor megjelent, a kollégáimmal elkezdtünk végigmenni a közel ezer elemű listán. Az volt a célunk, hogy a szabályozói kontrollokhoz dokumentumsablonokat rendeljünk hozzá, a technikai kontrollokhoz pedig a portfóliónkban megtalálható technológiai elemeket. De nem is fejeztük be, mert olyan minőségű volt a szöveg, hogy nem láttuk értelmét", említi az első komoly problémát ezzel kapcsolatban Csinos Tamás.

Mire is gondolt a minőséggel kapcsolatban? A NIST SP 800-53 igen átfogó információbiztonsági ajánlásgyűjtemény, jóval szélesebb, mint az elektronikus információs rendszereket szabályozó NIS2. „Ha kiberbiztonsági kontrollokat akarunk definiálni, miért kell bevenni a listába az analóg, fizikai dokumentumok védelmére vonatkozó előírásokat, különös tekintettel arra, hogy az uniós jogszabály ezt tagállami hatáskörbe delegálja?", teszi fel a költői kérdést a Clico hazai vezetője.

Ki az érintett?

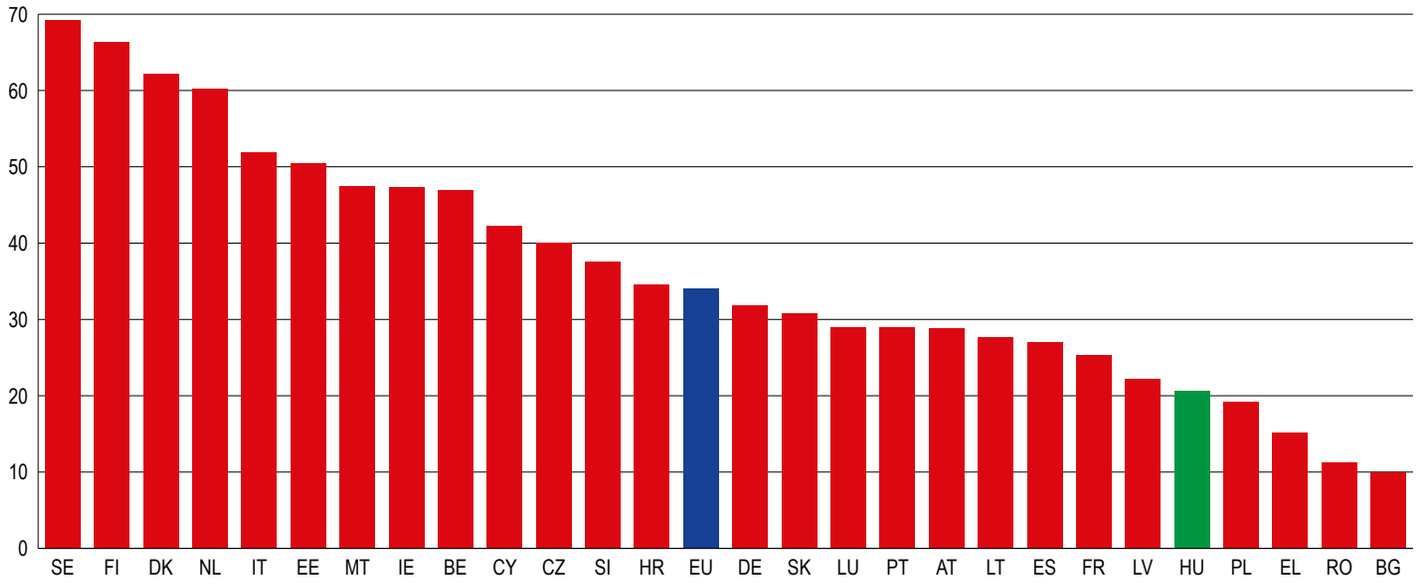
Minden erre irányuló erőfeszítés dacára az sem teljesen egyértelmű, hogy mely vállalkozásokra és szervezetekre terjed ki a NIS2 és a kibertantv. hatálya. Csinos Tamás tapasztalatai szerint ezen a téren óriási még a bizonytalanság. „Beszéltünk végfelhasználókkal, akik tudják, hogy a hatálya alá tartoznak. Beszéltünk olyanokkal, akik nem tudják. Beszéltünk olyanokkal is, akik szerintük nem tartoznak az érintetti körbe, szerintünk viszont igen", érzékelteti a helyzetet.

Vannak persze bizonyos fogódzók, például a törvényben felsorolt vertikumok, illetve az SZTFH a TEÁOR-számok alapján lekért egy cég-

FORRÁS: 123RF.COM

Felhőszolgáltatásokat igénybe vevő vállalkozások aránya, 2023

(Válaszolók százalékában)



listát a KSH-tól – de ezt a listát már nem tette közzé, csak érdeklődésre mondja meg, hogy az adott vállalkozás szerepel-e rajta. Az is kérdés, hogy csak a főtevékenység számít, vagy minden egyéb, amit a vállalkozás korábban felvett a cégjegyzékbe? Jó lenne erről egy hatósági állásfoglalás, mert jelenleg nincs, mondja Csinos Tamás.

Nem lehetetlen egyébként, hogy a listát szándékosan nem tették közzé: a döntéshozók nem akarják, hogy vállalkozások úgy bújjanak ki a NIS2 hatálya alól, hogy leadják az inkriminált tevékenységi kört.

Információhiány hátráltatja a felkészülést

Az általános, több területre is kiterjedő információhiánynak pedig egyenes következménye, hogy az érintettek (és a potenciális érintettek) nem haladnak kellő ütemben a felkészülésben. „Mi most annyit tudunk tenni, hogy azoknál a vállalkozásoknál, amelyek egyértelműen a törvény hatálya alá tartoznak, segítünk az információs rendszerek osztályba sorolásában. Mindenki azt tanácsolja, hogy neki kellene állni a GAP-analízisnek, azaz felmérni a jelen állapot és a követelmények közötti szakadékot. De hogyan mérjük fel az eltérést, ha a kontroll-lista hiányában nem ismerjük a pontos védelmi követelményeket? Persze, kiindulhatunk a már említett NIST SP 800-53-ból, de most még nem tudhatjuk, hogy azt mennyire követi a végleges magyar szabályozás. Fölé- vagy alálövünk a követelményeknek? Elindulhatunk, de a konkrét követelmények ismeretében biztosan finomhangolnunk kell majd a védelmi rendszereket”, említ egy nehézséget Csinos Tamás.

Ugyanez a helyzet a megkívánt szabályzatokkal is. A jelenlegi előzetes ismeretek fényében azokat is el lehet kezdeni megírni vagy frissíteni a meglévőket, de véglegesíteni még biztosan nem tudja őket senki. Különösen nehéz lesz a helyzete az érintett vállalkozásoknak, ha valamilyen okból tavasz helyett csak az ősz elején jelenne meg a végrehajtási rendelet – ez esetben ugyanis gyakorlatilag csak egy hónap maradna, hogy az október 18-i határidő előtt be is vezessék ezeket a kontrollokat.

„Láttunk már arra példákat, hogy információbiztonsági törvényekhez évekkel később jelentek meg a részleteket tisztázó végrehajtási rendeletek. Akkor azonban szűkebb, és főleg állami körről volt szó. A kibertantv. viszont legalább 2500 hazai vállalkozásra, és azok közül is a nagyobbakra, gazdaságilag jelentősebbekre vonatkozik. Nagyon nem szerencsés, hogy ezt a kört olyan bizonytalan helyzetbe hozzák, hogy bármikor lecsaphat rájuk a hatósági vagy auditori szigor”, teszi hozzá mindehhez Csinos Tamás.

Egyedül keveseknek megy

Még ha lesznek is értelmező segédanyagok, magyarázó dokumentumok, sablonok, az is csak az érintettek egy részén segít. Számos, a törvény hatálya alá tartozó szervezetnél nem dolgozik jogász, főállású információbiztonsági és/vagy compliance szakember. Ezek a cégek aligha tudják átfogóan értelmezni a kontrollokat, a követelménylistát

Amit ma megtehetsz...

A számos bizonytalanság ellenére van néhány olyan tevékenység, amelyeket már érdemes elkezdenie azoknak a vállalkozásoknak, amelyek a NIS2 hatálya alá tartoznak. Ezek közé tartozik:

– az informatikai rendszerek (hardverek, szoftverek) felmérése,
– üzletkritikus rendszerek meghatározása,
– előzetes kockázatelemzés,
– adatvagyon nagy vonalakban történő felmérése,
– információbiztonsági felelős kiválasztása,
– tanácsadói kapacitás lekötése későbbi időpontra,
– beszállítói és partneri kör felmérése.

vagy saját erőforrásokat használva elvégezni akár a rendszerek osztályba sorolását, hiszen korábban nem is kellett ezzel foglalkozniuk. Számukra elkerülhetetlen, hogy külső szakértőket vegyenek igénybe a felkészüléshez. A piaci kapacitásokat ez akkor is túlterhelné, ha 6-8 hónap állna rendelkezésre a felkészülésre – egy hónap alatt viszont praktikusan lehetetlen.

Sok esetben ráadásul nem csak informatikai-technikai kérdésekről és döntésekről van szó. Az osztályba sorolás ismérvei közé tartozik, hogy egy adott információs rendszer kritikus-e az üzletmenet szempontjából, illetve hogy milyen kockázatokat tud elviselni a szervezet – ezek pedig üzleti döntések, amelyeket az üzleti vezetésnek kell meghoznia, mint ahogy azt is, mennyi költséget vállalnak be az információbiztonság növelése érdekében.

Hozzáteszi még: rendkívül veszélyes az a hozzáállás is, hogy mivel nincsenek még pontos részletszabályok, sok ügyfél nem csinál semmit. Valóban sok a bizonytalanság, de bizonyos fajta előkészítő tevékenységre már most is szükség van, különben esély sem lesz a feladatok befejezésére. *(Ezek listájáról lásd az „Amit ma megtehetsz…” című keretet!)*

A felhőnek több bejárata is van

A NIS2 és az arra való felkészülés ugyan sokak figyelmét leköti, de messze nem az egyetlen információbiztonsági téma, amellyel manapság foglalkozni kell. A magyar vállalkozások is (végre-valahára) egyre nagyobb számban elkezdték használni a felhőszolgáltatásokat. Viszont ahogy ez gyakran megesik az informatikában, a veszélyekre csak utólag gondolnak, és később kezdenek el foglalkozni azok elhárításával. „Nehéz meggyőzni a döntéshozókat, hogy amikor a felhőstratégiáról döntenek, már az első pillanattól kezdve mérjék fel a kockázatokat is, és gondoskodjanak azok mérsékléséről”, mondja tapasztalatai alapján Csinos Tamás.

Ezzel kapcsolatban felidézi az elterjedt mondást is, miszerint „a felhő igazából valaki más számítógépe”. Annyi igazság mindenképpen van ebben, hogy üzemeltetés szempontjából nem kell foglalkozni a számítógéppel. „De ha valaki úgy érti ezt a mondást, hogy neki egyáltalán nem kell azzal a géppel és a rajta futó szoftverekkel foglalkoznia, akkor rendkívül káros lesz az üzenet”, hangsúlyozza.

Hozzáteszi: számos esetben találkoznak ilyen gondolkodásmóddal. A vállalatnál fejlesztik a felhő alapú szoftvert, szoftvereket, rendszeresen frissítik is azokat, és boldogok, mert jól működik. Amikor a szak-

FORRÁS: 123RF.COM

Felhőbiztonság lépésekben

A felhős rendszerek biztonságánál is alap, hogy a megelőzés mindig hatékonyabb, mint az utólagos védekezés. Ennek alapján Csinos Tamás az alábbiakat javasolja:

– minden új fejlesztés elején gondolkodjanak el annak kockázatkezelési és biztonsági feladatain,
– a kész rendszerek kapcsán is valósítsák meg a védelmi intézkedéseket,
– építsenek ki a rendszerek működését folyamatosan figyelő monitoring rendszert,
– készüljenek fel a NIS2-ben is előírt kötelező incidensbejelentési kötelezettségre.

értők rákérdeznek a biztonságra, a kód esetleges sérülékenységeire, akkor azt mondják, hogy végeznek behatolási (penetrációs, pen-) teszteket.

Csinos Tamás szerint ezzel az a probléma, hogy a teszteket a külső behatolások és behatolók ellen végzik el, pedig, ahogy mondja, a felhőnek és a felhőszolgáltatásoknak két bejárata van: nem csak az internet felől, hanem a céges rendszerek felől is el lehet érni. „A külső pen-tesztek nem mutatják meg, hogy futnak-e olyan szolgáltatások a felhőentitásokon, amelyeknek nagyon nem kellene. Mert ha egy kiberbűnöző valamilyen más úton bejut a vállalati rendszerekbe, akkor ezeket a szolgáltatásokat is ki tudja használni saját rosszindulatú céljaira.”

Előnyt kovácsolni a késésből

Vagyis jó látszik, hogy a felhasználók még nem mérték fel teljes egészében a felhővel kapcsolatos biztonsági kockázatokat és veszélyeket. Ebből pedig valószínűleg az következik, mint ami a hagyományos informatikai infrastruktúrákkal és alkalmazásokkal is történt, vagyis hogy utólagosan építik be a védelmi funkciókat.

„Technikai szempontból ez nem gond, jó minőségű biztonsági funkciókkal később is el lehet látni a felhős rendszereket – csak éppen jóval többe fog kerülni. Célszerűbb lenne, ha a fejlesztési folyamatokban már eleve lennének beépített biztonsági kontrollok, így a teljes környezet biztonsága is magasabb szintre kerülhetne”, mondja Csinos Tamás.

Olyan tanulság lehetne ez, amelyet a magyar vállalatok mások kárán tanulhatnának meg. A magyar piac ugyanis sok szempontból szerencsés időszakban ül fel a felhős hullámra. Sokszor kárhoztatják a magyar vállalkozásokat amiatt, hogy késve karolnak fel bizonyos technológiákat, mint például a felhőt. Ugyanakkor ez lehetőséget is ad arra, hogy tanuljanak az úttörők hibáiból, és ne kövessék el ugyanazokat a baklövéseket, amelyeket mások már elkövettek.

Ilyen hiba például, hogy csak egyetlen felhőben gondolkodtak – mára nyilvánvalóvá vált (és a választék is rendelkezésre áll hozzá), hogy több felhőszolgáltató mellett tegye le a voksát egy szervezet, és mindegyikből azt vegye igénybe, amely a legjobban megfelel üzleti igényeinek és technológiai adottságainak. A másik tipikus hiba az volt, hogy a hagyományos adatközpontban működő alkalmazásaikat változtatást nélkül töltötték fel a felhőbe, miáltal elmaradtak a várt pénzügyi és teljesítménybeli előnyök.

„Vagyis aki egy kicsit is figyel a trendekre, az egyből a felhős működés magasabb fokára léphet fel, nem kell a kísérletezésre költenie. Kihagyhatnak egy-két lépcsőfokot, így a felzárkózás is gyorsabb lehet, nem lesznek riasztó példák a hazai cégek előtt. Bízom benne, hogy a felhő biztonsági oldalával is így lesz, ott is gyorsan felismerik saját érdekeiket a vállalkozások”, teszi hozzá a Clico country managere. *(A lehetséges intézkedésekről lásd a „Felhőbiztonság lépésekben” című keretet!)*

A platformok időszaka jön

A felhő és az általa jelentett biztonsági kihívások csak megerősítettek egy korábban is jelen lévő trendet, nevezetesen az információbiztonsági platformok előtérbe kerülését. Ez erősen összefügg a számítási környezet és a védekezés abból következő változásaival.

Amikor a vállalati alkalmazások a telephelyen működő adatközpontban futottak, egy jól körbehatárolható rendszert kellett védeni – azon belül a felhasználókat, a hálózatokat, az alkalmazásokat. Az internet hatására azonban a határok kinyíltak, a felhasználók nemcsak belső alkalmazásokat értek el az irodaépületen belülről, hanem felbukkantak a webes szolgáltatások, a felhős alkalmazások, valamint a távmunka is. Az új határ a felhasználó lett, őt kell védeni mindenütt és minden körülmények között. A kitettség szélesedésével a biztonsággal tudatosan foglalkozó szervezet akár 10-15 különféle biztonsági rendszert is alkalmazhat különféle feladatokra, ismerteti a jelenséget Csinos Tamás.

Ennyi rendszer működtetése és karbantartása annyi szakembert és szakértelmet igényel, amely sem a felhasználónak, de igazából a szállítóknak sem áll a rendelkezésükre. Márpedig, ha egy biztonsági rendszert nem frissítenek rendszeresen, a beállításaival nem követik a kockázati tényezők és kitettségi helyzet változásait, akkor az nem fogja hatékonyan ellátni a feladatát.

Ez tette szükségessé, hogy a védelmi szigetrendszereket elkezdjék konszolidálni, egyetlen platform alá terelni. „Adja magát a végponti és a hálózati telemetria – ami az egyiken megjelenik, az előbb-utóbb a másikon is feltűnik, tehát érdemes a kétféle adatsor korrelációját elvégezni. Ha erre két külön rendszerem van, és egy harmadikban végzem az elemzést, máris három szállítóval, három, különféle tudást igénylő üzemeltetési személyzettel kell számolnom, és ha az egyik gyengébb a többinél, máris gyengül a védelem. Ha a fenti rendszerek egyetlen gyártótól származnak és egységes XDR-környezetet alkotnak, akkor egységes hozzájuk a támogatás is, és számíthatunk arra, hogy mind a három ’láb’ egyenszilárdságú”, mondja Csinos Tamás.

Aki egy kicsit is figyel a trendekre, az egyből a felhős működés magasabb fokára léphet fel, nem kell a kísérletezésre költenie.

A szélesebb funkcionalitású biztonsági platformok előnye még, hogy többféle kontroll is kialakítható a segítségükkel, miközben a mögöttes információtartalom, a végpontokból vagy a hálózatról származó adatok egységesek. Egyszerűbb a menedzsment, könnyebb reagálni a változó biztonsági környezetre és igazából csak egyféle szakértelemre lesz szükség a vállalaton belül, nem kell minden termékre külön csapatot fenntartani.

Schopp Attila

FORRÁS: FREEPIK.COM

AZ ÖTÖDIK ELEM A VÉDELEM

Hogyan alakítja át a digitális technológia a környezetvédelmet?

Ahogy a világ továbbra is olyan környezeti kihívásokkal küzd, mint az éghajlatváltozás, az erdőirtás és a környezetszennyezés, egyre nagyobb az érdeklődés az iránt, hogy a technológia miként segíthet ezeknek a problémáknak a megoldásában. Az egyik olyan technológia, amely sok figyelmet kap, a mesterséges intelligencia (MI). Körülnéztünk az MI világában, hogy a konkrétumokat is egyenként megdicsérhessük.

Az MI egyik legígéretesebb alkalmazása a környezetvédelemben a környezeti feltételek monitorozása. Az Európai Űrügynökség például mesterséges intelligencia segítségével elemzi a műholdadatokat a városi légszennyezettség szintjének nyomon követésére. A rendszer részletes információkat nyújt a szennyezés forrásairól, ami segíthet a döntéshozóknak célzott stratégiák kidolgozásában.

Egy másik új MI-alkalmazási terület a természeti katasztrófák előrejelzése. A National Oceanic and Atmospheric Administration (NOAA) például mesterséges intelligencia segítségével javítja a hurrikán-előrejelzést. A rendszer elemzi a műholdaktól és érzékelőktől származó adatokat, hogy pontosabb modelleket hozzon létre a hurrikánok viselkedéséről, amelyek segíthetik a vészhelyzeti krízisközpontokat a hurrikánokra való felkészülésben és az azokra való hatékonyabb reagálásban.

Túlcsorduló szemetesek és orvvadászat

A hulladékcsökkentés és az energiafogyasztás optimalizálásának területei is sokat profitálnak az MI egyre gyarapodó képességeiből. Az egyik olyan vállalat, amely a mesterséges intelligenciát a keletkező hulladék mennyiségének csökkentésére használja, a Winnow. A vállalat olyan, mesterséges intelligenciával működő rendszert fejlesztett ki, amellyel a kereskedelmi konyhák akár 50%-kal csökkenthetik az élelmiszer-hulladékot. A rendszer kamerák és mérlegek segítségével követi nyomon a felgyűlő élelmiszer-hulladékot, a mesterségesintelligencia-algoritmusok pedig azonosítják a mintákat, és javaslatokat tesznek a hulladékcsökkentés mikéntjére.

Az írországi University of Limerick tavalyi kutatása egy eddig jelentéktelennek ítélt részterület, a háztartási és kereskedelmi szemetesek túltelt állapotának észlelését célozta MI-vezérelte számítógépes látás segítségével. A jelentéktelenség csak látszólagos, a probléma pedig globális, a túltöltött konténerek átvétele mindenütt túlterheli szemétszállítókat, és a hatékonyság csökkenéséhez vezethet.

A hulladékok kukákba vagy más konténerekbe gyűjtése a hulladékkezelés első lépése, ám ha a kukákat túltöltik, a szemétszállító járművek hulladéktárolóját a gyűjtőút befejezése előtt megtölti a szemét. Ekkor egy második szemétszállítóra lesz szükség, ami magasabb üzemeltetési költségeket és károsanyag-kibocsátást eredményez.

Ma a túltöltött hulladéktároló tartályok állapotrögzítésének folyamata majdnem mindenütt manuális, és szemétszállító kezelőjének minden esetet rögzítenie kell. A kutatók megvizsgálták, hogy a számítógépes látás módszerével automatizálható-e a feladat, az Egyesült Államokban

> Eredményesnek bizonyult az MI a környezetkárosító illegális tevékenységek felderítésében.

gyűjtött, valós útvonalfelvételek felhasználásával. Az eredmények szerint az MI irányította számítógépes látás életképes eszközt jelent az optimalizáláshoz, ami ismételt példa arra, hogy a gépi tanulás és látás milyen váratlan területeken hoz megoldásokat.

Az MI a környezetet károsító illegális tevékenységek, például az erdőirtás és az orvvadászat felderítésére és megelőzésére is kitűnően bevált. A WWF például mesterséges intelligenciát használ a védett területeken folyó állati tevékenység nyomon követésére. A rendszer mesterségesintelligencia-algoritmusok segítségével elemzi a kameracsapdákból és más forrásokból származó adatokat, hogy azonosítsa az illegális tevékenységre utaló mintákat. Ezek az információk felhasználhatók a bűnüldöző szervek és a parkőrök tájékoztatására is, akik így felléphetnek az orvvadászat megelőzése és a veszélyeztetett fajok védelme érdekében.

Szemétalapozó

A Világbank becslései szerint évente globálisan 2,24 milliárd tonna hulladék keletkezik, ami naponta átlagosan 0,79 kilogramm hulladék fejenként. Ez 2050-re várhatóan évi 3,4 milliárd tonnára nő majd. A tanulmányok azt is kimutatták, hogy a hulladékgyűjtés és -szállítás a fejlett országok városi hulladékgazdálkodási költségvetésének 60%-át teheti ki ma, a fejlődő országokban pedig 70% is lehet ez a szám.

Az MI az új statisztikai analitika

A mélytanulási algoritmusok 2010-es megjelenése után exponenciálisan megnőtt az érdeklődés a mesterséges intelligencia eszközeinek környezetvédelmi feladatokra való felhasználása iránt. Az olyan területeken, ahol a mesterséges intelligencia idővel jelentős segítségnek bizonyult, a korábban hagyományos statisztikai és matematikai modellek segítségével megoldott környezetvédelmi feladatok több mint 65 százalékát tudta átvenni az MI a University of Chicago kutatása szerint.

Nyilvánvaló előnyei ellenére a mesterséges intelligencia még mindig a fejlődés korai szakaszában van, és paradox módon környezetvédelmi aggályokat is felvet. Az MI-modellek betanításához szükséges energiafogyasztás és idő nagymértékben befolyásolhatja a számítógépekhez köthető széndioxid-kibocsátást. Jelenleg komoly erőfeszítések folynak olyan MI-technológia kifejlesztésére, amely környezeti szempontból fenntarthatóbb, kisebb az energiafogyasztása, ezért kisebb a CO_2-lábnyoma. Van olyan kutatás, amely szerint a megfelelő MI-modellarchitektúra kiválasztásával az energiafogyasztás közel 90 százalékkal csökkenthető.

Zöld épületek és fenntartható építészet

Az épületek építése és üzemeltetése jelentős hatással van a környezetre. Az MI bevonásával zajló zöld építési gyakorlat fenntarthatóbb építészetet eredményez, ahogy a többihez képest nehézkesebben fejlődő szektor is a digitalizáció útjára lép. A digitális épületinformációs modellezés (BIM) összekapcsolása a 3D-s tervezőprogramokkal és a néhol már robotizáltan működő, szintén MI vezérelte épületelem-gyártó üzemekkel hatalmas energia- és költségmegtakarításokkal járhat, megreformálva egy olyan szektort, amely számos tekintetben még a 20. század közepének örökségét hordozza.

Az olyan technológiák, mint az intelligens ablakok, amelyek a napfény alapján állítják be áttetszőségüket, az energiahatékony szigetelőanyagok, a tetőtéri kertek, vagy az MI által vezérelte, fényviszonyoknak, illetve az időjárásnak megfelelően formát váltó homlokzati elemek beépülnek az épületek tervezésébe az energiafogyasztás csökkentése érdekében. Az MI jelen van és lesz az épületek átadása utáni üzemeltetésben is, főképp az energiafelhasználás optimalizálásában.

Justin Viktor

Az Apple a legprofibb vállalatoknak is elég profi

A világ leginnovatívabb vállalatainak 84%-a jelentős arányban használ Mac-eket. Nem véletlen, hogy azok a szervezetek, ahol a kreativitás, a hatékonyság, az újítások vannak fókuszban, ott a végponti eszközöket is ezeknek a szempontoknak megfelelően választják ki.

Ma már itthon sem kérdés, hogy az Apple-flották aránya folyamatosan növekszik a vállalati szektor minden szegmensében. A nagyvállalatoknál pedig az Apple eszközök támogatása és integrációja is megoldandó feladat. Az IKON Informatika Zrt. nemcsak a beszerzésben, hanem a szakértői támogatásban és a rendszerintegrációban is innovatív partnere a magyar nagyvállalatoknak.

A bankszektorban egyre sürgetőbb felügyeleti elvárás, hogy a pénzintézetek minden végponti eszköze központi menedzsment rendszerbe illeszkedjen. A MacBookokat a legáltalánosabban elterjedt MDM-rendszerek nem kezelik igazán jól, így adódik, hogy a pénzintézeti Macek saját menedzsmentrendszert kapjanak. Ez egyben kiváló lehetőség is a vállalat számára, hogy átgondolja, milyen munkaeszközöket biztosít a munkavállalóknak, és felmerül a szabad platformválasztás kialakításának a lehetősége is.

Az Mac- és iPhone-felhasználók kevesebb támogatást igényelnek, jobban vigyáznak az eszközeikre, és tovább is használják azokat.

Ma már találgatni sem kell, milyen hatása lenne egy ilyen döntésnek, vannak erre nemzetközi példák: a Cisco központjában már évekkel ezelőtt bebizonyosodott, hogy ha a munkavállalók ugyanolyan támogatást kapnak, és így szabadon választhatnak, hogy Apple vagy Windows-alapú eszközökön dolgozzanak, a munkavállalók kb. 60%-a választott inkább MacBookot. A megdöbbentő az, hogy ezek a kollégák végül kevesebb támogatást igényelnek, jobban vigyáznak az eszközeikre és tovább használják azokat, mint a más márkák mellett maradók.

FORRÁS: IKON INFORMATIKA

Ahhoz, hogy az Apple ökoszisztémában rejlő lehetőségeket valóban kiaknázza egy vállalat, érdemes jobban is elmélyedni abban, hogy mire képesek az Apple hardverei és szoftverei együttesen. Az új funkciók egy részét intuitív módon is használni kezdik a felhasználók, pont ezek miatt igényelnék sokszor a magánhasználatban már megszokott minőségű iPhone-t vagy MacBookot a munkahelyen is. De ennél több is van az Apple ökoszisztémában, ahogy a Volvo esete is mutatja.

Apple Hivatalos Viszonteladóként az IKON az elmúlt időben azt tapasztalta, hogy a legprofibb hazai vállalatokban mindenhol konkrét tervek és projektek vannak már az Apple eszközök bevonására, a flották bővítésére, az optimális MDM-rendszerek bevezetésére. Izgalmas projekteken dolgozunk, amelyek itthon is az Apple legfrissebb innovációit állítják a hatékonyságnövelés szolgálatába.

Ez remek lehetőség a tehetségek megtartására, a munkavállalói elégedettség növelésére kialakított HR-stratégiákba is illeszkedik, és kiválóan támogatja a fenntarthatósági célokat, tekintve, hogy az iPhone 15 és az Apple Watch-ok gyártása például a piacon egyedülálló mértékben karbonsemleges. Így akik számára a fenntarthatóság nem csak szlogen, érdemi lépést tudnak tenni „zöld” irányba azzal, ha növelik az újabb Apple-modellek arányát a vállalati eszközparkban.

Az pedig szinte közhely, hogy az adatbiztonság szempontjából minden IT-biztonsági vezető csak helyeselni szokta az Apple eszközök használatát. ■

A Volvo esete az Apple-lel

A Volvo a szervizhálózatában a vásárlói élmény javítása érdekében az autószerelők iPhone-jaira tervezett mobilapplikációt fejleszteni, amikor azonban felmérték az igényeket, felfedezték, hogy ennél jobb lehetőség is kínálkozik. Mivel a szerelő munkatársak keze gyakran foglalt, a telefonra érkező értesítések nem jutnak el hozzájuk elég gyorsan, pedig a legfőbb cél pontosan a gyors reagálás lett volna. Végül az Apple Watch bevonása lett a megoldás, amivel a megfelelő információ úgy jut el a munkatársakhoz, hogy nem is kell a szerszámot letenniük a kezükből vagy elővenni a telefonjukat. Végül a Volvónak nem kellett a szerelőket sem noszogatniuk, maguk kérték, hogy átállhassanak, és az Apple Watch-ra érkező prompt jelzések irányítsák a munkavégzésüket.

FORRÁS: HUNGAROCONTROL

IT-SZAKEMBEREKET ÉS MÉRNÖKÖKET TOBOROZ A HUNGAROCONTROL

Lépj be a repülés világába!

A HungaroControl Zrt., hazánk egyetlen légiforgalmi szolgáltatója, új munkatársakat toboroz IT- és mérnöki pozíciókba. A repülés iránt is érdeklődő szakembereknek most kivételes lehetőségük van arra, hogy csatlakozzanak egy nemzetközi hírű, stabil hátterű, a repülés világában tevékenykedő vállalathoz.

A légi közlekedés egyedülálló és dinamikus iparág, amely a legkorszerűbb technológiákra épül, így számtalan szakmai kihívást és fejlődési lehetőséget kínál a műszaki és IT-területek iránt érdeklődő munkavállalóknak. A HungaroControl a hazai légiforgalmi ágazat egyik zászlóshajója, amely óriási hangsúlyt fektet az innovációra és a kutatás-fejlesztésre. A hatékony és minőségi szolgáltatás nyújtása, valamint a magasabb szintű repülésbiztonság elérése érdekében pedig erősen ösztönzi a legmodernebb technológiai vívmányok alkalmazását. A társaság működését határainkon túlmutató elismertség övezi, kimagasló eredményei pedig nemzetközi összehasonlításban is figyelemreméltók.

Az IT- és műszaki területeken dolgozó munkatársak fontos szerepet játszanak abban, hogy a légiforgalom zavartalanul és biztonságosan áramoljon hazánk légterében, ezért olyan szakértőket keresnek, akik elkötelezettek a legmagasabb szintű szakmai teljesítmény iránt. IT-szakembereik a légiforgalmi irányítás legkorszerűbb informatikai rendszereit működtetik, míg mérnökeik egy rendkívül összetett és modern légi-navigációs infrastruktúrát üzemeltetnek és fejlesztenek.

A HungaroControlnál való munkavégzés nem csupán egy állás, hanem hivatás és életforma is. A vállalatnál dolgozó szakemberek nemzetközi környezetben dolgoznak, és rendkívül sokszínű projektekben vesznek részt, amelyek folyamatosan szolgálják a szakmai fejlődésüket. Nagy hangsúlyt fektetnek a közösségépítésre és az inspiráló munkakörnyezetet megteremtésére, ami az együttműködésre és az elhivatottságra épül, valamint díjazza a tehetséget és az elkötelezettséget.

Ha tehát IT- vagy mérnöki háttérrel rendelkezel, motivált és nyitott vagy az új szakmai kihívások iránt, akkor a HungaroControlnál a helyed!

Légy része egy dinamikusan fejlődő iparágnak, izgalmas projekteken keresztül ismerd meg a repülés világát! Fontos hangsúlyozni, hogy a vállalat hosszú távú perspektívában gondolkodik, így a munkatársakkal is a hosszú távú együttműködésre törekszik, ezért a szakmai fejlődés nálunk nemcsak lehetőség, hanem elvárás is. ■

Ne csak álmodj, váltsd is valóra az álmaidat, hiszen a repülés világa mostantól a te világod is lehet! Ne habozz tovább, legyen a HungaroControl a következő lépés a karrieredben, járulj te is hozzá a hazai légiforgalmi szektor fejlődéséhez és biztonságának növeléséhez. Látogass el a társaság karrieroldalára, ahol részletes információkat találsz az aktuális nyitott pozíciókról.
Válogass a különböző IT-s és mérnöki területeken elérhető állások között, és lépj be a repülés világába!

HungaroControl

FORRÁS: FREEPIK.COM

AZ ADATOK KINCSESBÁNYÁI

Kiber-össztűz alatt az egyetemek

Kevesen gondolnak bele abba, hogy a felsőoktatási intézmények adott esetben több százezer személyes adattal dolgoznak, amelyek védelme egyre komolyabb felkészültséget követel a szakemberektől. *Fekete Csaba,* a Szegedi Tudományegyetem Informatikai és Szolgáltatási Igazgatóság igazgatója úgy véli: a felsőoktatási intézményeknek egyre nagyobb figyelmet kell fordítani a kibervédelemre, ugyanis tapasztalataik szerint növekvő számú támadással kénytelenek szembesülni napról napra. Ráadásul, ezek nem kizárólag kívülről érkeznek.

„Az egyetemek, így a Szegedi Tudományegyetem fenyegetettségét leginkább az okozza, hogy sok belső ügyfelünk van, és ők rendkívül összetett tevékenységet végeznek”, bocsátotta előre *Fekete Csaba.* „Nyilván, van egy oktatói, illetve egy hallgatói kör, több tízezer diákról beszélünk, akik használják a szolgáltatásainkat, és nemcsak vállalati hálózaton belülről, hanem kívülről is, a nyílt internet irányából. Ez számunkra annyiban nehézség, hogy a nyílt internet felől érkező normál felhasználók közül valahogy ki kell szűrnünk a támadó szándékkal érkezőket. Ez nagyon nehéz, erre különösen oda kell figyelnünk, amikor a védelmi rendszereinket kialakítjuk”, tette hozzá.

Az elmúlt időszakban a minden egyetemi hallgató által napi szinten használt, országos Neptun-rendszert érintően számos olyan támadást tapasztaltak, amely több intézményben komoly károkat és jelentős veszteségeket okoztak, vagy adatvédelmi incidens alakult ki miattuk.

„A levelezőrendszereinket több tízezer felhasználó használja, és gyakran, szinte naponta tapasztalunk adathalász-kísérleteket, de ezeket eddig sikerült időben blokkolnunk”, számolt be a szakember. „Nehéz lépést tartani a támadókkal, de megpróbáljuk, mert kiemelten fontos számunkra az ügyfeleink bizalma. Napi tevékenységünk során rendkívül sok személyes adatot kezelünk. Jelen vagyunk az oktatás minden szintjén, továbbá van egy klinikánk, oktatunk, kutatunk és gyógyítunk is, ezért kiemelt feladatunk, hogy szofisztikált, többrétegű védelmi rendszert alakítsunk, működtessünk és fejlesszünk. Többféle gyártó védelmi technológiáját és többféle módszert, eljárást használunk annak reményében, hogy sikerül a támadások minél szélesebb spektrumát elhárítani. Ezidáig működőképes ez a megoldás”, mondta el Fekete Csaba.

A nyíltság kockázatokkal jár

Információbiztonsági szempontból a nagyobb egyetemek, így az ELTE kitettsége is magas. Az ilyen intézmények mérete és összetettsége, jó hálózati ellátottsága és a szükségszerűen decentralizált – például kutatók által működtetett – szolgáltatási környezet, valamint az a körülmény, hogy egy tudományegyetemen nem lehet olyan zárt és hierarchikus biztonsági környezetet kialakítani, mint például egy bankban, vonzza a támadásokat és a rosszindulatú próbálkozásokat.

Ritter Dávid, az ELTE informatikai igazgatója érdeklődésünkre elmondta: „A védekezés az intézmények jellegének megfelelően decentralizált, ami különböző módon és mértékben jelenik meg az egyes szolgáltatási területeken. Egyes, az intézmény működése szempontjából kritikus környezetek összetettebb, kevésbé kritikus szolgáltatások alacsonyabb szintű központi védelmet kapnak. Ettől még egy adott szolgáltatás védelme és biztonsága helyi eszközökkel igen magas szinten is megvalósítható”.

FORRÁS: SZTE

FEKETE CSABA, SZEGEDI TUDOMÁNYEGYETEM

FORRÁS: BRANDHUBER GYÖRGY

RITTER DÁVID, ELTE

„A központi menedzsment részeként biztosított védelmi szolgáltatások főbb jellemzői közül talán az a legfontosabb, amit már említettem is, hogy az ELTE teljes informatikai környezete decentralizált. Ennek részben történeti okai vannak, de a több központú kialakítás miatt nincs olyan forgatókönyv, ami valamennyi, működés szempontjából fontos rendszer leállásával járna”, fedte föl Ritter Dávid.

Tudományegyetemi részletek

A tűzfalak egyrészt a belső hálózatot, másrészt az egyes kritikus szolgáltatásokat védik. Klasszikus csomagszűréses funkcionalitás mellett egyes esetekben állapot szerinti szűrést is alkalmaznak. Bizonyos kritikus szolgáltatási környezetben alkalmazásszintű tűzfalmegoldásokat működtetünk. A tűzfalak védelmet nyújtanak a túlterheléses (DDoS-) támadások ellen is. „Fontosnak tartom megemlíteni a végponti védelmi szolgáltatásokat, ami központi felügyeletbe vont munkaállomásokat és laptopokat jelent. Az eszközök jelentős része olyan központi menedzsmentben van, amely lehetőséget ad az operációs rendszer, a védelmi és felhasználói szoftverek naprakészen tartására, a nem kívánt szoftverek telepítésének megakadályozására”, hangsúlyozta az informatikai igazgató.

Az igazgató a védelmi szolgáltatások sorában megemlítette még a monitoring eszközöket. Mint rámutatott: a hálózat és a főbb szolgáltatások működése folyamatos megfigyelés alatt áll. A rendellenes működést és aktivitásokat nemcsak üzembiztonsági, hanem védelmi szempontból is kiértékelik, vannak ilyen jellegű riasztások és beavatkozási lehetőségek is.

„Egyes szolgáltatásainknál a felhasználók viselkedésének elemzésére is képesek vagyunk a rendellenességek felfedése, illetve a problémák előrejelzésére is”, mondta el Ritter Dávid. „Ezzel adott esetben proaktívan, a tényleges káros aktivitást megelőzően be tudunk avatkozni. Végezetül hadd ejtsek szót a policy jellegű intézkedéseinkről is: egyes rendszereink csak dedikált gépről vagy hálózatról érhetők el és bizonyos jogosultsági szintekhez megköveteljük a VPN használatát”, jelezte az informatikai igazgató.

Az adminisztrátorok, rendszergazdák minden esetben csak dedikált gépről vagy hálózatból, titkosított kommunikációs csatornán tudnak bejelentkezni. A főbb szolgáltatások eléréséhez minden felhasználó számára kétfaktoros autentikációra van szükség, ebben az ELTE élen jár a hazai felsőoktatásban. A szolgáltatások többsége részletesen naplóz, így az esetleges incidensek után van lehetőség elemzésre, illetve a felelősségek elhatárolására.

Horváth Attila

IP audió rendszerek a kapuk előtt

Az elmúlt években sokat foglalkoztunk azzal, hogy az IT/IP technológia hogyan hódította meg a videó rendszerek piacát, mára szinte teljesen kiszorítva onnan az analóg megoldásokat. Mindeközben az utóbbi években – talán a videónál kevésbé látványos módon – az audió rendszerek is elindultak ezen az úton és mára kiforrott és az analóg megoldásoknál már most sokkal több szolgáltatással bíró, rugalmasabb kialakítású rendszerek hozhatók létre, amelyek ráadásul könnyedén integrálhatók. A technológia fejlesztésében – akárcsak a videó esetében – a svéd Axis Communications ezúttal is az élen jár, így a megoldásain keresztül kiválóan bemutatható az, hol tart ma ez a technológia.

A technológia

A legelterjedtebb hagyományos analóg hangrendszerek 100 V-os hálózatot használnak a hangszórók meghajtására. Erre a feszültségre azért van szükség, hogy viszonylag kis átmérőjű kábeleket lehessen használni és a veszteség is kisebb így. A hangszórókat párhuzamosan kötik rá egy központi erősítő kimenetére. Az egy kimenetre rákötött hangszórók számát az erősítő teljesítménye határozza meg az egyes hangszórók teljesítményigényének függvényében. A rendszer bemenetén lehet mikrofon, CD lejátszó, rádió, lényegében bármilyen eszköz, amely audió kimenettel rendelkezik. A bemenő jeleket egy keverőn keresztül vezetik az erősítő bemenetére, ezzel tudjuk szabályozni, hogy melyik hangforrás milyen arányban szóljon. A központi berendezések helyet foglalnak, energiát fogyasztanak, a nagyobbak esetleg még hűtést is igényelnek, szóval a fenntartásuk is jelentős költségeket emészt fel. Ezeket a hagyományos hangrendszereket elsősorban olyan klasszikus hangosítási feladatokra használják, mint például tömegközlekedési állomások, bevásárlóközpontok, iskolák, vagy éppen stadionok hangosítása. Fontos megemlíteni, hogy az alkalmazott technológia egyben le is korlátozza azt a területet, amelyet ki tud szolgálni egy ilyen rendszer.

Ezzel szemben egy IP alapú hangrendszerhez nem szükséges központi hardver, a rendszer az önállóan működő aktív hangszórókból, egy központi vezérlő szoftverből és néhány kiegészítő elemből – pl. audio bridge, mikrofon, stb. – áll. A lényeg, hogy az „intelligencia” a hangszórókban van, hiszen ezek közvetlenül IP hálózatra csatlakozó, erősítőt, sőt mikrofont is tartalmazó aktív egységek, beépített web szerverrel, lényegében mindegyik önálló működésre képes. Mivel a tápellátást is az Ethernet kábelen keresztül kapják a PoE technológia használatának köszönhetően, így máris megvan az egyik előnye, nevezetesen, hogy nem szükséges külön hálózatot kiépíteni, egyszerűen integrálható az épület strukturált hálózatába. Ugyanezen okból a hangrendszer bővítése is rendkívül egyszerű, csak ki kell húzni egy UTP kábelt a hangszóró helyéhez legközelebbi rendezőig, csatlakoztatni egy PoE switch-hez és máris működőképes a hangszóró. A hangszórók bel- és kültéri változatban egyaránt elérhetők, találunk a kínálatban álmennyezetbe építhető, különálló, vagy éppen

FORRÁS: ASPECTIS

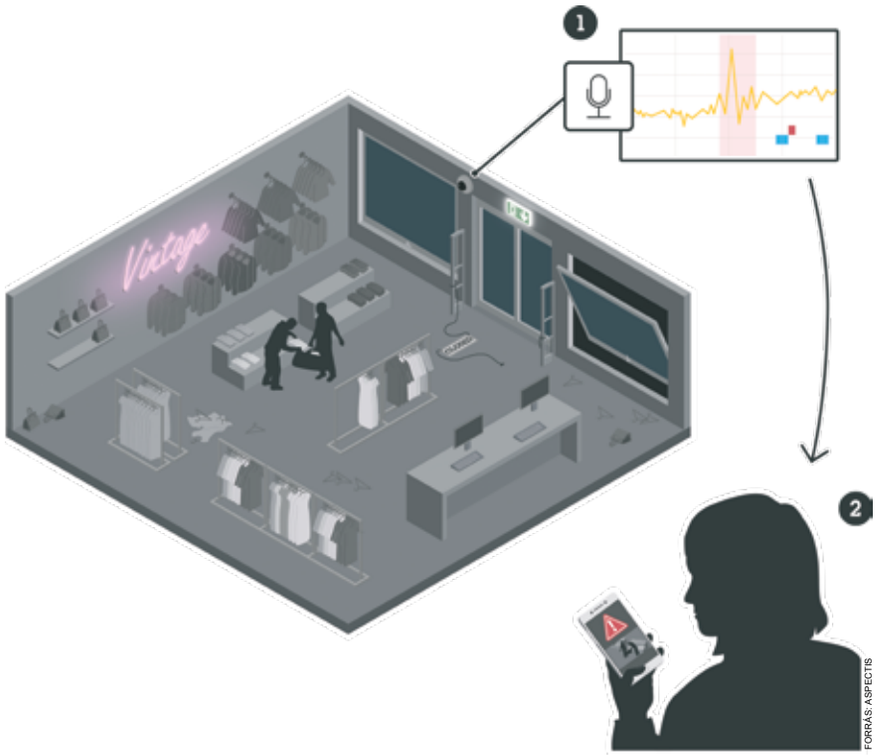
kültéri, tölcséres változatot is. A kristálytiszta hangzásról a beépített DSP (Digital Signal Processing) áramkörök gondoskodnak. Egyes hangszórók SD kártyákat is tudnak fogadni, melyen audió tartalmak tárolhatók (pl. standard figyelmeztetések) és onnan bármikor időzítve, vagy teljesen szabadon lejátszhatók. Annak sincs akadálya, hogy meglévő analóg hangszórókat integráljunk a rendszerbe, erre a hálózati audió erősítőt tudjuk használni.

A rendszer lelke

Azonban bármennyire is okosak a hangszórók, szükség van egy vezérlőre, amelynek segítségével meghatározhatjuk, hogy hol mi, milyen hangerővel, időzítéssel szóljon. Ebben az esetben ez a vezérlő nem más, mint egy szoftver, az Axis Audio Manager, melynek segítségével épp úgy vezérelhetjük az egyszerű, egy épületen belül működő audió rendszereket csakúgy, mint a több telephelyes, akár kontinenseken is átívelő világméretű kiterjedésűeket. Ez máris egy óriási előny az analóg rendszerekhez képest, hiszen azokkal ilyen léptékben nem tudunk gondolkodni. Az Axis Audio Manager – a hangszórókkal együttműködve – ráadásul egy igen hatékony hibafeltárásra is lehetőséget biztosít. A hangszórókba beépített mikrofon segítségével ugyanis állandóan monitorozható, hogy szól-e a hangszóró, hiba esetén a szoftver azonnal jelzi a kezelőnek a hibás berendezést, aki intézkedni tud a meghibásodott eszköz javításáról, vagy cseréjéről. Ráadásul itt egy eszköz hibája nincs hatással a rendszer többi részének működésére, míg egy analóg rendszernél egy esetleges zárlat teljes szegmensek kiesését okozhatja, ráadásul még a hibakeresés is hosszú ideig tarthat, megbénítva addig a működést. Az Axis Audio Manager (AAM) nagyon jól skálázható, a legkisebb 200 hangszórót és 20 zónát kezelő AAM Edge változattól a több ezer helyszínt menedzselni képes AAM Center változatig. Az AAM Edge ráadásul még külön hardware-t sem igényel, ugyanis minden Axis audió eszközön előre telepítve várja a felhasználóját, csak aktiválni kell amennyiben szükséges. Nézzük, milyen egyéb szolgáltatásai vannak még az AAM-nek. Tetszőlegesen keverhetjük és időzíthetjük a rögzített figyelmeztetéseket az élőkkel, szolgáltathatunk háttér zenét, vagy közvetíthetünk hirdetéseket. A zónák kialakítása is nagyon rugalmas, hiszen akár egy hangszóró is alkothat egy zónát, vagy akár több tucat is, és bármikor át is csoportosíthatjuk azokat. Ez szintén egy olyan előny, amivel az analóg rendszerek nem vehetik fel a versenyt. A hangszórók hangerejét akár hangszórónként is tudjuk szabályozni. Az audió tartalmakat könnyen időzíthetjük akár az időeltolódás figyelembe vételével is.

Integráció, tervezés

Napjainkban egyre fontosabb szemponttá válik, hogy az általunk használt rendszerek ne szigetszerűen működjenek egymás mellett, hanem egymást támogatva, információkat cserélve akár közös felületet nyújtva



segítsék a munkánkat. Egy analóg hangrendszer vajmi kevés lehetőséget biztosít bármilyen integrációra, ezzel szemben az Axis Audio rendszere tálcán kínálja a lehetőségeket. Szeretnénk például, hogy egy kamera által észlelt gyanús cselekmény kiváltson egy hangbemondásos riasztást, vagy szeretnénk váltani a háttérzene forrásán? Szeretnénk a PTZ kameránkat automatikusan a hang forrása felé irányítani? Esetleg a telefonunkat szeretnénk mikrofonnak használni? Semmi akadálya! Az Axis nyílt platformja erre és sok egyéb szolgáltatásra biztosítja a lehetőséget.

Ahhoz, hogy bármilyen rendszer jól szolgálja a használóit, elengedhetetlen a gondos tervezés. Különösen fontos a megfelelő hangszórók elhelyezése a megfelelő helyekre. Ehhez igénybe vehetjük az Axis Design Tool-t, de letölthetünk sémákat a Microsoft Visio és az EASE Evac tervező eszközökhöz egyaránt.

Alkalmazási területek

Az egyik fontos terület, ahol a hálózati audió rendszerek teret hódíthatnak a közeljövőben, az a videó megfigyelő rendszerek kiegészítése és hatékonyabbá tétele. Az olyan esetekben, amikor a videó rendszer valami gyanúsat észlel a beépített analitikáinak segítségével, vagy éppen az operátor vesz észre valamit, az elkövetőt egy határozott hangüzenettel eltántoríthatja attól, hogy folytassa a cselekményt. A hangszórókba vagy a kamerákba épített mikrofonok pedig riasztásokat generálhatnak nem szokványos hanghatások (pl. lövés, robbantás, autók ütközése, stb.) esetén.

Az épületek, bevásárlóközpontok, tömegközlekedési állomások, vagy akár városi terek hangosítása is igen izgalmas feladat. Itt már előjönnek olyan problémák, mint a visszhang vagy az érthetőség kérdése, de az IP audió eszközök ezekkel is megbirkóznak.

Összefoglalás

Bátran állíthatjuk, hogy az IP alapú audió rendszerek elkezdték hódító útjukat, és vélhetően hamarosan kiszorítják analóg társaikat. Ebben a folyamatban az Axis már ma is érett megoldásokkal lépett a színre, a legtöbb alkalmazás esetében jobb megoldást kínál analóg társainál, és mivel a szolgáltatásokat szoftveres megoldások jelentik, az ilyen rendszerek könnyen fejleszthetők. ■

ASPECTIS
DISTRIBUTION • SERVICES

SZEMFÉNYVESZTÉS

Idén már nemcsak a látszat csal, de a látvány is

Tavaly indult a generatív mesterséges intelligencia gyártotta videók forradalma, de idén érkezik majd meg igazán az életünkbe. Ebben az évben több mint 60 választás lesz, köztük az előttünk álló, rendkívül komoly tétet jelentő EU-s és USA-beli választások. A tömegpiacra szinte korlátok és szabályozás nélkül ömlő, csúcstechnológiás MI-szoftverszolgáltatásokat elnézve az AGI (az általános, embernél is okosabb mesterséges intelligencia) jóistene irgalmazzon nekünk.

A szöveget videóvá alakítani képes modellek első generációja 2022 végén jelent meg, olyan cégek szállították, mint a Meta, a Google és a Runway videótechnológiai startup. Ügyes trükköket tudtak, de az eredmények szemcsések, hibásak és mindössze néhány másodpercesek voltak. Tekerjünk gyorsan 18 hónapot előre az időgépen, és itt az OpenAI „Sora" nevű videógenerátora nagy felbontású, fotórealisztikus filmekkel, amelyek legjobbjai olyan lenyűgözőek, hogy egyes „szakértők" egyenesen Hollywood halálát jósolják. A Runway legújabb modelljei is képesek már olyan spotokat készíteni, amelyek vetekszenek a blockbuster animációs stúdiók által készített klipekkel. A Midjourney és a Stability

FORRÁS: DALL·E 3 – JUSTIN VIKTOR

AI, a két legnépszerűbb szöveg-kép modell mögött álló cég már szintén dolgozik a videógeneráláson is, ez hamarosan megérkezhet a szolgáltatásaikba.

Számos vállalat áll sorban egymást taposva, hogy üzletet csináljanak ezekből a technológiai áttörésekből, és az elmúlt MI-dominálta évhez hasonlóan eluralkodott lázas hangulat szerint most sem igazán számít, mi is ez az üzlet konkrétan, azt majd menet közben kitalálják. „Rendszeresen kiabálok önkéntelenül, hogy mennyire menő ez az egész, miközben ezekkel az eszközökkel játszom”, mondta *Gary Lipkowitz,* a Vyond vezérigazgatója, akinek cége point-and-click platformot kínál rövid, animációs videók összeállításához.

De mire lehet ezt felhasználni egy munkahelyen? Bármi is lesz a válasz a kérdésre, valószínűleg a vállalkozások széles körét fogja felforgatni, és sok szakember szerepét, munkakörét fogja megváltoztatni az animátoroktól a hirdetőkig. Természetesen a visszaélésekkel kapcsolatos félelmek is nőnek, a deepfake vagyis hamis videók készítésének széles körű elterjedése ugyanis minden eddiginél könnyebbé teszi, hogy az internetet elárasszák politikai propagandával és a szereplők hozzájárulása nélkül készített pornóval. Ez már nem a jövő, hanem a jelen, és a rossz hír az, hogy senki sem tudja igazán a megoldást a problémákra.

Versenytársak hosszú sora

Bár az OpenAI Sora jelenleg messze a versenytársak felett áll, más cégek is keményen dolgoznak a felzárkózáson. A brit székhelyű, Haiper nevű startup márciusban lépett elő a homályból. A céget 2021-ben alapították a Google DeepMind és a TikTok korábbi kutatói, akik a neurális sugárzási mezőknek (NeRF-nek) nevezett technológián dolgoztak, amely képes 2D-s képeket 3D-s virtuális környezetté alakítani. Kezdetben úgy gondolták, hogy az állóképeket a felhasználó által bejárható jelenetekké alakító eszköz hasznos lehet például a videójátékok készítésénél. Fél éve azonban a Haiper a virtuális környezetekről átállt a videóklipekre, és a technológiát is úgy alakította át, hogy megfeleljen egy olyan új elképzelésnek, amely *Yishu Miao* vezérigazgató szerint a játékoknál is nagyobb piac lesz. „Rájöttünk, hogy a videógenerálás az igazi piaci rés. Hatalmas kereslet lesz rá!”, mondta.

Akárcsak az OpenAI Sora, a Haiper generatív videótechnológiája is diffúziós modellt használ a vizuális elemek kezeléséhez, és egy transzformátort, hogy a képkockák közötti konzisztenciát kezelje. Ez a nagy nyelvi modellekben, például a GPT-4-ben is megtalálható komponens, amely felruházza azzal a képességgel, hogy megjósolja, mi is következik. A videók is csak puszta adatsorozatok, és a transzformátorok a legjobb ismert modellt jelentik az adatsorozatok megtanulására. A videógeneráláshoz használt transzformátorok növelhetik a klipek minőségét és hosszát, hátrányuk viszont, hogy ki is találnak dolgokat, vagyis „hallucinálnak”. A szövegben ez nem mindig nyilvánvaló, videóknál viszont azt eredményezheti, hogy egy személynek több feje lesz.

A transzformátorok helyes működtetéséhez ma hatalmas képzési adattárolókra és számítógépekkel teli szervertermekre van szükség, ezért az Irreverent Labs – amelyet a Microsoft korábbi kutatói alapítottak – más megközelítést alkalmaz: transzformátor helyett egy diffúziós modellt kombinál egy olyannal, amely a józan ésszel elvárható fizika alapján megjósolja, mi lesz a következő képkocka, például hogyan pattan le egy labda a falról, vagy hogyan fröccsen szét a víz a padlón. Ez a megközelítés csökkenti a képzési költségeket, és a hallucinációk számát is.

FORRÁS: OPENAI

EGY KÉPKOCKA A SORA ÁLTAL GENERÁLT 4K-S KLIPBŐL

A modell még mindig produkál hibákat, de ezek már csak a fizika apró torzulásai – például egy pattogó labda pályaívének alakja, amelyet ismert matematikai módszerekkel ki lehet javítani a videóban a generálás után.

A filmek titkos élete

A videó az internet médiuma: YouTube, TikTok, híradók, hirdetések, mindenütt találkozhatunk már szintetikus videókkal, a marketingipar pedig a generatív technológia egyik leglelkesebb alkalmazója. Az Adobe az Egyesült Államokban nemrégiben végzett felmérése szerint a marketingszakemberek kétharmada kísérletezett már generatív mesterséges intelligenciával a munkája során, és több mint a fele mondta azt, hogy használta már a technológiát képek előállítására is.

A „Somme Requiem” című 2,5 perces rövidfilmet a Los Angeles-i Myles produkciós cég készítette a Runway Gen 2 modellel, a kisebb klipeket pedig egy videószerkesztő csapat vágta össze. A kisfilm az I. világháború 1914-es karácsonyi tűzszünetének idején hólepte katonákat ábrázol több tucat különböző felvételen, melyeket a Myles emberi videószerkesztői színkorrigáltak, vágtak és zenét is tettek a kész kisfilm alá.

„A történetmesélés közeljövője ilyen hibrid munkafolyamat lesz”, mondta *Josh Kahn,* a Myles vezérigazgatója. Az Apple TV+ „Masters of the Air” című, második világháborús repülőkről szóló sorozata ugyanis nem kevesebb, mint 250 millió dollárba került. De említhetnénk *Peter Jackson* „They Shall Not Grow Old” című I. világháborús dokumentumfilmjét is, amelyet négy éven át készítettek több mint 100 órányi archív filmanyagot restaurálva.

A legtöbb filmkészítő a horribilis költségek miatt eddig csak álmodhatott arról, hogy valaha is lehetősége lesz egy ilyen műfajú történetet elmesélni. „Eddig!”, igazította a helyére a perspektívát Kahn. A horrorfilm műfaja az, ahol a filmrendezők klasszikusan új dolgokat tesztelnek, új dolgokat próbálnak ki, vagyis valószínűleg hamarosan jön majd egy olyan újszerű horrorfilm, melyet maximum négy ember készített valahol egy pincében, a mesterséges intelligencia segítségével, vélekedett a rendező.

Mit is lehet ehhez hozzátenni? Remélhetőleg nem politikai horror lesz.

Justin Viktor

Digitalizáció biztonságosan

Az ipari informatikai rendszerek védelme különösen hehéz feladatot jelenthet, a hirtelen megnőtt kitettség és a NIS2 miatt ugyanis számos ipari cégnek nagyot kell lépnie előre a biztonságos működés felé. A kancellar.hu az informatikai biztonság szakértőjeként több mint két évtizedes tanácsadói tapasztalatával segíti ügyfeleit a hiányosságok és a lehetőségek feltérképezésében.

Magyarországon felgyorsult az ipari digitalizáció, egyre szélesebb körben terjednek az Ipar 4.0 megoldások. Kiváló rendszerek születnek arra, hogy a gyártósorokról származó adatokat begyűjtsék és elemezzék. A legtöbb esetben viszont fel sem merül, hogy a megoldások IT biztonságával is foglalkozzanak, csak akkor, amikor már késő.

Óriási károk

Az ipari vállalatok gondolkodásmódjába még nem épült be olyan mértékben az IT-biztonság, mint más, a digitalizációban előrébb járó szektoroknál. A gyártósorok már nem alkotnak elkülönülő szigeteket, az üzemi terület és annak rendszerei állandó kapcsolatban állnak az irodai rendszerekkel, a gyártástervezéssel, a megrendeléssel és a logisztikával.

Az ipari cégek kiváló célpontot nyújtanak a kiberbűnözők számára, hiszen néhány órás termeléskiesés is óriási károkat tud okozni, és ez nem kizárólag a gyártósor kompromittálásából fakadhat. A kancellar.hu tapasztalatai alapján egy tipikus magyar kkv esetében naponta 50-300 millió forintot is elérheti a leállásból fakadó kár összege. A nem elfogadható károk költséghatékonyan elkerülhetők, ha megfelelő szakértelemmel egy zárt, teljes körű, folytonos és a kockázatokkal arányos védelem kerül kialakításra. A kancellar.hu az ilyen védelem megtervezéséhez, kialakításához, fenntartásához kínál komplex megoldásokat.

Két bástya ugyanazon a várfalon

Nem könnyíti meg az ipari rendszerek védelmét az sem, ha nincs független IT-biztonsági terület, az IT- és az OT-csapat gyakran nem érti meg egymást. „Azt kellene felismerniük, hogy mind a ketten ugyanazon a várfalon állnak, ugyanazt a várat védik, csak két külön bástyán küzdve. Nem egymás ellen kellene védekezniük, hanem egy egységként a várat ostromlók ellen, mert a működés hosszú távon csak így tartható fenn”, figyelmeztet *Sík Dávid,* a kancellar.hu governance csapatának vezetője.

A NIS2 most olyan vállalatoknál is reflektorfénybe helyezi az IT-biztonságot, ahol eddig kevés figyelmet fordítottak arra, azonban a digitalizáció és a kitettség növekedése miatt szükségszerűvé vált. Sík Dávid szerint komoly felvilágosító munkára van szükség. Sokan csak a jogszabályt látják, és annak IT-biztonsági okát nem ismerik, ezért gyakori az a vezetői megközelítés, amely csak látszatintézkedésekkel akar megfelelni az előírásoknak.

Kell néhány év

Sok esetben a helyi informatikai szervezet szorul segítségre: látják a biztonsági problémákat, de nem tudják meggyőzni a vezetést a kellő szintű védekezés szükségességéről. „Ahogy eddig is, ma is 27 percet kérünk arra, hogy bemutatkozzunk a vezetőknek. Ilyenkor egyfajta tudatosító munkát is végzünk. Meglátásom szerint legalább 3-5 év, mire a NIS2 előírásai ténylegesen beérnek abban az értelemben, hogy a biztonságról való gondolkodás bekerül a mindennapi informatikusi köztudatba, és a jelenlegi szakemberhiány valamelyest mérséklődik. Ugyanez volt a helyzet a GDPR esetében: most, évek múltán jutottunk el oda, hogy a legtöbb vállalatnál ténylegesen odafigyelnek az adatvédelemre”, teszi még hozzá Sík Dávid.

FORRÁS: KANCELLAR.HU

SÍK DÁVID, KANCELLAR.HU

„Amennyiben a szolgáltatásaink felkeltették az érdeklődését, kérjük szánjon 27 percet egy személyes beszélgetésre.” kancellar.hu

kancellar.hu
AZ INFORMATIKAI BIZTONSÁG SZAKÉRTŐJE

MINDEN VÁLTOZIK, A TANANYAG IS

Szuperaktuális oktatás egy szuperaktuális témáról

Nem egyszerű, de nem is lehetetlen a mesterséges intelligenciára alapozott szoftverfejlesztői eszközök használatának képzése. Az MI rohamos sebességgel fejlődik, így ennek megfelelően gyakorlatilag tanfolyamról tanfolyamra változik az ITware által kidolgozott és használt tananyag is. Ez rengeteg munkát jelent az AI4DEV csapatának, de rengeteg eredményt is ad.

A szoftverfejlesztők is naponta találkoznak a MI-ról szóló hírekkel. De a mindig sürgős napi munka mellett nehézséget okoz az új eszközök beépítése a fejlesztés folyamatába. Az AI4DEV ezen segít, az ITware tapasztalatai szerint.

„Nem csak a kifejezetten szoftverfejlesztéssel foglalkozó cégeknek fontos, hogy használni tudják a mesterséges intelligencia technológiai újításait", emelte ki *Dankó Sándor,* az ITware Kft. ügyvezetője. Ezt azonban a vállalkozások felső vezetőinek kell felismerniük, és azt is, hogy az MI-alapú eszközök bevezetésével és használatával jelentős előnyökre lehet szert tenni.

Méghozzá olyan területen is. ahol nem is gondolnánk, tette hozzá *Hajtós Bertalan,* a cég sales managere. Ma már egyre inkább előtérbe kerül a wellbeing, a kollegák jóllétének kérdése. Az új módszereket, eszközöket megtanuló, így munkáját eredményesebbé és hatékonyabbá varázsló, a repetitív „favágó" munkát az MI-nek átadó fejlesztő lesz a boldog fejlesztő. Ráadásul a tapasztalat szerint az új tudással felvértezve gyakran azoknak a problémáknak, elakadásoknak a megoldása is új lendületet kap, amelyeket korábban már „félreraktak". Így egy-egy vállalkozás esetében további működési vagy növekedési potenciál szabadítható fel.

Ehhez azonban az is szükséges, hogy az eredményorientált képzéssel sikerüljön egységes tudásszintre hozni egy fejlesztői csapatot. „Egyenszilárdságú tudást szeretnénk kialakítani még akkor is, ha különféle platformokon vagy környezetekben fejleszt az adott cég", hangsúlyozta *Nagybalyi Nándor,* az ITware kereskedelmi igazgatója. „Legyen szó Java vagy .Net alapú fejlesztésekről, alkalmazkodni tudunk többféle technológiához a képzéseinkkel. Arra azért figyelünk, hogy egy csapatban vagy egy oktatásban olyan fejlesztők legyenek, akik hasonló szinten és azonos platformokon fejlesztenek", tette hozzá.


FORRÁS: ITWARE


FORRÁS: ITWARE


FORRÁS: ITWARE

DANKÓ SÁNDOR, HAJTÓS BERTALAN ÉS NAGYBALYI NÁNDOR, ITWARE

Nem egyszerű feladat egy olyan, „cégre szabott" oktatási programot összeállítani, amilyen az **AI4DEV**, amely képes a megrendelő folyamataira is reflektálni. Emellett a folyamatosan változó MI-eszközök optimális használatát is elhozni úgy, hogy azok képességszintű beépítésével, rutinszerű használatával óriási lökést, egyben hatékonyságnövekedést kapjanak a fejlesztési folyamatok. Sok minden szükséges ehhez, hangsúlyozta Dankó Sándor. Az adott vállalkozás működéséből vett példákkal, megoldandó feladatokkal találkoznak a fejlesztők az oktatás gyakorlati részében.

Érdemes beletenni ezt a „pluszt": a tapasztalatok szerint sokat jelent, ha egy adott, a cégre igaz feladat vagy probléma megoldását keresik a hallgatók. Felmérik, hogy miképp lehetne megoldani akár a ChatGPT-re, akár a Copilot-ra építve. Sokkal jobban rávilágít

> A vállalkozások vezetőinek fel kell ismerniük, hogy az MI-alapú eszközök bevezetésével és használatával jelentős előnyökre tehetnek szert.

az MI-eszközök hasznosságára, ha egy valós, a résztvevők számára is ismert probléma kibontásában vagy megoldásában használják a viszonylag távoli mintapéldák helyett. „Sokszor alakul ki a fejlesztőben egyfajta belső gát vagy idegenkedés az MI forradalmi újdonságokat jelentő technológiáival szemben, de a saját problémákkal dolgozás oldhatja ezt", tette hozzá Nagybalyi Nándor. ■

A HANGFELISMERÉS ELESETT

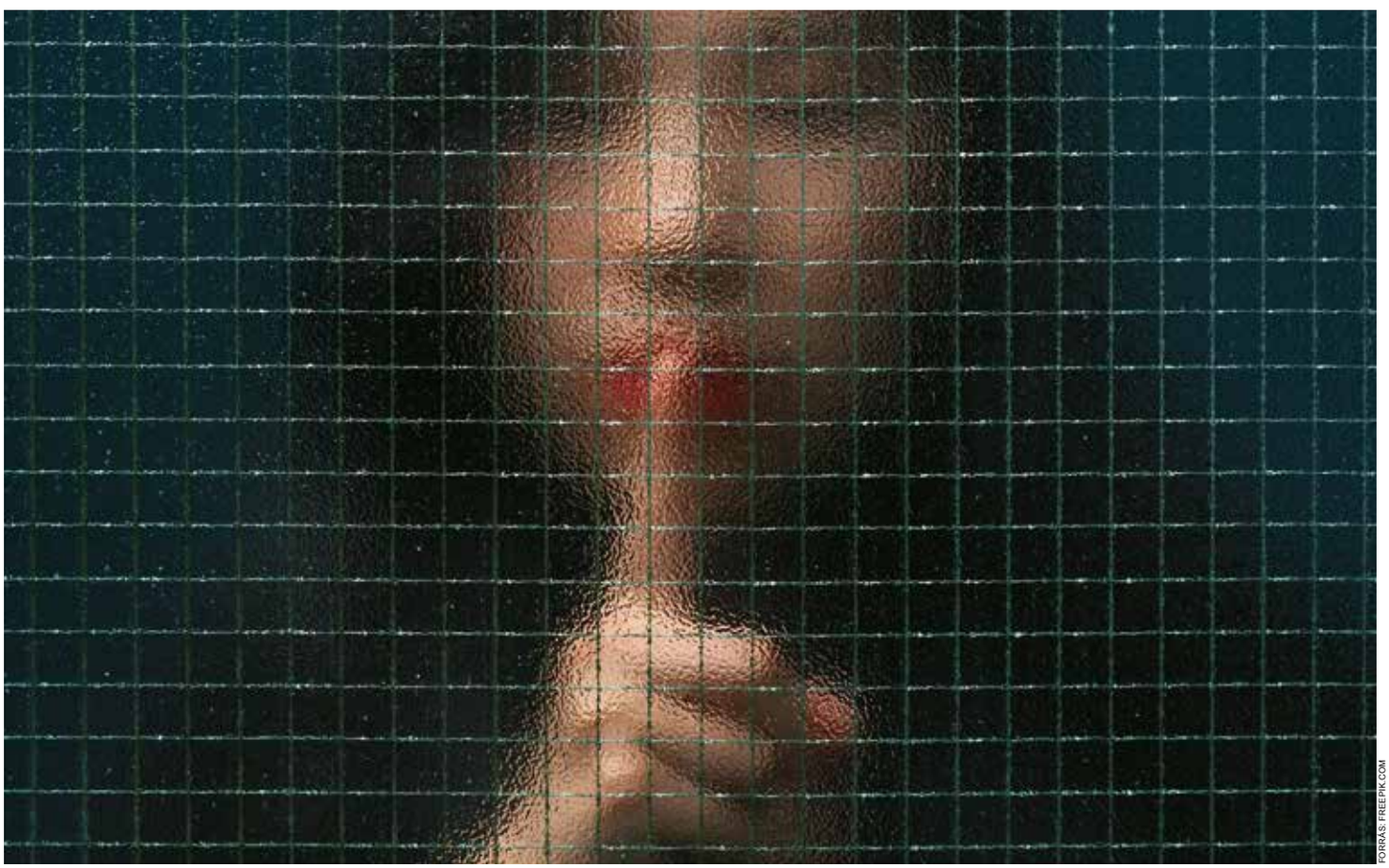
Nicsak, ki beszél?

A deepfake (MI-alapú álló- és mozgókép-hamisítás) másik kritikus komponense, a hangklónozás is hihetetlen léptékben fejlődik, jó megvalósítás esetén már nem tudjuk megkülönböztetni az emberi hangot a gépitől. Ez komoly veszélyt jelent mindenkire, beleértve a stratégiai döntésekért felelős vezetőket, cégvezetőket is, mondta az ITBUSINESS-nek *Keleti Arthur* kibertitok-jövőkutató, az Informatikai Biztonság Napja alapítója, az Önkéntes Kibervédelmi Összefogás (KIBEV) elnöke és alapítója.

Keleti Arthur több mint 20 éve foglalkozik kiberbiztonsággal, így testközelből látja azt a fejlődést, amely rapid módon ment végbe a hangklónozás terén. „A hangklónozás az emberi beszéd digitalizálásának egyfajta szintetizálása", bocsátotta előre a szakértő. „Lényege, hogy feltöltenek egy beszédmintát, és annak a hangjaiból illesztenek össze valami új hangzó szöveget, amit beszédnek nem neveznék, de ahhoz hasonló."

Ennek különböző szintjei, mélységei vannak, nyilván, ha csak egymás után rakunk hangokat, az nem lesz olyan, mint az emberi beszéd, erősen érezni lehet rajta azt, hogy ez gép „szülötte". A beszéd egyedi jellemzőjét több alkotóelem (hangfekvés, intonáció, hangsúly, hangmagasság) szintézise adja meg. Ám jó, ha tudjuk, ma már léteznek olyan szoftverek, amelyek elegendően sok és sokféle hangmintából közel emberi beszéd minőségű, az előbbi alkotóelemekkel rendelkező hangklónokat kreálnak.

Szerencsére az ember az evolúció során megkapta azt a képességet, hogy a hanghordozásból, a beszéd vokális jegyeiből képes leszűrni, ha valami nem stimmel. Gon-



FORRÁS: FREEPIK.COM

doljunk arra például, hogy bizony van, amikor megérezzük, ha valaki hazudik nekünk pusztán az illető hanglejtéséből, szóhasználatából. Vagy vegyük az újságíró hivatását: a zsurnaliszták némi rutint szerezve az előbb említett tényezők alapján pontosan tudják, hol kell vagy lehet közbevágni, kérdezni, hol ér a gondolatmenete végére a riportalany. A legtöbb „géphangnál", amilyen például az egyik kommunikációs szolgáltató telefonos asszisztense, már hallás alapján is nyilvánvaló, hogy a vonal túlsó végén nem hús-vér ember található, hanem egy hangklón – illetve robot. Nagyon gyorsan fejlődik azonban ez a szegmens, ma már nem mindig lehet könnyedén felismerni a hangklónozást.

Segít (?) az MI

A szakember hozzátette: mint az informatika minden szegmensében, itt is jelentős változást hozott a generatív mesterséges intelligencia, a ChatGPT-hez hasonló nagy nyelvi modellek már képesek „eldönteni" a kapott szöveg alapján a kontextust, és ehhez igazítják a klónozott beszéd hanglejtését, hanghordozását. Ennek a folyamatnak a tempója ma közel valós idejű, azaz valóban olyan, mint ha valakivel face to face beszélgetnénk.

Még ijesztőbb, hogy az ilyen minőségű hangklónozáshoz nem kell valamiféle hiper-szuper eszköztár, elegendő hozzá néhány ingyenes és nyílt forráskódú szoftver, valamint némi idő. A végeredmény pedig szinte bármire, akár a legsötétebb célokra is felhasználható. Volt már példa rá, hogy ilyen telefonhívással jelentős összeget utaltattak egy külső számlára, amikor a vezérigazgató hangján felhívták egy cég pénzügyesét. Olyan is megesett, hogy valakinek a gyereke szólt bele a telefonba, majd közölte, hogy elrabolták, ennyi és ennyi pénz utaljanak erre és erre a számlára, és ha ez megtörténik, nem esik bántódása a gyermeknek. De akár nagyvállalatok vezérigazgatóinak a nevében végzett információszerzésre is alkalmazható a hang.

Erősíti ezt a fajta módszert az a folyamat, hogy az elfoglalt emberek hamarosan már saját virtuális asszisztenssel rendelkezhetnek, „aki" a főnök nevében időpontot foglal, egyeztet, tárgyal – természetesen az ő hangján. Ha ez létjogosultságot nyer szélesebb körben (és miért ne nyerne!), már mindenkinek minden oka meglesz kételkedni abban, hogy a vonal másik végén helyet foglalót csak és kizárólag a jószándék vezeti-e.

Az MI mindenkire egyformán süt

Az ORFK kommunikációs szolgálatától megtudtuk: hazai viszonylatban ismertté vált bűncselekmények esetében is felmerült már olyan adat, amely alapján valószínűsíthető, hogy az elkövetők részben vagy egészben a „hangklónozás" technikáját alkalmazták. Mint azt kérdéseinkre lapunkhoz eljuttatott válaszukban írták: az online térben elkövetett csalások, visszaélések elkövetési módjai közül kiemelhető még a „social engineering" módszere, amelyet általában az üzleti szereplők körében alkalmaznak bűnelkövetők, megtévesztve olyan, nem vezetői szintű személyeket, akik jogosultsággal rendelkeznek üzleti tranzakciók lebonyolításához. A technikát alkalmazva az elkövetők manipulált audió- vagy audiovizuális tartalmak segítségével képesek az áldozatokban bizalmat kelteni, és kihasználva a jóhiszeműségüket, anyagi kárral járó ügyleteket elvégeztetni velük.

Hasonló módszerként azonosítható közismert személyek, politikusok vagy híresség hangjának másolása, utánzása, ami főként az állampolgárokat veszi célba, lejáratás, megtévesztés, álhírek terjesztésének szándékával. Ezen felül hozzátartozók vagy ismerősök hangjának utánzását alkalmazva a „hangklónozás" módszere ugyancsak alkalmas lehet megfélemlítésre, tévedésbe ejtésre, zsarolásra, vagy arra, hogy az elkövetők rávegyék a sértetteket pénzügyi tranzakciók megindítására.

FORRÁS: KELETI ARTHUR

KELETI ARTHUR KIBERTITOK JÖVŐKUTATÓ

A leggyengébb és a legerősebb láncszem is az ember

Ahogy a banki csalások esetében, úgy a „hangklónozásos" módszer használata kapcsán is elengedhetetlen a felhasználók tudatosságának növelése, az ismeretterjesztés a bűncselekmények megelőzése tekintetében. Mivel az elkövetői kör általában nyílt forrásból tudja beszerezni a csalások során módosított és felhasznált „alapanyagot", így kiemelten fontos az állampolgárok által megosztott kép- és videófelvételek számának minimalizálása, a felvételek hozzáférési körének tudatos korlátozása. A megtévesztést el lehet kerülni, ha a hívás közben (vagy a felvételen) hallható személlyel – akár a hívással párhuzamosan – kapcsolatot tud létesíteni a hívott fél, meggyőződve a kapcsolat hitelességéről – hívták fel a figyelmet.

Horváth Attila

Gigahertzek és a hang

Mintegy 24 éve (amióta 1 GHz-es vagy nagyobb a CPU-k órajele) az a helyzet, hogy a 44 kHz-es mintavételű (CD-minőségű) hang két mintavétele között 20 000 vagy több gépi kódú utasítást tud végrehajtani a processzor. Húszezer gépi kódú forrássornyit. Ennél kevesebb utasítás elegendő a másodfokú egyenlet megoldásához, tehát semmi csoda nincs abban, hogy a digitális hangképzés a programozásban „lejárt lemez": nem érdekes, minden elképzelhető feladatot megoldottak már. Legyen példa az „Autotune", amikor a hamisan éneklő előadó hangja valós időben a helyes hangnemben megy ki a hangszórókból – ez több mint 10 éve alapfunkció a színpadi erősítéstechnikában. Ez a deepfake egyik elődje. – *A szerk.*

NINCS LEHETETLEN, CSAK TEHETETLEN

NIS2-varázsige: a bölcsnek a kötelezettség valójában lehetőség, azaz profit

Az az Intalion megközelítése, hogy ne a lehető legkevesebb befektetéssel csússzunk át az auditon, hanem teremtsünk értéket, mert több van ebben, mint eszközbeszerzés és nyögés a kötelezettségek terhe alatt. *Kós Tamással,* az Intalion üzemeltetés-támogatás üzletágának igazgatójával, az ISACA Magyarországi Egyesülete elnökségi tagjával beszélgettünk.

A NIS2 az EU 2022/2555-ös, 2023-ban hatályba lépett irányelvének célja a magas szintű kiberbiztonság elérése az Európai Unió országaiban. Szelleme és filozófiája megbízhatóbb, egységesebb és a mostaninál magasabb biztonsági szintet követel meg a hálózati- és elektronikus információs-rendszerektől. Mivel az önkéntes fejlődés láthatóan elmaradásban van a területen, ezért a NIS2 direktíva kényszerítő eszköz is egyben, ám a kiszabható büntetési tételek miatti első sokkon átlendülve észre lehet venni az előnyöket is.

„Nem érdemes a 'megúszásra' játszani, így valójában több erőforrást égetünk el, mert mindig csak az audit pillanatára készítjük fel a szervezetet, ezért újra el kell végezni ugyanazokat a feladatokat anélkül, hogy azok hasznát élvezhetnénk. Ha átkeretezzük a kényszert lehetőséggé, meglepően értékes és hatékony dolgokat lehet létrehozni a NIS2 'farvizén'. A rendszerek felülvizsgálata során dönthetünk azok cseréjéről vagy megtartásáról. Mivel most mindenki NIS2-kompatibilis terméket ajánl a GDPR-korszakhoz hasonlóan, legyünk körültekintőek, és nézzünk szét alaposan a piacon", tanácsolta Kós Tamás.

„A NIS2-nek való megfeleléssel a folyamatainkat is át kell néznünk, felül kell vizsgálnunk vagy újakat kell létrehoznunk. Biztosra vehető, hogy a kiberbiztonsági tudatosság növelésének folyamata sok érintett esetében hiányzik ennek kultúrájával együtt", ismertette a szakember. Az átalakulás folyamatával megszülető új mindset a céges kultúra része lesz, beépül a szervezet életébe. Egy másik kiemelt haszon, hogy a megfeleléssel foglalkozó szervezetek (újra) ráeszmélnek arra, hogy hogyan működnek, illetve korrigálhatják működésüket a folyamatok leírásának frissítésével.

Az implementáció akkor nevezhető sikeresnek, ha nem, vagy csak csekély mértékben befolyásolja a core üzleti folyamatokat. „A NIS2-nek nem célja az üzleti működésbe beavatkozni, az üzleti folyamatok viszont fejlődhetnek, nőhet a tudatosság és a szervezet érettsége, a NIS2 implementáció közvetett hatásként, ami bár mellékhatásként aposztrofáljuk, valódi értéket képvisel", világított rá Kós Tamás.

„Bár a NIS2-nek nem célja az üzleti működésbe beavatkozni, az üzleti folyamatok viszont fejlődhetnek a megfelelőség elérése során."

Az első teendő az önazonosítás elvégzése, szögezte le a kiberbiztonsági vezető, majd elmondta, hogy ha érintett a cég, ki kell jelölni az elektronikus információs rendszerekért felelős személyt, illetve 2024. június 30-ig kell be kell jelentkezni az SZTFH (Szabályozott Tevékenységek Felügyeleti Hivatala) felé. A következő lépés annak felmérése, hogy az elvártakhoz képest hol tart a szervezet, hol szükséges fejleszteni. Minden szervezet más és más, eltérő felkészülési roadmap vár mindenkire. Ha nem vagyunk a terület szakértői ne halogassuk a megfelelő partner felkérését!

FOTÓ: ITBUSINESS

KÓS TAMÁS, INTALION

„Ha csak egyetlen eszközt lehetne beszerezni ehhez a piacról, biztosan számításba venném az IBM Qradar eszközét, amely régóta bizonyítja, hogy használatával magasabb szintre lehet emelni a kiberbiztonságot, legyen szó SIEM-ről vagy SOAR-ról", zárta mondandóját Kós Tamás. ■

AZ SAP ÉS AZ MI

A megoldás elemei elérhetőek, integrációjukkal szintet léphetünk

Nem kérdés, hogy a mesterséges intelligenciával valamilyen formában minden vállalatnál foglalkozni kell. Nagymértékben növeli viszont a siker esélyét, ha az ad hoc próbálkozás helyett előre kidolgozott stratégiát követve és tanácsadó segítségével vág bele a tervezésbe és bevezetésbe a vállalat.

Számos buktatót rejt az út, amelyen egy vállalkozás elindul a mesterséges intelligencia használata felé. Segíthet elkerülni ezen buktatók nagy részét, ha a vállalat – képletesen szólva – nem üres vászonra kezd festeni, hanem támaszkodik meghatározó informatikai szállítójának és annak partnerének szakértelmére és megoldásaira.

Ért a szóból

Ilyen segítséget tud kínálni az SAP és az egyik legnagyobb hazai partnere, az NTT DATA Business Solutions kettőse is. Mind a két cég régebb óta foglalkozik MI alapú megoldásokkal, de a lehetőségeket új szintre emelte, amikor az SAP tavaly ősszel kiadta Joule nevű szoftverét. Ez egy természetes nyelvi, generatív MI-megoldás, egyfajta copilot, amelyet lépésről-lépésre integrál az SAP a felhő alapú termékeibe, mondja *Bózsik Márton,* az NTT DATA szenior SAP-tanácsadója. Így a Joule az Early Adopter Care program keretében már a publikus felhőben futó S/4 HANA rendszerekhez is elérhető – ehhez csupán egy regisztráció szükséges.

Természetesen a Joule elsősorban nem szöveges információk generálásában jeleskedik, hanem más módokon könnyíti meg az SAP-felhasználók életét. Ilyen lehet például a lekérdezés-generálás: a végfelhasználó úgy fogalmazhatja meg a kérést, mintha az informatikus kollégához beszélne („kérem az elmúlt három negyedévből az 50 legnagyobb ügyféllel végrehajtott tranzakciókat, összehasonlítva a tavalyi év hasonló időszakával"), a rendszer pedig a kért formában szállítja a riportot, hoz egy példát *Baranyai Zsolt*, az NTT DATA IT-technológiai üzletág-igazgatója.

Folyamatok parancsszóra

A végfelhasználók mellett a tanácsadókat és a fejlesztőket is segítheti a Joule. A Signavio megoldásban a copilot segítségével, szöveges promptokat megadva, új üzleti folyamatok hozhatók létre a már meglévő folyamatelemekből. „Csak" azt kell leírni, hogy mi lesz a folyamat inputja, milyen típusú feldolgozást kell elvégezni azokon és milyen kimenetet várunk el. Az MI megoldás a folyamatmodellező eszközből kiemeli a szükséges építőkockákat és azokból összerakja a kívánt folyamatot. „Nyilván szükség lesz még bizonyos igazításra, finomhangolásra, de a munka oroszlánrészét már elvégezte a Joule", említ egy újabb lehetőséget Baranyai Zsolt.

FORRÁS: ITBUSINESS

BARANYAI ZSOLT ÉS BÓZSIK MÁRTON, NTT DATA

A rendszert könnyen használatba tudják venni a felhasználók. A promptok megfogalmazására szolgáló felület egységes; a tudásbázist pedig, amely alapján a válaszokat megadja, az SAP rendszerben tárolt adatok, struktúrák és folyamatok jelentik, mondja Bózsik Márton. A SAP BTP környezetben az AI Foundation segítségével elérhetőek külső rendszerek és adatforrások is.

Terv szerint haladva

A Joule-hoz hasonló eszközök megkönnyítik a mesterséges intelligencián alapuló megoldások használatba vételét, de nem teszik feleslegessé, hogy a szervezetek végiggondolják MI-stratégiájukat, emlékeztet Baranyai Zsolt. Számtalan területen bevethető az MI, éppen ezért nem mindig egyszerű megtalálni a legmegfelelőbb felhasználási módját.

Az NTT DATA szolgáltatáscsomagja a vállalatok MI-érettségi szintjét méri fel. „Abban segítünk, hogy a vállalkozás tervezetten tudjon az MI-vel foglalkozni. Felmérjük a meglévő informatikai eszközeit, az üzleti környezetét és céljait, majd ez alapján javaslunk egy célzott stratégiát. Leírjuk, hogy milyen technológiai elemekből és milyen üzleti célokra érdemes kialakítani a vállalati MI-megoldást", teszi még hozzá az NTT DATA üzletág-igazgatója. ■

SZÚRÓS ÉS BARÁTSÁGOS SZEMEKKEL NÉZI EGYMÁST A SOK-SOK SZEREPLŐ

Mikor és milyen valóság lesz az ipari metaverzumból?

FORRÁS: FREEPIK.COM

A metaverzumot hol mint az ipart a következő diszrupcióba repítő technológiai innovációként, hol pedig kaliforniai techguruk eszement lázálmaként jellemzik. Mindkettőnek van alapja, sok a technológiával kapcsolatos bizonytalanság, azonban egyre inkább kirajzolódik egy, az ipari felhasználás mellett szóló irányzat, amelyet tudományos cikkek mellett megvalósult ipari projektek is erősítenek.

Mark Zuckerberg 2021-ben bejelentett víziója, amelyet sokan egy olyan virtuális valóság (VR) térként képzeltek el, amely a felhasználókat egy tokiói tinibuli helyszínére száműzi, ahol VR-szemüvegben, számítógépes játékfigurákként, avatárjaik mögé búvva bájologhatnak felebarátaikkal, biztosan nem ipari metaverzum. Ahonnan mi vizsgáljuk a metaverzumot, sokkal inkább egy olyan kooperatív térnek látszik, ahol kutatómérnökök dolgoznak együtt például az AGN-201 kísérleti atomreaktor felügyeletén, az eredetivel megegyező digitális iker segítségével szimulálva és távolról irányítva annak biztonságos működését az Idaho National Laboratory projektjében.

Ebből az aspektusból nézve, az ipari metaverzum egy olyan valóságszimuláció, amely a legmodernebb technológiákat ötvözve teszi lehetővé az együttműködést a különböző vállalatok, tudományos kutatóintézetek és döntéshozók között. Képes valóságban létező gépeket, gyárakat, épületeket, városokat, hálózatokat és közlekedési rendszereket a virtuális térben modellezni, miközben integrálja a felhő- és az edge computing, az ipari mesterséges intelligencia és a digitális ikrek technológiáit.

Ezek összeadódnak, hogy a valós és a digitális világ között egy olyan erőteljes interfészt hozzanak létre, amely több, mint az egyes részek összege. Így tudja optimalizálni a folyamatokat még azok fizikai megvalósítása előtt vagy már működő létesítmények esetén a gépek, folyamatok digitális ikreinek létrehozásával és valós adatainak elemzésével.

Erősödő hangok a technológia mellett

Utóbbi megközelítést az MIT Technology Review „The emergent industrial metaverse" című, a Siemens-szel közös riportja több működő ipari együttműködésen keresztül tárja fel. Az ipari metaverzum a technooptimista forgatókönyv szerint így nemcsak képes forradalmasítani a munkafolyamatokat, és jelentős értéket teremteni, mind a vállalkozások, mind a társadalmak számára, hanem ezt már aktuálisan is teszi több működő projekt révén.

> „Ahogy a mobiltelefonok forradalma megváltoztatta a médiafogyasztásunkat, úgy a metaverzum is megváltoztatja majd a valós és virtuális világgal való interakcióinkat."
>
> – *HEMDAT SAGI,* STRATÉGIAI ÉS ÜZLETFEJLESZTÉSI IGAZGATÓ, KONNECT VOLKSWAGEN GROUP INNOVATION HUB

Egy példa a BMW debreceni gyára és az Nvidia Omniverse együttműködése. A technológia megkönnyíti a tervezést a termelőüzem és folyamatainak teljes modellezésével, hogy digitálisan kezelni tudják a kihívásokat még a debreceni üzem megépítése és a valós termelés beindulása előtt. Ez a képesség

A jövő szabványosítása a jelenben

Az ipari informatikai (IT) és operációs technológiai (OT) rendszerek integrációja kiemelt figyelmet igényel a gyártószektor szereplőtől. Ahhoz, hogy ezek a technológiai fejlesztések sikeresen valósuljanak meg, elengedhetetlenül fontos a megfelelő szabványok kialakítása és alkalmazása.

A szabványosítás terén például az Industrial Metaverse Interoperability Group, amely a Metaverse Standards Forum keretein belül működik, olyan vállalatokat tömörít, amelyek az ipari metaverzum egységes és szabványos környezetének létrehozásán dolgoznak. Ezek a kezdeményezések a „közös nyelv" megtalálásához járulnak hozzá.

Az átjárhatóság és az együttműködés ma már nemcsak előny, hanem alapvető elvárás is. Ahhoz, hogy a vállalkozások valóban versenyképesek maradjanak, érdemes bekapcsolódniuk egy szélesebb, nyitottabb ökoszisztémába.

Az ilyen platformok nemcsak a vállalatok közötti kapcsolatokat erősítik, hanem elősegítik az adatok, az erőforrások és az ötletek közötti áramlást is. Tehát, ha valóban az új dolgok felé tartunk és kihasználjuk a metaverzum előnyeit, akkor ezek a nyílt platformok azok, amelyek elindítják az iparágak közötti együttműködést.

FORRÁS: SIEMENS ZRT.

JERÁNEK TAMÁS, A SIEMENS ZRT. VEZÉRIGAZGATÓJA

segít optimalizálni a munkafolyamatokat, és ösztönzi az innovációt is a termékeny és interaktív kapcsolat révén, amely létrejön a valós és a virtuális világok között az adatoknak és a valós idejű szimulációnak köszönhetően.

Egy másik példa Nanjing, ahol az SNC egy üzemének teljesítményét digitális ikerrel szimulálták – mielőtt az első vödör betont kiöntötték volna. Ez segített elkerülni a tervezési hibákat, amelyek a múltban sok pénzbe és sok időbe kerültek. A tervezőcsoport például egy virtuális ellenőrzés során kiszúrta a megfelelő szellőzés nélküli festőgépet, és csak néhány apró változtatásra volt szükség ahhoz, hogy a gépet egy megfelelőbb helyre helyezzék. A napi működésben a digitális ikreket most már az üzem

> „Az ipari metaverzum egy olyan hely lesz, ahol a szoftverek sebességével újítunk. Hatalmas lehetőségeket kínál majd gazdaságaink és iparágaink átalakítására."
>
> – *ROLAND BUSCH,* A SIEMENS AG ELNÖK-VEZÉRIGAZGATÓJA

optimalizálására használják a folyamatban lévő termelés és a szimuláció közötti folyamatos visszacsatolás révén. A digitális gyár előnyei jól mérhetők: a gyártási kapacitás 200, a termelékenység pedig 20 százalékkal nőtt.

A légkör optimista

Iparági becslések szerint az ipari metaverzum globális piacának értéke 2030-ra elérheti a 100 milliárd dollárt. A Világgazdasági Fórum „Navigating the Industrial Metaverse: The Blueprint for Future Innovations", 2024 márciusában publikált riportjában úgy jellemzi a technológiát, hogy az forradalmasítja az ipari folyamatokat. Azt írják, hogy az innováció célja egy olyan kevert valóság létrehozása, ahol a fizikai és digitális világok összeolvadnak, így nyújtva agilitást és valós idejű interaktivitást.

A jelentés hangsúlyozza, hogy a metaverzum elősegíti az ipari forradalom következő fázisát, összekapcsolva a digitális ikreket más fejlett technológiákkal. A jelentés alkalmazási esetetek mutat be, így kívánja a technológia mellé állítani a döntéshozókat. A technológia iránti érdeklődés élénkülését jelzi, hogy az idei CES külön szekcióban foglalkozott a területtel, ahol többek között *Liz Hyman,* az XR Association, *Thomas Dexmier* a HTC Vive és *Peter Koerte* a Siemens képviseletében járták körül a technológia lehetőségeit és kihívásait.

Akku-metaverzum

A FREYR akkumulátorgyártó a Siemens segítségével optimalizálta az akkumulátorok gyártásának folyamatát, ehhez a vállalat által létrehozott digitális ikrek nyújtottak segítséget. Ezek valós adatokra épülve modellezték a gyárat és a gyártás teljes folyamatát, követhetővé, monitorozhatóvá téve a keverőgépek, a gyártósorok, a rakodó robotok és a gyártásban részt vevő humán munkaerő tevékenységét is. A valós produkciós adatok alapján a termelést felügyelő mérnökök pontosabban határozhatják meg a termelés főbb KPI-ait, a karbantartásért felelős mérnökök valós időben követhetik a gyártásban részt vevő gépek állapotát, míg a gyár operatív vezetői teljes képet kaphatnak az üzem teljes energiafelhasználásáról, annak költségéről és CO_2 -kibocsátásáról, vagy akár a beszállítói lánc folyamatairól.

> „Az ipari metaverzumban való részvétel egyik legfontosabb eleme az üzleti agilitás. Ha a nagyvállalatok nem válnak agilisabbá, nem lesznek képesek hatékonyan részt venni ezekben a partnerségi ökoszisztémákban, amelyek igazán hatékony megoldásokat hozhatnak létre."
>
> – *LESLIE SHANNON,* A NOKIA TREND- ÉS INNOVÁCIÓS FELDERÍTÉSÉRT FELELŐS VEZETŐJE

Interoperabilitás, ökoszisztéma

Ha manapság egy ipari vezetővel beszélgetünk, akkor biztosak lehetünk benne, hogy a mesterséges intelligencia mellett az „ökoszisztéma" és az „interoperibilitás" szavakat is bele fogja szőni mondanivalójába. Az iparágakon átnyúló problémák korszakát éljük, amelyekre az iparágakon túlnyúló partneri együttműködések jelenthetnek megoldást. Ilyen együttműködésen és tudásmegosztáson alapuló problémamegoldó platformként tekinthetünk az ipari metaverzumra.

Az előbb hivatkozott MIT-riport szerint az ipari metaverzum olyan dinamikus, sokszereplős rendszereket hoz létre a folyamatos adatintegráció- és elemzés révén, amelyek összekapcsolva az informatikai (IT) és üzemeltetési technológiákat (OT), egyedi lehetőségeket nyitnak meg az ipari hatékonyság és innováció terén.

Nehézségek az ipari metaverzum terjedése előtt

A fenti varázsszavak jelentik a technológia fejlődésének gátját is. A sikeres megvalósítás érdekében az ipari metaverzumnak partnerségekre van szüksége, amelyek átívelnek az iparágakon és elősegítik a közös szabványok kialakítását és az infrastruktúra fejlesztését. El tudjuk képzelni, ahogy az egymással vetélkedő cégek vagy a szabályozást befolyásoló felügyeleti szervek közösen megosztott adatok alapján fejlesztenek? Az ilyen együttműködések kultúráját még ki kell alakítani. A rendszerek ilyen mértékben összehangolt működtetése sok erőfeszítést igényel a gépek és az emberek között is, ami viszonylag magas belépési költségeket eredményez.

> „Egy fizikai tárgy digitális változatának megalkotása valójában csak a kezdet."
>
> – *DANNY LANGE,* A UNITY TECHNOLOGIES MESTERSÉGES INTELLIGENCIÁÉRT FELELŐS VEZETŐ ALELNÖKE

FORRÁS: FREEPIK.COM

Az ipari metaverzum megvalósításához szükséges technológiai infrastruktúra fejlesztése is kihívásokat okoz. Az egyik legfontosabb megoldandó kihívás az interoperabilitás hiánya, vagyis az ipari belső rendszerek és például a digitális ikrek összekapcsolhatóságának nehézsége. Meg kell oldani az ipari rendszerek közötti akadálytalan adatáramlást, valamint kis késleltetéssel hatalmas mennyiségű adat továbbítását, hatékony feldolgozását. Ez feltételezi a „standalone" (campus) 5G technológia alkalmazásának széleskörű, ipari elterjedését, emellett azt is, hogy az adatok ellenőrzött és biztonságos csatornákon haladhatnak át.

A digitális ikrek csak akkor lehetnek alapjai a hatékony döntéshozásnak, ha minden szempontból pontos adatokat tartalmaznak. Ha egy autógyár jövőbeli termelését akarjuk modellezni, akkor komplex és megbízható adatokra van szükségünk, amelyek a gyártás minden apró részletére kiterjednek a beszállítói láncoktól, a logisztikai folyamatokig, ehhez pedig az egész értéklánc minden résztvevőjének együttműködésére van szükség.

Ebben a piaci szereplőknek és a szabályozó hatóságoknak egyaránt meg kell találniuk az egyensúlyt az innováció előmozdítása és a kockázatok minimalizálása között, ami érinti az adatvédelem és kiberbiztonság területét is, hogy az ipari metaverzum valóban teljes potenciáljában kibontakozhasson.

Az ipari metaverzum tehát valóban forradalmi változásokat hozhat az ipar számára, és előnyöket kínálhat a vállalkozásoknak, amelyet sok alkalmazási példa is megerősít, ezek alkalmasak arra, hogy ezeket meg-

> „Az emberek kölcsönhatásba lépnek majd a digitális tartalommal és egymással, hogy ökoszisztémát alkossanak a technológia olyan fúziójában, amely elmossa a fizikai, a biológiai és a digitális világ közötti határokat."
>
> – *LANDRY SIGNE,* A THUNDERBIRD SCHOOL OF GLOBAL MANAGEMENT ÜGYVEZETŐ IGAZGATÓJA

vizsgálva kialakulhasson az együttműködés kultúrája. A döntéshozóknak a következő években érdemes nyitott szemmel követni az ipari metaverzum fejlődését. Például VR-szemüvegben: ez is egy olyan technológia, amely alapja lehet a jövő ipari innovációinak.

Myat Kornél

AZ IPARI IOT BIZTONSÁGÁNAK HELYZETE

Tűzfalakba ütközve

Az internetre kapcsolt számítógépek biztonságával mára a felhasználók nagy része valamilyen szinten foglalkozik. A gyárakban az OT- és IT-rendszerek integrációjával hálózatba kapcsolt gépek és IIoT eszközök biztonsága azonban sok iparvállalatnak okoz még fejtörést, pedig számtalan lehetőség adódik számukra a kényes adatok és rendszerek védelmére. *Varga Pál*, a BME tanszékvezetője segít átlátni a tűzfalakon.

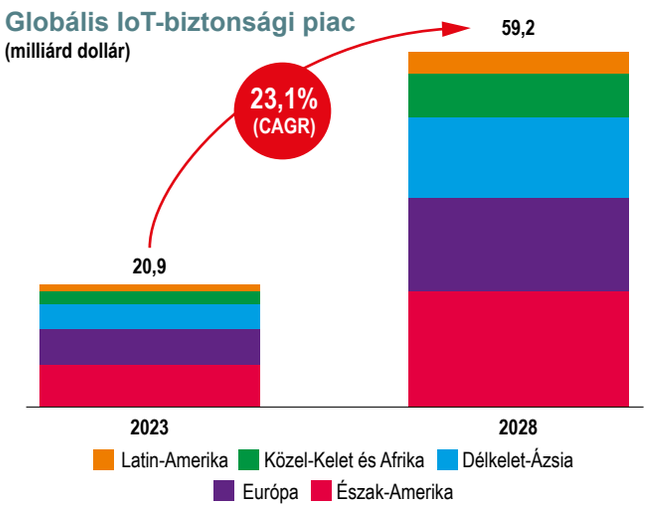
FORRÁS: FREEPIK.COM

A kiberbűnözők is imádják az IoT-eszközöket, találékonyak, és minden olyan gyenge pontot megtalálnak, amelyet kihasználva betörhetnek egy számítógépes hálózatba. Ez történt akkor is, amikor néhány éve egy kaszinó adatait egy távoli felügyeletet lehetővé tevő, high-tech akváriumon keresztül szerezték meg. Kétségtelenül kényelmes, ha távolról követhetjük a vízhőmérsékletet, a pH-t, vagy intézhetjük a halak etetését, de az fájdalmas, ha közben 10 GB érzékeny adatot is ellopnak tőlünk.

Sokféle IoT-eszköz osztozik egy-egy hálózaton. Nem azonosak a bennük lévő biztonsági protokollok, lehetnek köztük elavult okostelefonok vagy olyan számítógépek, amelyeken nem frissek a biztonsági tanúsítványok. Ezek a látszólag ártatlan eszközök így sokszor védtelenek – és hátsó ajtóként szolgálnak a teljes hálózathoz, a tulajdonosoknak érzékeny, a hackereknek értékes adatokhoz.

A lakat már nem segít, de mi van helyette?

A fizikai falak erős védelmet jelentettek, nemcsak a gyárak állóeszközeit, hanem azok által „termelt” adatokat is védték. Az ipar megállíthatatlan digitalizálódása és az OT-IT rendszerek összekapcsolódása, az adatalapú döntéseket segítő, hálózatba kapcsolt és felhőkben tárolt szerverekkel folyamatos kapcsolatban lévő IIoT- (ipari IoT-) eszközök



FORRÁS: MARKETS AND MARKETS

és szenzorok „okosabb” védelmet igényelnek, ami sok kihívást jelent az ipari döntéshozóknak. Ezért az IoT-biztonság piaca évről évre jelentősen bővül, becslések szerint a 2023-as 20,9 milliárdról 2028-ra eléri az 59,2 milliárd dollárt.

Dr. Varga Pál felhívja a figyelmet arra, hogy az IT-biztonsági problémák megjelentek az IIoT területén is. Ez le is lassítja a technológia elfogadását, sokan tartanak attól, hogy nem elég biztonságos. Ahhoz, hogy még szélesebb körben elterjedjenek, meg kell oldani felmerülő biztonsági kérdéseket. Létre is jöttek nemzetközi fórumok, amelyek célja a probléma közös kezelése, a biztonság fontosságának tudatosítása.

Kihívások, amelyek megoldásra várnak

Az IIoT biztonságának legfontosabb kihívásai közé tartozik a rendszerek komplexitása és heterogenitása. Az egységes biztonsági szabványok és protokollok hiánya megnehezíti a teljes körű védelmet és az eszközök egységes kezelését. Emellett a fizikai biztonság kiemelt fontosságú marad az ipari IoT rendszerekben, mivel a támadók jelentős károkat okozhatnak az eszközökben vagy a termelésben.

Az eszközök távoli elérhetősége és kapcsolódása a hálózathoz további biztonsági kockázatokat jelent. Az élettartam-kezelés és frissítések szintén kritikusak az ipari IoT rendszerek biztonsága szempontjából, mivel az eszközök hosszú élettartamúak, ezalatt új biztonsági sebezhetőségek jelenhetnek meg, amelyekre a rendszer frissítéseivel és megfelelő stratégiákkal kell reagálni.

A NIST keretrendszer

A NIST kiberbiztonsági keretrendszerének funkciói bemutatják, hogyan kezeljük és védekezzünk a kibervédelmi kockázatok ellen az IIoT-rendszereiben. Az AZONOSÍTÁS funkció célja az eszközök, rendszerek, adatok és folyamatok azonosítása és kategorizálása, míg a VÉDELEM funkció meghatározza és végrehajtja a megfelelő védelmi intézkedéseket az azonosított kockázatok ellen. A FELISMERÉS funkció az incidensek és kockázatok felfedezését szolgálja, míg a REAGÁLÁS funkció célja a gyors és hatékony reakció a kiberbiztonsági incidensekre. A VISSZAÁLLÍTÁS funkció azután lép életbe, hogy az incidenseket kezelték, visszaállítva a rendszereket és az üzleti folyamatokat a normál ügymenethez.

FORRÁS: NIST

IoT-biztonsági irányzatok

- **Edge Security** Az eszközökön belüli biztonság az adatok helyben történő feldolgozását, elemzését és titkosítását biztosítja, még azelőtt, hogy eljutnának a felhőbe vagy távoli infrastruktúrákba, így csökkenti a támadási felületet és növeli az adatvédelmet.
- **Felhő alapú vezérlés** Vannak olyan IIoT-eszközök, amelyeket távolról lehet vezérelni, szoftverüket frissíteni akár egy felhőből, kis késleltetésű 5-6G hálózatokon.
- **MI és gépi tanulás a biztonságban** Az MI és a gépi tanulás révén az IoT-rendszerek is megszerzik a gyanús működésminták felismerésének képességét, és azonnal tudnak reagálni is ezekre, ki is szűrik az ismeretlen vagy új típusú támadásokat.
- **Fenyegetésmenedzsment és elemzés** Az előrejelző elemzések és a fenyegetésmenedzsment kulcsfontosságúak. Az IoT-rendszerek által gyűjtött adatok nagy mennyisége és változatossága segítheti a fenyegetések korai azonosítását és a proaktív védekezést a biztonsági incidensek ellen.
- **Blockchain technológia** A blokklánc technológia az eszközök közötti biztonságos kommunikációt és az adatok hitelesítését, nyomon követését teszi lehetővé elosztott és átlátható módon. Lehetőséget kínál az IoT-rendszerek biztonságának javítására és az adatok védelmére, különösen érzékeny és kritikus ipari területeken. Az IoT integráció kiterjed a beszállítói láncokra, így a blokklánc technológia és az elosztott hitelesítési mechanizmusok (DLT-k) egyre inkább segíthetik azok biztonságát.
- **IT- és fizikai biztonság integrációja** Az ipari IoT-ban nem csak a digitális hálózatok és adatok, hanem a fizikai rendszerek és eszközök védelmére is összpontosítanak. Figyelik és védelmezik az ipari rendszerek fizikai összetevőit, például az ipari robotokat.

Az ipari IoT eszközök széles körű felhasználása és integrációja további kihívásokat jelenthet a szabványosítás és az interoperabilitás terén.

IIoT-biztonsági keretrendszerek

Az egységes biztonsági szabványok és protokollok hiánya megnehezítheti az eszközök közötti együttműködést és az integrációt, ezért az IIoT-fejlesztőknek és üzemeltetőknek figyelemmel kell kísérniük az iparági standardokat és keretrendszereket. Varga Pál kiemeli, hogy iparvállalatok döntéshozóinak arra érdemes törekedniük, hogy a rendszerek zártsága és az ezzel járó biztonság, valamint a digitális szolgáltatások előnyeiért célzottan kinyitott csatornák között őrizzék meg az egyensúlyt.

A BME szakembere kiemeli az összefogás szükségszerűségét és a nemzetközi szabványok és testületek munkáját, amelyek célja, hogy az IIoT terén nyújtsanak segítséget az iparvállalatoknak és döntéshozóiknak.

Az egyik ilyen a NIST Cybersecurity Framework (CSF), amely iránymutatást nyújt az ipar, a kormányzat és a kormányzat számára a kiberbiztonsági kockázatok kezeléséhez. A másik az IISF keretrendszer, aminek betartása garantálhatja a biztonságot ezen a téren. Magyarországon a Hírközlési és Informatikai Tudományos Egyesület az egyik platform, amely zászlajára tűzte az IoT-biztonság kérdését.

Myat Kornél

FORRÁS: DELTA

NIS2 ÉS AZ ÜGYFÉLIGÉNYEK

Az IT-biztonságban nem működik a konfekció

Nincs egységes, mindenkinél alkalmazható csodaszer vagy varázseszköz a NIS2 követelmények teljesítésére. A meglévő állapot és a hiányosságok felmérést senki nem úszhatja meg, az egyéni igényekre szabott megoldások bevezetése és üzemeltetése pedig a felhasználók aktív és folytatólagos részvételét igénylik.

Minden figyelmeztető jel és híradás ellenére a magyar vállalkozások nem kis hányada mindeddig struccpolitikát folytatott, amikor az információbiztonságról volt szó. Talán bevezettek valamilyen védelmi intézkedéseket, üzembe állítottak eszközöket, technológiákat, de nem vették komolyan, és különösen nem gondolták végig, hogy pontosan mit és miért kell(ene) csinálniuk. *(A leggyakoribb és legkárosabb téves elképzelésekről és gyakorlatokról lásd „A biztonság hamis érzete” című keretet!)*

Munka lesz bőven

Ennek a „gondtalan”, bár sok veszéllyel terhelt állapotnak sokak esetében véget vet a NIS2 szabályozás. Nemcsak meghatároz különféle kötelezettségeket, hanem azok megvalósítását auditáltatja is, a notórius nem teljesítőkre pedig komoly bírság vár. Maguk a követelmények is olyanok, amelyeket nem tud könnyen teljesíteni egy vállalat, ha eddig nem fordított kellő figyelmet az IT-biztonságra: kockázatokat kell felmérni; szabályzatokat kell írni; védelmi intézkedéseket megvalósítani; ha szükséges, új rendszereket bevezetni (márpedig a legtöbb helyen szükséges lesz); penetrációs tesztet végeztetni; végül pedig mindezt auditáltatni is.

Nincs varázseszköz, egyfajta „silver bullet”, amely megoldja a fenti gondokat, oszlatják el az esetleges reményeket az egyik legnagyobb hazai rendszerintegrátor, a tőzsdén is jegyzett Delta Technologies Nyrt. 100%-os tulajdonában álló Delta Systems Kft. szakemberei. Ők inkább a gondosan összeválogatott és az ügyfelek igényeire szabott termék- és szolgáltatáscsomagokban hisznek, és ilyeneket kínálnak a felhasználóknak.

Mindenhol van hiányosság

A vállalat több évtizedes szakmai tapasztalattal rendelkezik az informatikai rendszerek megtervezése, kiépítése, integrációja és üzemeltetése terén, ezért szakembereik gyakorlatilag szinte minden igénnyel találkoztak már, legyen szó kisvállalkozásról vagy több milliárd forintos árbevételű nagyvállalatról.

A munka mindig azzal kezdődik, hogy fel kell mérni a jelenlegi és a kívánt (előírt) biztonsági helyzet közötti űrt. A NIS2 kapcsán még nem ismert minden részletszabály, de a főbb irányvonalak igen, így meghatározhatók azok a pontok, területek, ahol komoly elmaradás látszik – például határvédelem, logelemzés stb., és elsőként ezekre a területekre lehet irányítani az erőforrásokat.

A Delta szakembereinek tapasztalatai szerint még az IT-biztonsági szempontból érettebbnek számító vállalatok döntő többségénél sincs az információkat és eseményeket automatizáltan kezelő SIEM-rendszer, és nem foglalkoznak kiemelten a munkakörükből adódóan magas jogosultságokkal rendelkező felhasználók hozzáférés-menedzsmentjével.

Lépésről-lépésre haladva

Az első cél az, hogy a legnagyobb elmaradásokat pótolják, és legalább egyenszilárdságú, 70-75 százalékos készültségi szintre emeljék a biztonsági rendszereket. A pontos követelmények ismeretében így már könnyebb lesz a még mindig hiányzó intézkedések megtétele.

Óriási különbségek lehetnek ügyfél és ügyfél között. A Delta azoknak is tud megoldást kínálni, akik a lehető legkisebb költséggel szeretnék elérni a kívánt eredményt, és azoknak is, akik kritikus rendszereket üzemeltetnek, ezért a legmagasabb szintű védelemre van szükségük. Akár a nulláról építkezve meg tudják valósítani a végpontvédelmet, a sérülékenységvédelmet, a logelemzést vagy a folyamatos monitoringot. Biztonsági forráskód-elemzést is végeznek, amely a nyílt szoftverek egyre gyakoribb használata miatt létfontosságú, ráadásul a kritikus besorolású cégek számára kötelező feladat a NIS2-ben. Be tudnak vezetni különféle integrált (SIEM-, SOAR-, XDR-) rendszereket, amelyek nemcsak figyelik az eseményeket, hanem szükség esetén automatikusan be is avatkoznak.

Magasabb szintű védelmi intézkedéseket is be lehet vezetni: a Delta szakemberei ki tudnak alakítani georedundáns infrastruktúrákat, azokon helyreállítási (disaster recovery) teszteket végrehajtani, és mindezekre építve teljes üzletmenet-folytonossági tervet (BCP-t) kialakítani.

A biztonság hamis érzete

A Delta szakemberei számos olyan esetet fel tudnak idézni, amikor a vállalkozás látszólag gondoskodott saját kiberbiztonságáról, vagy legalábbis meg volt erről győződve. Néhány a gyakoribb tévhitekből és rossz gyakorlatokból.

- **Nem ellenőrzött mentések** A cég készít biztonsági mentéseket a kritikus adatairól, de soha nem próbálta meg visszaállítani a működést ezekről a mentésekről.
- **Nem ellenőrzött szoftverek** Amennyire hasznosak, annyira veszélyesek is lehetnek a szabadon elérhető, nyílt forráskódú szoftverek, a bennük rejlő esetleges sérülékenységek miatt.
- **Hiányos biztonságtudatosság** A leggyengébb láncszem az ember: a hamis emaileket fel nem ismerő, a linkeket, dokumentumokat gondolkodás nélkül megnyitó kollégák az egyik legkomolyabb veszélyforrást jelentik.

Az audit során is az ügyfél mellett állnak

Segít a Delta a felhasználói tudatosság növelésében is. A vállalat kapcsolatban áll több, a kibertér biztonságát folyamatosan figyelő szervezettel és hatósággal, és ha jelzést kapnak tőlük, azonnal felhívják az ügyfeleik figyelmét az új veszélyre. Végeznek célzott penetrációs teszteket is – a rendszeresen ismételt vizsgálatok jól mutatják, hogy milyen sikeres volt a felhasználói tudatosság erősítése. A technikai védelmi megoldások mellett a humán tényező erősítése nélkülözhetetlen eleme a kitettség, a kockázatok csökkentésének.

Biztonsági tanácsadói tevékenysége során egyedi szolgáltatást is kínál a Delta. A védelmi rendszerek megtervezése és kiépítése után sem engedi el az ügyfelek kezét, hanem az auditokon is ott vannak a felhasználók mellett. Így csinálták ezt az ISO 9001 és ISO 27001 auditok során is, ezt fogják tenni, amikor a NIS2-es auditokra kerül sor valamikor 2025-ben. Így az auditor azonnal választ kaphat kérdéseire, gyorsabb lesz maga az ellenőrzés és az esetlegesen feltárt hiányosságok pótlása is.

Ember is kell a technika mellé

A Delta szakemberei hangsúlyozzák, hogy a NIS2 előírásainak való megfelelés nem pusztán pénzkérdés: nem elegendő a rendszereket megvenni és beüzemelni. Azokat utána folyamatosan monitorozni kell, a beállításokat hozzá kell igazítani a megváltozott üzleti környezethez, folyamatokhoz és az újonnan felbukkanó fenyegetettségekhez. Ennek pedig komoly emberi erőforrás-igénye van: a biztonsághoz magas szinten értő szakemberekre van szükség.

Kevés felhasználónak lesz annyi szakembere, hogy ezeket a feladatokat házon belül ellássa, a többségnek külső segítséget kell igénybe vennie. A Delta tudatosan készült arra, hogy minél több ügyfélnek tudjon ilyen jellegű szolgáltatásokat kínálni. Egyrészt bővítették saját szakértői bázisukat, másrészt együttműködési megállapodásokat kötöttek más tanácsadó és IT-biztonsági cégekkel, így az ő erőforrásaikra is támaszkodhatnak. ■

EZ MIND MESTERSÉGES INTELLIGENCIA

Hangalapú utasítások, kommunikáció a raktári rendszerekkel, autonóm targonca

Szinte berobbant az életünkbe a mesterséges intelligencia (MI), amely ma már minden szektorban jelen van. Nincs ez másként a logisztikában sem, egyes szakemberek szerint forradalmasítani fogja azt. Megkérdeztünk néhány hazai döntéshozót, mint gondolnak erről.

A mesterséges intelligenciával kapcsolatos legfontosabb logisztikai fejlesztések közé tartozik a raktárak automatizálása, az autonóm járművek, az intelligens utak használata, valamint a prediktív analitika. Az MI segítségével számos folyamat automatizálható és egyszerűbbé tehető, így a vállalatok időt és pénzt takaríthatnak meg, főként munkaerő-vonalon. A McKinsey tanácsadó cég szerint 2030-ra a mesterséges intelligencia paradigmaváltást hoz a logisztikába, amely ma számos kihívással kénytelen szembenézni, ám az MI ezek leküzdésében is segíthet.

„A mesterséges intelligenciának két nagy ága van: az analitikus és a generatív", mondta elöljáróban a svéd Qamcom IT-tanácsadó cég magyarországi leányvállalatának ügyvezetője, *Fülöp Géza*. „Éppen a logisztikában nagyobb a szerepe a problémamegoldó, azaz analitikus intelligenciának. Ebben legalább annyi munka van és minimum annyi relevanciával bír a logisztikai cégek számára, mint a popouláris, generatív MI-nek."

Az érzékek birodalma

A logisztikai szakterületen rengeteg a gépi látásos feladat: minőségellenőrzés, a biztonság garantálása, adatkezelés stb. Már léteznek olyan MI-megoldások, amelyek képesek különféle szagok és vegyi anyagok felismerésére adott légtérben, például raktárban, hűtőkamionban. A prediktív karbantartásban ma már fel lehet szerelni a teherautókat, kamionokat szenzorokkal, és a mesterséges intelligenciának betanítható

FORRÁS: BUSINESS WIRE

az adott motorfordulatszámhoz tartozó hangfrekvencia, vagy hőmérsékleti érték – ha a rendszer bármilyen változást érzékel, azonnal jelez, ez az anomália-detektálás. Így a meghibásodások a kezdet kezdetén diagnosztizálhatók, és szükség esetén kezelhetők is, megeshet, hogy így jelentős többletköltségeket lehet megelőzni.

Használható az MI a korábbi adatok elemzése alapján például megrendelések előrejelzésében is. „Tudok olyan esetről, amikor egy fagylaltforgalmazó cég következő nyári megrendeléseit a mesterséges intelligencia 80 százalékos pontossággal 'jósolta meg', miközben a hús-vér munkavállalók 60 százaléknál jobb arányú becslésre nem voltak képesek. Sajnos, nem hittek az MI-nek, átírták a prognózist, így a szezonra 70 százalékot sikerült realizálnia a cégnek, pedig, mint utólag kiderült, meglett volna az a 80 is", mesélte Fülöp Géza.

Arról is beszélt, hogy az új technológia segítségével egy komplett raktár teljes területe megfigyelhető. „Klasszikusan" egy biztonsági őr egyszerre 40 kamera képét próbálja befogadni, illetve kontrollálni, ami nyilván nem lehetséges 100 százalékosan. De a mesterséges intelligencia egy másodperc alatt egyszerre kezeli mind a 40 kamera képét, pontosabban az általuk továbbított jeleket.

Valós idejű viselkedésfelismerés

„Készítettünk egy tanulmányt, hogy ez a technológia a városok közterein kapásból beazonosítja a zsebtolvajokat a mozgásmintájuk alapján, mert máshogy mozognak, viselkednek, mint az egyszerű sétáló emberek", mondta az ügyvezető. „Hasonlóan az illetéktelen személyek könnyedén beazonosíthatók adott esetben egy logisztikai komplexumban, raktárban is", tette hozzá. De képes például a menetlevelek összehasonlítására, vagy szerződések készítésére korábbi minták alapján, akár az éppen aktuális módosításokat is beépítve. Mindez azonban nem jelenti azt, hogy a mesterséges intelligencia elveszi az ember munkáját, mert rengeteg szegmensben elengedhetetlen az ember jelenléte, elsősorban az olyan helyeken, ahol nem elég választani, hanem meg is kell azt indokolni.

Fülöp Géza szerint Magyarországon a kkv-k még nemigen élnek az MI kínálta lehetőségekkel nemcsak bizalmi okokból, hanem anyagi meggondolásból is: nem szívesen invesztálnak addig, amíg nem győződtek meg használatának vitathatatlan előnyeiről. Ezzel együtt némi elmozdulás érzékelhető, ha a jó tapasztalatok körbeérnek, akkor várható nagyobb fellendülés.

FORRÁS: QAMCOM

FÜLÖP GÉZA, QAMCOM

FORRÁS: WABERER'S

TOBAK TAMÁS, WABERER'S INTERNATIONAL

Logisztika = = IT

Tobak Tamás, a Waberer's International IT-igazgatója szerint ma már egy logisztikai operáció hatékony működése elképzelhetetlen fejlett informatikai rendszerek, így például a mesterséges intelligencia nélkül. „A mesterséges intelligencia fokozatosan épül be a napi működésbe, használata egyre inkább el fog mozdulni a klasszikus analitikus alkalmazási területek, az ügyfélszegmentálás, értékesítés és lemorzsolódás-előrejelzés felől az operatív munkafolyamatokba való beépülés irányába", fogalmazott Tobak Tamás. „Egy-egy részfeladatot ember, egy másikat pedig mesterséges intelligencia fog végezni, hasonló módon, mint ahogy ezt már megszoktuk a gyártásban az ember-robot együttműködés kapcsán", részletezte.

Az egyik izgalmas terület a fuvarozási operáció erőforrás-optimalizálása. Nem mindegy, hogy adott feladatot melyik járművezető hajtja végre, milyen vontatóval és pótkocsival, ahogy nő a volumen, egyre nehezebb feladat kiválasztani, hogy mikor, kinek, melyik járművel, melyik fuvarfeladatot kellene elvégeznie. Az optimum megtalálása számos mutatószám együttes értékelését igényli.

A Waberer's több mint 250 000 m^2-en végez valamilyen raktározási megbízást az ország több pontján. Vannak olyan raktárai, ahol a komissiózást (melyik termékből mennyit kell összekészíteni) félautomata targoncák és ún. „voice picking" rendszerek segítik. Egyrészt a targoncát a vezérlőnek nem kell végig fizikailag vezetni, hanem az eszköz követi őt. A voice picking pedig lehetővé teszi a hangalapú (beszéd-) utasításokat, így könnyen és hatékonyan lehet kommunikálni a raktári rendszerekkel, ami kevesebb időt és energiát vesz igénybe a hagyományos adatbevitelhez képest.

„Az említett példák mellett már vizsgáljuk azt is, milyen előnyökkel jár a mesterséges intelligencia használata a járművek műszaki állapotának rendszeres vizsgálata, illetve tervezett karbantartásai kapcsán", árulta el végül Tobak Tamás.

Beszélt egy másik optimalizációs fejlesztésről, az itiner-tervezésről is. Ez az útvonaltervezés kiegészítése egyéb fontos információkkal, például parkolással, pihenéssel, komphasználattal, tankolással stb. Nemcsak azt kell figyelembe venni a tervezés során, hogy minél gyorsabban vagy minél rövidebb úton jusson el egyik pontról a másikra a jármű, hanem azt is, hogy ezt milyen tranzitköltséggel, érkezési idővel, parkolással teljesíti.

Az alacsony haszonkulcs pillanatok alatt elillan egy rossz tranzitútvonal-választással vagy egy fölösleges alagút-áthajtással, de akár egy nem optimális kúthasználattal is. Ezt IT-oldalról azzal lehet megtámogatni, hogy minél pontosabb kalkulációkat és minél több információt bocsátanak a gépkocsivezetők rendelkezésére arról, hogy melyik az optimális útvonal. Sok ezer megbízás esetében utanként már néhány euró is komoly megtakarítást jelenthet.

Horváth Attila

FORRÁS: FREEPIK.COM

VEZÉRIGAZGATÓI FELMÉRÉSEK

Rózsaszín szemüveggel nézik a világot a cégvezetők

Pesszimista 2023 után optimista 2024-re számítanak a magyar és a világ ügyvezető igazgatói és vezérigazgatói két magyar és nemzetköz vonatkozású kutatás szerint. A mesterséges intelligenciával szemben a várakozások elég magasak a szervezeten belül, így elképzelhető, hogy több vállalat csalódni fog amikor az eredményekkel szembesül.

Néha csak egy optimista szemüveg kell ahhoz, hogy a vállalat merjen nagyokat álmodni, és merjen nagyobb kockázatokat vállalni. Ez a világot rózsaszínben láttató szemüveg idén felkerül a vállalatvezetők, ügyvezetők és vezérigazgatók szemére – legalábbis két, a CEO-k állapotát felmérő kutatás szerint.

Optimista kilátások

A KPMG kutatásában a 297 magyarországi cégvezetővel készült személyes interjúkból kiderül, hogy a tavalyi rekord pesszimista év után a többség gyorsulásra számít: a világgazdaság húzóerejének erősödésében 54 százalék, a magyar gazdaság növekedési ütemének gyorsulásában 60 százalék hisz. Lassulást globálisan és magyar viszonylatban is 22 százalék jósol, szemben a tavalyi 76 százalék és 85 százalékkal. A felmérés történetében idén először fordul elő, hogy a magyar vállalatvezetők a gazdasági növekedéssel kapcsolatban optimistábbak, mint a saját bevételeik alakulását illetően. Azok aránya, akik bíznak cégük 2024-es gyarapodásában, a 2012-ben mért 47 százalékos szintre esett vissza.

Noha a Deloitte kutatásában „kihívásként” jellemezték a mögöttük hagyott 2023-as évet, ők is rózsaszínűbb szemüveggel nézik az előttük

álló időszakot: míg a 2023 őszi kutatásban csak 7 százalékuk volt optimista, ami a világgazdasági kilátásokat és saját vállalatukat illeti, a téli kutatásban már 27 százalékuk gondolkodik hasonlóan. Ez nyilván még mindig nem a többség, de mutatja, hogy a növekedés a trend. Érdekes, hogy a Deloitte kutatásában is a vállalatvezetők a gazdasági növekedéssel kapcsolatban optimistábbak, mint a saját bevételük alakulását illetően.

A KPMG adatai szerint a vállalatvezetők a külső, fenyegető tényezők közül továbbra is az infláció hatásától tartanak a legtöbben (51 százalék). Ezt követi a szakképzett munkaerő hiánya (48 százalék), majd közel azonos eredménnyel a makrogazdasági volatilitás (37 százalék), a geopolitikai konfliktusok (36 százalék) és a kiberkockázatok (35 százalék). 2023-hoz képest a makrogazdasági volatilitásnak és a geopolitikai konfliktusoknak való kitettség érzése csökkent legnagyobb mértékben, nem változott azonban a klímaváltozás hatásaitól és a kibertámadások okozta kockázatoktól való aggodalom. A Deloitte felmérésében is ugyanezek az aggodalmak szerepelnek, más súlyozással, a geopolitikai instabilitás a vezető ok, amiért a vezetők aggodnak, az infláció csupán a harmadik ezen a listán – az októberi kutatáshoz képest 24 százalékponttal csökkent ennek fontossága. A kiberbiztonsági támadásoktól a vezetők 18 százaléka fél csupán, ami 7 százalékponttal kevesebb, mint a korábbi felmérés.

Nagyobb az MI füstje, mint a lángja

A 2023-as év slágere a generatív mesterséges intelligencia volt. Sok szó esett róla, de az adatok alapján a vállalatok alig ötödének működésében játszott csak szerepet, és a vezetők 27 százaléka nyilatkozott úgy, hogy a technológiai stratégiájában már helyet kapott a generatív MI. Kivételt képez ez alól a technológia, média- és szórakoztatóipar, valamint távközlési iparág, ahol a generatív mesterséges intelligencia jóval előrébb jár, mint a többi iparágban; itt az elvárások és a félelmek szintje is magasabb az átlagosnál.

Az amerikai piacon a generatív mesterséges intelligenciában ennél sokkal többen bíznak. A megkérdezettek több mint fele, 56 százaléka megnövekedett produktivitást és alacsonyabb költségeket vár el a technológiától. A vezetők 58 százaléka már elkezdte a generatív MI bevezetését annak érdekében, hogy a manuális feladatokat automatizálják (ősszel ez az arány csak 40 százalék volt). A tengerentúli szervezetek 45 százaléka ugyanakkor az üzleti működési költségek csökkentésére használja a technológiát. Az biztos, az amerikai üzleti vezetők a generatív MI-t a „next best thing”-nek tartják, melynek használatáról nem szabad lemaradniuk.

A kutatások

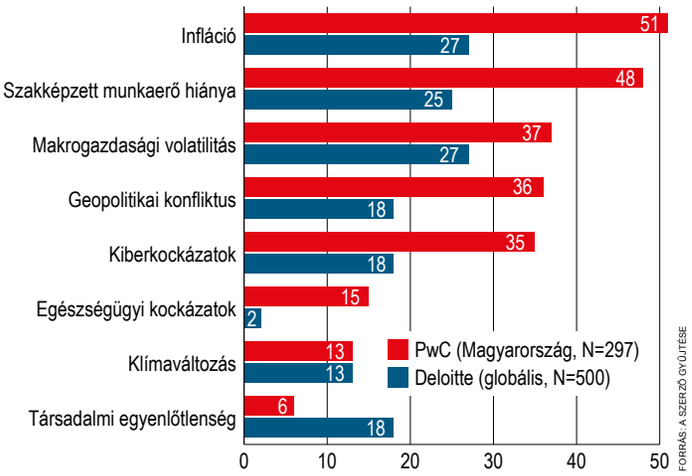
Cikkünkben a KPMG és a Deloitte kutatásai alapján vázoljuk fel, hogy milyen vállalati és technológiai jövőt látnak a cégvezetők. (KPMG „CEO Outlook 2024” és Deloitte „CEO Survey Winter 2024”), a KMPG kutatását tizenharmadik alkalommal készítették el. A magyarországi felmérés készítése során a személyes interjúkészítés módszerét alkalmazták, amelynek keretében a KPMG szakemberei 2023 októbere és decembere között 297 hazai vállalat vezérigazgatóját kérdezték meg, és a kvantitatív adatokat kérdőívek segítségével rögzítették. A Deloitte kutatását 107 CEO megkérdezésével készítették 2024 februárjában, döntően amerikai vállalatvezetőket faggattak.

Bővülő vezérigazgatói kompetenciák

A magyar felmérésben arról is kérdezték a vállalatvezetőket, hogy szokásos feladataikon túl mivel foglalkoznának szívesen és hol látják még a szerepüket a vállalati struktúrában. A magyar válaszadók négyötöde több figyelmet kíván fordítani szervezete humánerőforrást érintő kérdéseinek megoldására (80 százalék). Emellett csaknem négyötödük (78 százalék) a saját digitális készségeinek fejlesztését tartja fontosnak, (háromnegyedük a kollégáiét is), és 62 százalékuk közelebb kerülne a technológiai döntések meghozatalához: elsősorban a fejlesztésekkel felmerülő üzleti vagy szervezési kérdésekben (63 százalék), valamint stratégiai partnerségek kialakításában (56 százalék) vállalnának több szerepet.

Mitől félnek a vezérigazgatók?

(válaszolók százalékában, 2024-ben)



FORRÁS: A SZERZŐ GYŰJTÉSE

Míg itthon a vállalati adaptáció aránya ilyen alacsony, a várakozások már a közeljövőre nézve is elég magasak a generatív mesterséges intelligencia átalakító szerepével kapcsolatban. A következő egy évben a magyar vezetők fele számít arra, hogy az MI javítja a termékek vagy szolgáltatások minőségét és növeli a munkaidő hatékonyságát. A következő három évre a cégvezetők hat tizede úgy véli, hogy nem pusztán új készségeket követel majd meg az MI a munkatársaiktól, hanem megváltoztatja majd az értékteremtés módját csakúgy, mint a verseny természetét az iparágukban. Reméljük, a technológia nem okoz csalódást.

Kockázatokat is rejt az MI

A generatív mesterséges intelligencia szerepével kapcsolatos rövidtávú aggodalmak közül a kiberkockázatokat 72 százalék említette, öt éves távlatban már 77 százalék ez az arány. A vezérigazgatók 52 százaléka véli úgy, hogy az MI a téves információk terjedését gerjeszti már egy éven belül, öt éves távlatban 71 százalék lát ilyen kockázatot. Emellett vállalatuk hírnevét fenyegető kihívásokkal és a jogi kötelezettségek növekedésével számolnak a vezérigazgatók, jövőre 53 százalékuk, 5 év távlatában pedig 62 százalék várja ezen hatások erősödését.

Vass Enikő

LEHET A FEJLESZTÉS ÁTGONDOLT ÉS ZÖLD IS EGYBEN

Tudatos felkészülés a jövőre

Ma már rengeteg tényezőt kell számításba vennie egy cégvezetőnek. Ehhez a listához most csatlakozik egy, már régen ismert terület, a környezetvédelem egészen új ága. Lehet szoftvert fejleszteni és üzemeltetni „zölden" is – csupán előre gondolkodás és a jövő kihívásainak helyes értékelése szükséges hozzá.

Környezetünk megóvása, a karbonlábnyomunk és az energiafogyasztásunk csökkentése a mindennapjainkban már jól megszokott jelenség. „Azonban mondjuk egy korszerű, minimális elektromos energiát fogyasztó mosogatógép beszerzésénél és használatánál jelentősen összetettebb ez a kérdés a vállalati szoftverek területén", emlékeztetett *Schramm Károly,* a MIKRUM Business Development Managere.

Az informatika egyre inkább szem elé fog kerülni. Egyelőre – a felmérések szerint, hasonlóan a környezetvédők célkeresztjébe került légiközlekedéshez –, a globális károsanyag-kibocsátás 3 százalékáért felel ez az iparág. 2040-re ez az arány egyes becslések szerint akár 14 százalékra is felszökhet. Ahogyan például a járművek vagy a már említett légiközlekedés is egyre komolyabb korlátozásokkal és szankciókkal, büntetésekkel kénytelen együtt élni, hasonlóan fokozatosan szigorodó szabályozói környezetre lehet és kell is számolni a következő 5-10 évre tervező cégvezetőnek.

„Ahhoz, hogy a zöld szempontokat sikeresen be lehessen építeni egy-egy fejlesztésbe, és valódi, mérhető előnyöket érjünk el ennek segítségével, sok mindenre van szükség", tette hozzá a szakember. Legelsőként arra, hogy a felsővezetés is megértse, hogy erre szükség van. Ezt a belátást több aspektus is segíti, például a piaci nyomás. Felismerhető tendencia ma már, hogy egyre fontosabbá válik a cégek valós „zöld teljesítménye", legyen szó akár a marketingről, a fogyasztói megítélésről, akár a fiatal munkatársak toborzásáról vagy megtartásáról. Emellett nem szabad elfelejteni az elmúlt esztendők meglehetősen hektikus energiapiaci folyamatait – így a céges áramszámla összegeit – és a horizonton már kirajzolódó, szigorodó szabályozói elképzeléseket.

FORRÁS: MIKRUM

SCHRAMM KÁROLY, MIKRUM

A „zöldítés" egy folyamat, amelyet az adott cég folyamatait alaposan átgondolva már most el kell indítani.

„De van lehetőség érdemben előre tervezni és lépni is", hangsúlyozta Schramm Károly. Méghozzá a tudatosságot az előtérbe helyezve. A „zöldítés" egy folyamat, amelyet az adott cég folyamatait alaposan átgondolva szükséges elindítani – méghozzá most. Az informatikai fejlesztési folyamatok gyorsasága miatt nagyvállalati környezetben ma hozzuk meg azokat a döntéseket, amelyekből 1-2-3 év múlva lesz működő, letesztelt, a termelésben, szolgáltatásban használatban lévő rendszer. És ez csak az életciklus eleje: az a cél, hogy a most megalkotott szoftverek, rendszerek ne csak 3 év múlva, hanem a már említett 5-10 éves időtávlatban is hatékony és minél inkább energiatakarékos megoldásokként hozzanak üzleti hasznot.

És mik a konkrét szakmai aspektusai a zöldítésnek? Az alkalmazások takarékosabb adatkezelése, optimális algoritmusok, a helyzetnek megfelelő platform és programozási nyelv (!) kiválasztása. Emellett a funkcionalitás és bővíthetőség ésszerű kezelése. Számos eszközünk lehet, de ezek részletesebb kifejtése túllépi a cikk terjedelmi kereteit.

Ehhez viszont már most kell előre gondolkodni, és a felmerülő kérdésekre helyes és zöld választ adni. Rengeteg a változás, a bizonytalansági tényező: a piac változásai, a marketingérték előtérbe kerülése, a szabályozó hatóságok lépései, az esetleges vevői nyomás, a költségszerkezet átalakulása – vagy „csak" éppen az egyre növekvő energiaigény miatt felszökő áramár.

A jó vezető súlyozni is tud, hiszen minden fejlesztés célja az üzleti előny biztosítása. Azt azonban már ma fel kell ismerni, hogy a zöld szempontokat is figyelembe vevő fejlesztések már középtávon is konkrét előnyöket hozhatnak az azokat okosan bevezető és alkalmazó cégeknél. A tudatosság „zöldben" is kifizetődő. ■

Neuron Software Takeover – a módszertan, amely a vállalatok fenntarthatóságát biztosítja

A Neuron Software közel 50 főből álló szakértői csapatával és több mint 26 éves szakmai tapasztalatával felvértezve veszi át részlegesen vagy teljeskörűen az egyedi szoftverek támogatását akár a legmagasabb banki szolgáltatási elvárásoknak is megfelelve, majd fenntarthatóan üzemelteti, támogatja azokat. A módszertanról *Mórocz Mátéval,* a Neuron Software kommunikációs vezetőjével beszélgettünk.

A Neuron Software kutatásainak alapján a pénzügyi szektorban akár 300-600 rendszer is üzemelhet, de egy-egy nagyvállalat akár ezres nagyságrenddel birkózik meg. Ezek közül évente több is kerülhet abba a helyzetbe, hogy veszélyeztetetté válik a támogatása. Annak ellenére, hogy egy csapat akár több rendszer támogatását is képes ellátni, belátható, hogy a vállalatonként több százas rendszerállomány mögé nem juthat megfelelő számú szakértő. Sokféle okból fordulhat elő, hogy a támogató személy vagy szervezet váltani szeretne (megszűnik a motiváció, nem akar régi technológiákkal dolgozni, túl nagy már a felelőssége, új kihívásokat keres, közeleg a nyugdíj stb.)

A pénzügyi szektorban gyakori, hogy 15-20 éve kialakított rendszerek támogatását még ma is meg kell oldani: sok esetben kiválóan megírt szoftverekről van szó, amelyek nem igényelnek állandóan nagy ráfordításokat, azonban ettől függetlenül ott kell legyen mögötte valaki, aki probléma vagy az üzleti, jogi környezet változása esetén beavatkozhat, és tudja, mit kell csinálni. „Ha az említett szakember távozik, akkor ott állunk, hogy adott egy rendszer, amely mögött már nincsen megfelelő tudás és munkaerő ahhoz, hogy biztonságosan üzemeltethető legyen”, vázolja a szükséghelyzetet Mórocz Máté.

Ilyenkor el kell dönteni, hogy mi legyen a sorsa: újraírás, kiváltás vagy átvétel. „Hisszük, hogy ezeket a rendszereket nem kell minden esetben azonnal kidobni majd újraírni, vagy éppen lecserélni egy újra: elkerülhető, hogy hatalmas erőforrások felhasználásával, hosszas fejlesztési idő alatt új rendszerek kifejlesztésével legyen szükséges megoldani az üzletkritikus folyamatokat működtető szoftverek támogatását. A fenntarthatóságot tűztük ki célul: a módszertanunk szerint a rendszerek megtarthatók, és kiváló szolgálatot tudnak tenni a cég számára”, ismerteti a Neuron Software alap hozzáállását Mórocz Máté.

Minden eset a rendszer átvilágításával indul, ami nagyjából egy hónapig tart. „Feltárjuk a kockázatokat és problémákat: analízist végzünk, megvizsgáljuk, hol találhatók a sérülékenységek, valamint konkrét cselekvési tervet állítunk össze a legmagasabb prioritású feladatoktól az alacsony kockázatúakig”, részletezi a folyamatot. A szakértői elemzési anyag nem ritkán 50-60 oldalas, ezt összefoglalva, prezentáció formájában be is mutatják a vezetőknek és szakértőknek egyaránt.

Mindez az ügyfél számára azonnali értéket képvisel, hiszen innentől kezdve kristálytiszta alapokon nyugvó döntést tud hozni a rendszer sorsával kapcsolatban: a saját kollégáival hozza helyre azt, és továbbfejleszti, támogatja a jövőben a rendszert, vagy olyan szakértőkre bízza, akik az ilyen helyzetek megoldására specializálódtak. De ha a cselekvési terv végrehajtásához van elegendő anyagi és szakmai erőforrása, akár maga az ügyfél is képes a szoftver normalizálására, elkerülve a szállítótól való esetleges függőséget.

FORRÁS: NEURON SOFTWARE

MÓROCZ MÁTÉ, NEURON SOFTWARE

Az ügyfelek 50%-a a Neuron általi átvételt választja. Ilyenkor egy hónap alatt a Neuron Software átveszi a kódot, hogy minden feltétel biztosított legyen a rendszer helyreállításához, fejlesztéséhez. Majd feladatok prioritásai mentén haladnak abban, hogy a rendszer stabilan, az elvárt biztonsági kritériumoknak megfelelően tudjon működni, és a szakértő csapat folyamatosan biztosítja a rendszer támogatását.

„Az elmúlt években több mint 50 sikeres Software Takeover projektet hajtottunk végre. Magabiztosan jelenthetem ki, hogy képesek vagyunk részlegesen hibrid együttműködésben a belső csapatokkal, de akár teljeskörűen is átvenni a vállalati egyedi szoftverek támogatását, és akár a legmagasabb banki szolgáltatási elvárásoknak is megfelelve, fenntarthatóan működtetni azokat”, mondta. Móricz Máté. ■

A Neuron Software közel 50 fős csapatában megtalálható a szoftverfejlesztési életciklus minden folyamatához szükséges szakértői erőforrás, köztük a projektmenedzser, architect, üzleti elemző, szoftverfejlesztő, tesztelő, DevOps, üzemeltetési szakértő-, és támogató egyaránt, szenior, medior és junior szinten.

STRATÉGIA BLOKK

Mi van a motorháztető alatt?

Ma már a vállalati ügyfelek is elvárják, hogy számukra is minél több digitális felület és szolgáltatás legyen elérhető, Ennek azonban előfeltétele az, hogy a pénzintézetek „rendbe tegyék" saját core rendszereiket is, illetve tovább erősödjön és bővüljön a fintech-cégekkel folytatott együttműködés. Digitalizálni kell – csak nem mindegy, hogyan.

Az ügyfél volt a középpontban a Finance & Technology 2024 első, „Stratégia" nevet viselő blokkjában. Nem véletlenül: legyen szó vállalati vagy fogyasztói szektorról, az elvárások egyre nőnek mind a bankokkal, mind a fintech-cégekkel szemben, emelte ki *Szombati Anikó*, a Magyar Nemzeti Bank ügyvezető igazgatója. Ma már minden ügyfél számára alapvetésnek számít, hogy nem kell mindenért személyesen elmenni egy bankfiókba vagy a biztosító ügyfélszolgálatára: rendelkezik már egyfajta digitális identitással, amivel biztonságosan képes azonosítani magát a különböző ügyintézési folyamatokban, tette hozzá *Jeney Gábor*, a Comnica ügyvezetője. A területnek újabb jelentős lendületet adhat a Nemzeti Digitális Állampolgársági Program is: az ügyintézés-központúság helyett az élethelyzet alapú megoldások keresése azonban a pénzügyi piac ügyféltudatos szereplői számára ez már korábban „alapműködésnek" számított.

Nicsak, ki beszél a túloldalon?

A mesterséges intelligencia megjelenése és várható elterjedése új kihívásokat támaszt mind a szabályozó hatóságok, mind az IT-piac fejlesztői, beszállítói és felhasználói elé. A nagy adatbázisok nemcsak adatvagyont jelentenek, de komoly veszélyforrást is, figyelmeztetett Szombati Anikó: az öntanuló mechanizmusok a tapasztalatok szerint részrehajlóvá és diszkriminatívvá is válhatnak. El kell kerülni, hogy ezek eredményeként egyes fogyasztói csoportok kizáródjanak a szolgáltatások fókuszából, tette hozzá az MNB ügyvezetője.

Az MI valóban kiemelt téma, de csak az egyike a feltörekvő trendeknek, jegyezte meg *Schramm Károly*, a MIKRUM üzletfejlesztési vezetője. Hasonlóan jelentős hatású a digitalizáció is, amelynek egyik hatása a folyamatosan növekvő komplexitás és az absztrakciós szint. De nem mindegy, hogy mikor mit választunk: teljesen egyedi, a low-code/no-code megoldások, illetve a kész vagy dobozos rendszerek testre szabása is megoldás, ha okosan választunk.

„De válasszon bármit is a megrendelő, fejlesztőre szükség lesz", hangsúlyozta *Bodrogközi László*, a Neuron Software ügyvezetője. Számtalan rendezvényen került elő a kérdés: az egyébként jól működő, a vállalat folyamatait kiválóan kiszolgáló rendszer mögül hova tűntek el a fejlesztők? Ráadásul a pénzügyi szektor ilyen szempontból az átlagosnál is speciálisabb, hiszen nem csupán az üzleti folyamatok leállása miatti, jelentős veszteségekre kell számítani, hanem a szabályozó, felügyelő szervezetek figyelmére és komoly összegű bírságára is, figyelmeztetett. A probléma az, hogy egyre drágább és ritkább a jó munkaerő, tette hozzá Schramm Károly. A platformok okosodnak, fejlődik az MI is, de bizony a nap végén még mindig az ember fogja kiválasztani

SZOMBATI ANIKÓ, MAGYAR NEMZETI BANK

JENEY GÁBOR, COMNICA

SCHRAMM KÁROLY, MIKRUM

BODROGKÖZI LÁSZLÓ, NEURON SOFTWARE

DR. PINTÉR ÉVA, CORVINUS FINTECH CENTER; HOFFMANN BENCE, SHIWAFORCE; SCHRAMM KÁROLY, MIKRUM; PERECZES JÁNOS, MBH BANK; FÁYKISS PÉTER, MNB DIGITALIZÁCIÓS IGAZGATÓSÁG; FISCHER ANDRÁS, OTP BANK

az irányokat és megoldani a felmerülő problémákat. Ráadásul ma még eléggé kevés az olyan tartalom, ahol a mesterséges intelligenciát jól használják, ahol megfelelő szerepet kap az MI a folyamatokban, jegyezte meg Jeney Gábor.

Okos, de eszköz

Lehet, hogy a mesterséges intelligencia funkcionalitásban nagyon sokat tud adni, kitágítva a lehetőségeket, de ahhoz, hogy új terméket és szolgáltatást fejlesszünk, igenis kellenek a fejlesztők, kellenek a cégek: a bankok, a fintech-ek és persze a szabályozók is. Az emberi erőforrást nem lehet megkerülni, és nem kell attól sem félni, hogy „jön az MI, és elveszi" a kapacitásokat, a munkát bárkitől. Eszközként kell rá tekintenünk és arra kell koncentrálni, hogy miképp tudjuk használni ezeket az MI adta lehetőségeket, hangzott el a blokkot záró kerekasztal-beszélgetésen.

Könnyű akkor digitalizálni, ha nincs régi, az üzleti folyamatok szempontjából kritikus fontosságú rendszer a képben, jegyezte meg *Pereczes János*, az MBH Bank ügyvezető igazgatója. A hagyományos bankok többségénél még nem az MI bevezetése a jelen kihívása, hanem az, hogy hogyan tud egyensúlyt teremteni a legacy és az új üzleti modell, így a régi rendszereket üzemeltető és az új technológiában jártas tehetségkultúra között. Ez azonban nem jelenti azt, hogy nem kell figyelni a mesterséges intelligenciára. Nemrég egy másik beszélgetésen, én is amellett tettem le a voksomat, hogy most vagyunk a hype-görbe tetejének közelében, tette hozzá *Fischer András*, az OTP Bank Innovation Tribe vezetője. De ez egy szükségszerű dolog: a „túlfújásra" szükség van ahhoz, hogy megérkezzenek azok a felső vezetői támogató döntések, erőforrások, melyek segítségével a soron következő kiábrándulás után végül beállhat az a produktivitási szint, amely hosszú távon meghozza az eredményeket, és a befektetések meg is fognak térülni.

A digitalizációra leginkább alkalmas a bankszektor

Ha belegondolunk, a szektorban semmilyen fizikai jószág nem mozog, gyakorlatilag „csak" számokkal dolgozunk, emelte ki *Fáykiss Péter*, az MNB Digitalizációs igazgatóságának igazgatója. Azt azonban látni kell, hogy bár a hazai bankok már foglalkoznak az MI implementációjának kérdésével, de még a legtöbb intézménynél nincs erre egy elfogadott, egységes stratégia. De akad jó hír is: a legtöbb szereplő nagyon komoly potenciált lát abban, hogy a szakemberhiányt akár belsős képzésekkel, akár egyéb folyamatautomatizációs megoldásokkal kezelni tudják. Az MNB elég komoly hatékonysági tartalékot lát még a hazai intézmények körében, tette hozzá.

A hatékonyság más területeken is előtérbe kerül: Schramm Károly példaként a környezettudatosságot emelte ki. Mint hangsúlyozta, az angolszász országokban már egyre komolyabb trendet jelent fejlesztőként a zöld energia hatékony használata. Csak annyit fejlesszünk, csak olyan kódokat futtassunk, amennyire és amilyenre valóban szükség van. A zöld átállásban a szabályozói hatóságnak is nagy szerepe van. Az MNB az egyik legelső jegybank, ahol külön csapat dolgozik a fenntarthatósággal. „Nálunk emiatt az összes digitális fejlesztésnél figyelembe veszik a zöld szempontokat is", tette hozzá Fáykiss Péter.

Minden változik és változáson belül is folyamatosak a hangsúly-eltolódások. Az elmúlt három évben a digitálisan aktív lakossági ügyfelek száma 27 százalékkal, míg a kkv-ké 19 százalékkal nőtt. Ha azonban a csatornamegoszlást vesszük górcső alá, akkor egyértelmű a böngészős internetbank részesedésének egyértelmű csökkenése. Ma már a digitálisan aktív ügyfelek teljes csoportján belül 78 százalék okostelefont és azon futó applikációt használ. A „mobil first" részben organikus trend is, de a pénzintézetek is errefelé terelik az ügyfeleket. ■

BIZTONSÁG BLOKK

Állóháború

Mindenki veszélyben van, de a bankok, pénzintézetek különösen vonzó célpontot jelentenek a kiberbűnözők számára: nemcsak az ügyfelek pénze, hanem személyes adataik is csábítóak. A védekezést nehezíti, hogy a támadások zöme már személyre szabott, és villámgyorsan megtörténik.

Az első megszólaló *Ádám Zoltán,* a Palo Alto Networks Regional Sales Managere volt, előadását a felhőszolgáltatásokkal foglalkozó nemzetközi felmérésekkel gazdagította. A felhőszolgáltatások a jelen meghatározó jellemzői és a jövőt is jellemezni fogják a magyar bankszektor számára. A fintech-cégeket érintve elmondta, hogy példátlan módon felgyorsultak a fejlesztési folyamatok. A Forrester szerint ezen cégek 77 százaléka heti rendszerességgel indít új alkalmazást a felhőben. A generatív MI pedig a DevOps-teamek munkasebességét képes akár megtízszerezni

A generatív MI sötét oldalát bemutatva elmondta, sok helyen használnak nyílt forráskódú szoftvereket, amelyek jelentős része, több mint 80 százaléka tartalmaz valamilyen sebezhetőséget. „A generatív MI-ről az is elmondható, hogy a hackerek ma már 15 percen belül fel tudnak törni egy napvilágra került sérülékenységet", figyelmeztetett Ádám Zoltán.

Az előadást kerekasztal-beszélgetés követte *Bagó Péter* a Corvinus egyetem adjunktusának moderálása mellett, „Veszélyek mindenütt" címmel. A résztvevők a már bemutatott Ádám Zoltán, *Kincses Zoltán* a Radar Payments információbiztonsági vezetője, és *Zala Mihály,* az EY Magyarország partnere voltak. A kerekasztal során a bankokra, fintechekre és biztosítókra leselkedő leggyakoribb kiberbiztonsági kockázatokat elemezték.

Zala Mihály elmondta, hogy míg Magyarországon egy átlagos betörés 15 percig tart, a különböző statisztikák szerint – attól függően, hogy milyen támadási potenciál rejlik egy-egy cég felkészületlensége, vagy alkalmi hibái mögött – egy kibertámadás öt perctől két hónapig bármilyen hosszú időt igénybe vehet. A legnagyobb probléma az, hogy a támadások zöme személyre szabott, és amit a hazai cégek nem igazán tudnak elképzelni, azok a versenytársak által megrendelt támadások. Vannak azonban sok helyütt olyan kollégák, akik időnként a legális, időnként pedig a „dark" világban közlekednek, és képesek ilyesmire. Zala Mihály mellettük még a beszállítókat említette, amelyeknek van hozzáférésük a céges rendszerekhez, így nagyon sok támadás akarva-akaratlan felőlük érkezik.

Kincses Zoltán a helyzet jobb megértéséhez a MITRE ATT&CK® frameworköt ajánlotta böngészni egy sikeres támadás összetettségének megértéséhez. „A támadók gyakran heteket, hónapokat beleölnek az előkészítésbe, szervezetten dolgozva, akár belső embereket is felvéve a műveletbe, majd maga a támadás lehet 15 perc, de akár három másodperc is, az azonnali átutalásnak köszönhetően, amibe még a fraud monitoring is belefér", mondta a szakember.

Ádám Zoltán konkrét esetet említve egy olyan célzott támadást ismertetett, ahol csak az mentette meg a pénzügyes kolléganőt az ügyvezetőtől kapott hamis email-üzenet nyomán történő átutalástól, hogy nem volt elegendő összeg a számlán, így meg kellett kérdeznie az ügyvezetőt, hogy akkor honnan utaljon – így derült ki a csalási kísérlet. „Ezeket a célzott támadásokat nagyon nehéz megfogni", mondta el Ádám Zoltán. ■

ÁDÁM ZOLTÁN, PALO ALTO NETWORKS

DR. BAGÓ PÉTER, CORVINUS EGYETEM; ÁDÁM ZOLTÁN, PALO ALTO NETWORKS; KINCSES ZOLTÁN, RADAR PAYMENTS; ZALA MIHÁLY, EY MAGYARORSZÁG

COMPLIANCE BLOKK

A biztonság ára

A közös munka a megfelelőség területén is alapfeltételnek számít a mindenki számára megfelelő végeredményhez. A jó szabály segítség – ha megfelelő javaslatokra, visszajelzésekre is alapozva lehet felépíteni.

„2021-ben az Európai Unión belül 5,5 milliárd eurós kárt okozott a kiberbűnözés – így gazdaságilag is igen fontos az eredményes kibervédelem kiépítése", hangsúlyozta *Dr. Pataki-Vízi Linda*, a PR-AUDIT ügyvezetője. Ennek az óriási számnak két fő oka azonosítható. Egyrészt a kritikus sérülékenységek száma is igen magas az Unión belüli cégeknél, szervezeteknél, sőt, a magánszemélyeknél is, másrészt a felhasználók egyszerűen nem rendelkeznek alapszintű biztonságtudatossággal sem. A biztonsági kockázatok azonban jóval nagyobbak pusztán a pénzügyi költségeknél: az egész társadalom szintjén jelentkező probléma ez, tette hozzá

Érthető tehát, ha az Európai Unió is megfelelő szabályozórendszert igyekszik felépíteni: ennek egyik igen fontos eleme pedig a pénzügyek digitális működési rezilienciájának megőrzésére dedikált keretrendszer, a DORA (Digital Operational Resilience Act). A rendelet mellé szigorú menetrend is érkezett: 2025. január 17-től alkalmazni is kell a rendelet előírásait. Igaz, a szakma ma még vár a végleges végrehajtási szabályok megjelenésére. Az viszont már biztos, hogy a DORA öt fő pillérének egyike a digitális működési reziliencia vizsgálata, legyen szó alap- vagy fejlett tesztelésről. „Nagyon fontos lenne", emelte ki a szakember, „hogy ne csak magának a tesztelésnek az eredményét vegyük tudomásul, hanem ez illeszkedjen egy olyan keretbe vagy folyamatba, amely az eredmények feldolgozását jelenti."

A szabályokból azonban néha túl sok is lehet. *Buró Szilárd*, az Equilor pénzügyi innovációs vezetője szerint az elmúlt évek során már a túlszabályozottságot lehet érezni – ennek egyik eredménye a complinace területen mozgó kollegák számának jelentős megemelkedése a cégen belül. Mind az EU részéről érkeznek a jogszabályok, mind a Magyar Nemzeti Bank szabályozóként alakít ki olyan környezetet, amelynek meg kell felelnie a piac szereplőinek. A „szabályrengeteg" láttán az sem véletlen, tette hozzá *Dr. Vajda Viktor*, a Neumann Nonprofit Közhasznú Kft. ügyvezetőigazgató-helyettese, hogy a Digital Europe manifesztuma is azt javasolja az Európai Bizottság számára, hogy a jövőben a deregulációs törekvések mentén végezzék a jogszabályalkotási tevékenységet.

A jó, hatékony és egyszerűen alkalmazható jogszabályok megalkotásához a szabályozó hatóságok, az iparági szervezetek és a piac párbeszédére van szükség, hangzott el a blokkot záró kerekasztal-beszélgetésen.

„Sok meglepetéssel találkoztunk mi is a szabályozói oldalról", tette hozzá *Vidákovics Attila*, a DLabs/Mosaic Alpha alapítója. „Ha van valami, ami nem szeretnék lenni, az a szabályalkotó", tette hozzá, hiszen elképesztően nehéz dolguk van. Példaként említette a kripto területét: a decentralizált világban is szükség van megfelelő jogszabályi keretekre, hiszen rengeteg támadást és csalást szenvednek el a felhasználók.

Az egyre merevebb jogszabályok a kártyaelfogadó cégek életét is érintik, jegyezte meg *Kiss László*, a HelloPay üzletfejlesztési és értékesítési igazgatója. Egyre komolyabb kritériumoknak kell megfelelniük, főleg, ha az EU határain kívül is szolgáltatnak. Komoly kihívást jelentett például a kínai WeChat Pay-jel történő magyarországi fizetések kimenő adatforgalmának GDPR-kompatibilis kezelése.

DR. PATAKI-VÍZI LINDA, PR-AUDIT

DR. PINTÉR ÉVA, CORVINUS FINTECH CENTER; BURÓ SZILÁRD, EQUILOR; KISS LÁSZLÓ, HELLOPAY; DR. VAJDA VIKTOR, NEUMANN NONPROFIT KÖZHASZNÚ KFT.; VIDÁKOVICS ATTILA, DLABS/MOSAIC ALPHA

PARTNEREK BLOKK

Csapatmunka minden területen

A verseny mellett az együttműködés is központi szerepet kap a pénzügyi szektor jelenében, de még inkább a jövőjében, hangzott el több területtel összefüggésben a 2024 Finance & Technology konferencia „Partnerek” blokkjának kerekasztal-beszélgetései során. Az is kiderült, hogy kevés a jogszabályok jelentette keret: ha a bankok nem fejlesztenek – akkor nem lesz ügyfélélmény sem.

A jövő sokszínű lehet és lesz is: erre taníthat minket az elmúlt 15-20 év fintech-történelme, emelte ki *Ács Zoltán*, a Magyar Fintech Szövetség elnöke és az MBH Fintechlab ügyvezetője. Ma már a csapatmunka a jellemző: a „hagyományos” bankok és a fintech-cégek, akár startupok is együttműködnek. is. Ez a jövő iránya is: kooperáció és a B2B-fintech elterjedése, ami egyben komoly kihívást is jelent majd a pénzügyi rendszerben.

„A korszakalkotó ötletek mellett láttunk jelentős pénzégetéseket is”, tette hozzá *Tresch András*, a Quattrosoft ügyvezetője, ezért érthető a befektetők óvatossága is. Ez azonban nem jelenti azt, hogy nem lehet okosan fejleszteni, emelte ki *Horányi Gergő*, a Wise termékigazgatója, aki szerint jól látható, hogy merrefelé mozdul tovább a pénzügyi világ. Az együttműködés mellett a legfontosabb irány az, hogy egyszerre figyelni kell a felhasználókra, adataikra és igényeikre egyaránt. Transzparencia, az azonnali pénzmozgás lehetősége, kényelem, alacsony költségek – ezek határozzák majd meg mind a bankok, mind a fintech-cégek jövőképét.

„A jövőhöz azonban a múlt is csatlakozik, néha egészen meglepő módon”, tette hozzá *Bodrogközi László*, a Neuron Software ügyvezetője. A bankokra jellemző az akár több évtizedes legacy rendszerek használata, amelyeket valahogy „össze kell fésülni” a fintech-ekkel és a felhasználók által igényelt szolgáltatásokkal. Itt is az együttműködés lesz a kulcs: nagyon könnyen használható szolgáltatások és a nagyon szigorú szabályok között kell megtalálni a dinamikus egyensúlyt.

Verseny és együttműködés

A jövőt a „nagy csapat” minden tagjának - bankok, fintech cégek, felhasználók - az jelenti majd, ha a digitalizáció, a mesterséges intelligencia észrevétlenül beépül a tranzakciók folyamatába. Nagy verseny várható, hiszen mindenki a legjobb megoldást igyekszik nyújtani ügyfeleinek. Ehhez az adatok jelentik a kulcsot: sok adat egyenlő jól ismert és a lehető legjobban kiszolgált ügyfél. Sokan mondják azt is, hogy a készpénz előbb-utóbb eltűnik, de ez hosszú folyamat lesz, emlékeztetett *Németh Balázs,* a K&H Bank innovációs vezetője. Nehéz most megmondani, hogy a jövőben mivel fogunk fizetni: a számlapénztől a kripto-megoldásokon keresztül széles lehet a választék. Egy dolog azonban biztos: egyszerűbb és könnyebb lesz mindez. Az MI segítségével a tranzakciók úgy épülhetnek be a folyamatokba, hogy szinte észre se vesszük. Minden digitalizáltabb lesz, de nem minden lesz digitalizált:

DR. BAGÓ PÉTER, CORVINUS EGYETEM; NÉMETH BALÁZS, K&H BANK; BODROGKÖZI LÁSZLÓ, NEURON SOFTWARE; HORÁNYI GERGŐ, WISE; TRESCH ANDRÁS, QUATTROSOFT; ÁCS ZOLTÁN, MAGYAR FINTECH SZÖVETSÉG / MBH FINTECHLAB

GYIMESI ISTVÁN, CARDINAL

DR. BAGÓ PÉTER, CORVINUS EGYETEM; FODOR ANDREA, PROJEKTCOACH CONSULTING; FÓRIZS ISTVÁN, OTP MOBIL; KÁRAI ANITA, HUMANFIELD; MÉRŐ GÁBOR, TRIVE BANK

a komoly döntéseknél továbbra is tanácsadásra, emberi kapcsolatra lesz szükségünk. A mindennapi életben viszont digitális, személyre szabott, azonnali megoldásokra számíthatunk.

Ha a Központ leszól

„40 évig próbálkoztunk a tervgazdasággal, tudjuk, hogy nem működik”, emelte ki előadásában *Gyimesi István*, a Cardinal fejlesztési vezetője. A központi feladatmeghatározás, -leosztás, a mutatók „odafenti” meghatározása azt eredményezte, hogy a szervezetek nem voltak motiválva azok teljesítésében, megvalósításában. A szakember hasonlóan problémásnak tartja az EU Payment Services Directive (2015/2366, PSD2) direktíváját: a pénzügyi szektor központi irányítása ugyanezeket a problémákat hozza elő.

2018-19-ben, a PSD2 bevezetésekor a fintech területén volt egy jelentős felfutás: sokan bennük látták a jövőt. Ma már viszont látható, hogy a szabályozóval elindítani vágyott forradalomból sok minden nem lett. A nyílt bankolás szabályozásának jelenlegi formája miatt például a több mint 5000 európai bank egyedi XS2A-implementációval rendelkezik – az EU-s piacra belépő fintech-cégeknek így bankonként kell integrálni saját megoldását.

A megoldást itt is az együttműködés hozhatja el. Gyimesi István szerint a pénzintézetek és a fintech-szereplők is rájöttek arra, hogy ha közösen gondolkodnak, dolgoznak, és együtt hoznak létre olyan megoldásokat, amelyek mindkét félnek jók, akkor mindketten motiváltak lesznek a hasznos szolgáltatások bevezetésében. És végső soron pont ez a jó az ügyfélnek is.

A szakember a kerekasztalon már említett legacy systemek problémáját érintve a banki oldalon kialakítható, megfelelő kiszolgáló réteg fontosságát hangsúlyozta. Ezt már képes kívülről „megszólítani” a fiatal fintech rendszerfejlesztő szakember is, így kinyithatók lehetnek a banki szolgáltatások és az ügyféladatok is. Stabilitás, kiszámíthatóság – ezek a kulcsfontosságú tényezők.

Az új technológiák új tudású szakemberek iránt teremtenek igényt, új pozíciók nyílnak meg a cégeknél. Mindenki jól ismeri a bankszektorban végbemenő változásokat, a a digitalizáció irányába fordulást, emelte ki *Kárai Anita*, a HumanField üzletfejlesztési igazgatója. Három olyan kiemelt terület azonosítható, ahol nagyon megnőtt a tapasztalt szakemberekkel szembeni igény: az IT-biztonság, az adat és a mesterséges intelligencia. A toborzás szempontjából ma már a bank inkább egy IT-cégre hasonlít, hiszen rengeteg biztonságtechnikával foglalkozó szakemberre van szükség: IT-auditor, etikus hekker, biztonságtechnikai rendszergazdák kellenek. Emellett az adatokkal foglalkozó szakemberek (data engineering, data scientist, üzletiintelligencia-elemző) iránti kereslet is rohamosan nő. Nem juniorok, hanem szenior szakemberek vannak a célkeresztben,

Új idők, új skillek

Nemcsak szaktudásra, de még inkább olyan képességekre, készségekre van szükség, mint amilyen a kritikus gondolkodás, a folyamatokban gondolkodás, az ellentmondások kiszűrésének képessége, tette hozzá *Fodor Andrea,* a Projektcoach Consulting ügyvezetője. Az ilyen embereket azonban nem egyszerű bevinni a csapatba, a szervezetbe.

„Ha a cégnél nálam nincs meg a megfelelő tudás, honnan tudom, hogy az érkező ember jó vagy nem?”, tette fel a kérdést *Mérő Gábor*, a Trive Bank IT-igazgatója. Hogyan lehet megállapítani, hogy a keresett tudás tényleg benne van meg és pont az ő tudására van szükség? Az új tudások területén, az új generációs kollégáknál nagy kérdés, hogyan illeszthetőek be a cégkultúrába, a már meglévő csapatunkba?

Az együttműködésre, azaz az fejlesztők és az üzemeltetők közös munkájára épül a DevOps is. Bár ez már egy több éves folyamat, de sok helyen még csak keresik a helyét, a határait, tette hozzá *Fórizs István*, az OTP Mobil SimplePay IT-vezetője. Nincs helye az elkülönülésnek: csapatmunkára van szükség. Meg kell teremteni – és nem csak a banki szektorban – a DevOps-os mindset kultúráját.
A már említett hard skillek mellett azonban még ma egyre fontosabbá válik a soft skill. A technológiákat ugyanis meg lehet tanulni, de fontos, hogy a „józan paraszti ész” is meglegyen mellette. A szakember tudjon kérdezni, legyen kritikus a gondolkodása, de így a kapott válaszokat se fogadja el feltétel és kritika nélkül! Sajnos, ezt a legnehezebb megtalálni és megtartani is. ■

FORRÁS: FREEPIK.COM

A HASONLÓSÁG MEGÍTÉLÉSE KOMOLY TUDOMÁNY

Védjegyből üzleti érték

A védjegykutatás és -védelem nem felesleges luxus – már a vállalkozás létének első pillanatától súlyos milliókat lehet megtakarítani a használatával, a későbbiekben pedig segíthet megvédeni a nehezen kivívott üzleti pozíciókat.

Új vállalkozást indítunk, kitaláltunk egy jól hangzó, könnyen megjegyezhető nevet termékünknek, szolgáltatásunknak. Gyors ellenőrzés: nincs ilyen cégnév bejegyezve Magyarországon, a doménnév is szabad, csapjunk hát bele! Bejegyeztetjük a céget, lefoglaljuk a domént, létrehozzuk a közösségimédia-csatornákat, felépítjük a marketingkampányt, elköltünk több (tíz)millió forintot. Majd egyszer csak kapunk egy levelet, hogy az általunk használt elnevezés összetéveszthető egy, már évek óta a piacon lévő másik cég védjegyével, ez bitorlás, azonnal hagyjunk fel a jogsértő tevékenységgel: változtassuk meg az elnevezést. Eddigi erőfeszítéseink, a milliók mennek a levesbe, vállalkozásunk kezdheti elölről a márkaépítést, az arc(ulat)vesztésről nem is beszélve.

Mindenhol keresni kell

„A fenti szcenárió egyáltalán nem a képzelet műve, hanem jó pár konkrét megtörtént eset valós leírása”, figyelmeztet *Hennelné dr. Komor Ildikó,* a Komor Hennel Attorneys ügyvédi iroda irodavezető ügyvédje. Ezért is fontos, hogy a cégalapítás (és később a termékfejlesztés) folyamatába már a legelején beépüljön a védjegykutatás. „Nem elég a cégnyilvántartásban vagy a Google-ban keresgélni az azonos cégneveket. Lehetnek olyan apró eltérések, amelyek esetében megáll az összetéveszthetőség lehetősége, és mivel a cégnév-hasz-

nálattal is megvalósulhat az engedély nélküli védjegyhasználat, ilyenkor a másik fél jó eséllyel nyerhet meg egy védjegybitorlási pert. Sok nemzetközi védjegy hatályos Magyarországon, amit csak speciális kutatással lehet felderíteni", mondja arról, miért kell már a nulladik pillanattól kezdve foglalkozni a védjegyekkel. Több adatbázis is van, de a frissítések nem minden esetben naprakészek, és lehetnek eltérések is, Hennelné dr. Komor Ildikó szerint érdemes minden egyes adatbázist végigböngészni. *(Lásd a „Védjegy-adatbázisok" keretet!)* Amikor távoli, más írásrendszert használó országok védjegyeit kell ellenőrizni, a magyar ügyvédi iroda helyi partnereket hív segítségül.

A hasonlóság fokai

Ezekben az adatbázisokban bárki böngészhet és kereshet védjegyeket – a végeredmény akár egy hosszú lista is lehet, amely az egyezőségeket mutatja. A védjegyoltalom azonban nemcsak egyezőségre terjed ki, hanem (szakkifejezéssel élve) az „összetéveszthetőségig való hasonlóságra" is, ami korántsem egyértelmű, figyelmeztet Hennelné dr. Komor Ildikó. Vannak alapelvek, amelyeket mindenképpen figyelembe kell venni.

Ilyen például, hogy minél több karakterben egyezik két szó, minél hasonlóbb az összhatás, annál erősebb a hasonlóság. Ugyancsak védjegyjogi alapelv, hogy a szavak első tagja a hangsúlyosabb – ha az egyezik, és csak az elnevezés második felében/tagjában van kisebb eltérés, az nagyobb fokú hasonlóság, mintha a szavak első fele térne el. Vizsgálni kell a védjegyek formai elemeit is: logó, betűtípus, írásmód szintén tiltott lehet. Számít, hogy mennyire hasonló két elnevezés kiejtése (a fonetikai hasonlóság), illetve az asszociációs hasonlóság is – ha a név jó eséllyel felidéz valami ismert dolgot, az problémát okozhat.

„Számos, különféle paraméterezésű keresést kell lefuttatni, hogy minél nagyobb eséllyel találjuk meg a hasonlónak tekinthető védjegyeket. A gyakorlat itt is rengeteget számít. Nemegyszer előfordul, hogy az ügyfél megkeres bennünket egy elnevezéssel, mi pedig egyből azt tanácsoljuk, hogy találjon ki másikat, mert biztosan rengeteg találat lesz, és nem tudja majd sikeresen használni az elsőre kiválasztott megjelölést", teszi hozzá az ügyvéd.

Áruk és osztályok

Két elnevezés nagyon hasonlíthat egymásra, de ha az egyiket túrafelszerelés, a másikat pedig bioélelmiszerek megjelölésére használják, akkor nem áll fenn az összetéveszthetőség veszélye, eltérő áruosztályokban használható (és bejegyezhető) már oltalom alatt álló védjegy is. De néhány globális brand áruosztályokon átnyúló védelmet élvez, például a Coca-Cola. Előfordulhat, hogy két áru besorolása közel van egymáshoz, még ha szám szerint nem is ugyanabba az osztályba tartoznak, ilyenkor fennáll az összetéveszthetőség esélye.

A szoftverek a 9-es áruosztályba tartoznak, ahol földmérési eszközöktől kezdve a búvármaszkokon át a tűzoltókészülékig rengeteg áru szerepel, és ugyanide sorolandók a szoftvertermékek is. Szinte kötelező tehát az adott áruosztályon belül pontosan megjelölni, hogy milyen szoftvertermékről van szó, milyen feladatot lát el, amelyre védjegyoltalmat igénylünk. Kellően szűk árujegyzék-meghatározással jelentősen csökkenthetjük a kockázatokat, mert egy korábbi, hasonló védjegy jogosultja javarészt ez alapján fogja eldönteni, hogy zavarja-e majd őt a piacon a mi új védjegybejelentésünk, és az ez alatt végzendő piaci tevékenységünk, ez alapján dönt arról, hogy fellépjen-e a bejelentésünkkel szemben.

A saját védjegy érték

A sikeres bejegyzéssel vagyoni értékű jog kerül a vállalkozáshoz, és erős jogi eszközök állnak rendelkezésre ahhoz, hogy a cég fellépjen a bitorlókkal szemben. „Ha már ismertséget szerez egy brand, akkor számítani lehet rá, hogy mások a siker farvizén evezve hasonló elnevezésekkel akarják megkönnyíteni és meggyorsítani a piaci terjeszkedésüket. A védjegy birtokában velük szemben legtöbbször eredményesen lehet fellépni", mondja Hennelné dr. Komor Ildikó. Nemcsak szavakat lehet bejegyeztetni: le lehet védeni ábrákat, logókat, szlogeneket, vagy akár magát a termék csomagolását, és bizonyos esetekben színeket is (lásd magenta), hangokat is (szignált), vagy akár mintákat is.

FORRÁS: KOMOR HENNEL ATTORNEYS

HENNELNÉ DR. KOMOR ILDIKÓ,
KOMOR HENNEL ATTORNEYS

Védjegy-adatbázisok

- **Hazai:** Szellemi Tulajdon Nemzeti Hivatala (SZTNH) e-Nyilvántartása
- **Európai:** EUIPO
- **Globális:** WIPO Global Brand Database.
- A **tmView a**z egyik leghasznosabb: elméletileg tartalmazza a többi adatbázist, beleértve az egyes országok védjegyhivatalainak nyilvántartásait is.

Kockázati tényezők

„Látható, hogy a kutatás sok esetben a munka könnyebbik felét jelenti", mondja az ügyvéd. A találatokat rangsorolni kell: mennyire releváns, mekkora kockázatot jelenthet egy védjegybitorlási per vagy felszólalási, törlési eljárás. Rengeteg tényező határozza meg, mekkora kockázatot jelent egy adott elnevezés használata. A hasonló védjegyet aktívan használja-e a cég, vagy csak bejegyeztette? Milyen vehemensen védi a védjegyeit? Mennyire tér el a két áruosztály? Használja-e Magyarországon a védjegyet?

Mindebből születik egy részletes jelentés, egy jogi szakvélemény, amely tartalmazza a kockázati tényezőket, és ez alapján dönthető el, hogy jogi szempontból mennyire veszélyes a kérdéses elnevezés használata.

Schopp Attila

SZERZŐI JOG ÉS AZ MI

Ki fizeti a gép-észt, kié a legyártott tartalom?

Az MI-szolgáltatások berobbanásával a szerzői jog világa a feje tetejére állt, és bár kívülről talán nem látszanak a mindent átalakító folyamatok, könnyen lehet, hogy a holnap jogrendszerére rá sem ismerünk majd. A valószínűleg mindent átalakító változások főképp az USA-ban zajlanak, a lehetséges kimenetelekről pedig *Ormós Zoltán* internetjogászt kérdeztük.

Ahogy azt az ITBUSINESS online már tavaly decemberben megírta, az USA szerzői jogi hivatala azon gondolkodik, hogy legalizálják a nagy LLM-szolgáltatók szerzőijog-tipró, szürke vagy egyenesen feketezónás, darkwebről beszerzett adatkészleteinek felhasználását. A lépést annak a gazdasági kockázata indokolhatja, amit az MI-piac gigantikus tőkebefektetéseinek befuccsolása, vagy profittermelő képességük csökkenése jelenthet.

Mindeközben hatalmas perek zajlanak a The New York Times, a Microsoft, az OpenAI vagy éppen (sok tucat más író mellett) *Nora Roberts* bestseller-írónő részvételével, akik műveik jogdíjfizetés nélküli felhasználását sérelmezik például a Bloomberg chatbotjának vagy a ChatGPT feltanításához, amelyek valószínűleg többek között azért képesek olyan élethű narratívákat írni, hogy sokan hajlandóak havi 20 dollárért előfizetni rájuk. Innen nézve persze ebből a pénzből nyilván járna azoknak az „óriásoknak", akiknek a vállán a szoftver áll.

FORRÁS: FREEPIK.COM

Jogfilozófia és felelősség

„Egyfelől ott a 'Sein' síkja, tehát ami van, ami a most aktuális szabályozás, és ott van a 'Sollen', aminek lennie kellene", véleményezte a helyzetet Max Webert idézve Ormós Zoltán internetjogász, aki évtizedek óta nyomon követi az online jog világának viharos eseményeit. A reformötlet szerinte egyelőre a jogfilozófiai fejtegetés szintjén mozog, vagyis messze még a bármilyen konkrét jogrendszert érintő átalakulás. Ezért most senkinek nem ajánlható, hogy az MI által előállított anyagot szabadon felhasználható, jogtiszta forrásnak tekintse, amely nem sértheti valakinek a szerzői jogát.

Az OpenAI például egyértelműen azt kommunikálja, hogy minden felelősség a felhasználót terheli, tehát nekünk kell ellenőrizni, hogy a felhasznált anyag jogtiszta-e. Magyarul ez semmivel sem ad többet, mint a Google kereső használata, körülbelül ennyit csinál a ChatGPT is, egy kicsit szintetizál, és egy gyakornokhoz hasonlóan összevagdossa a szövegeket.

Ha a felhasznált anyagok tekintetében megvan a részleges egyezőség, a szolgai másolás, akkor bizony ugyanúgy szerzői jogot sértünk a szerzői jog megsértésének terminológiája, illetve definíciója szerint – figyelmeztetett rá az internetjogász. Ha a használt MI-chatbot ennél jobban átdolgozta a szöveget, tehát minden szót kicserélt valami másra, de gyakorlatilag ugyanaz a mondat jelentése, akkor lehet vitatkozni, hogy pusztán egy átdolgozás, vagy egy új eredeti szerzői mű keletkezett. „Szerintem, ha csak szinonim szavakra cserélte a szöveget, vagy egy részét, azzal még nem valósul meg az egyéni, eredeti szerző jelleg, hiszen az eredeti átdolgozásával jött létre a mű", mondta Ormós Zoltán.

ChatGPT felhasználási feltételek

Az OpenAI például a „ChatGPT terms"-ben – azaz az ÁSZF-ében – a felhasználóra hárítja a felelősséget,– mutatott rá Ormós Zoltán. Ha a saját anyagunkat dolgoztattuk át a chatbottal, akkor az output a miénk, és azt is megtaláljuk az ÁSZF-ben, hogy sok más személy is kaphat hasonló outputot, mint mi. Az idevágó, leglényegesebb rész egy elég komoly rendelkezést is tartalmaz, kimondva, hogy nem használhatjuk úgy a szolgáltatást, hogy az bármilyen szempontból illegális károkozást eredményezzen vagy visszaélésszerű legyen. Nem használhatjuk úgy sem a szolgáltatást, hogy az sértse, félreértelmezze, vagy megsértse mások jogait. Vagyis a joganyag kimondja azt, hogy ha megsértettük valakinek a jogait, az a mi használatunkból eredő cselekedet. „Érdemes tehát a chatbotok összes kimeneteire plágiumellenőrző eszközöket használni, ha el akarjuk kerülni a jogsértéseket", figyelmeztetett rá Ormós Zoltán.

Ami az USA szerzői jogi törvényének esetleges megváltozását illeti, azt is érdemes szem előtt tartani, hogy maga az Egyesült Államok fektetett be rengeteg időt és energiát azokba a szerzői jogi egyezményekbe, amelyek ma meghatározzák a szerzői jogot, és aktív résztvevő a szerzői művek piacán a II. világháború végétől a mai napig. „Tehát valószerűtlen, hogy most hirtelen ráfordulnának egy olyan

> Ha a generatív MI használata során megsértettük valakinek a jogait, az a mi használatunkból eredő cselekedet.

ösvényre, amely a semmibe veszi ezeket az előzményeket. Nem tartom valószínűnek, hogy a közeljövőben ez megtörténhetne", mondja a jogász. „Ha persze teljes paradigmaváltás lesz, és így az emberi teljesítmény és a szerzői teljesítmények teljesen háttérbe szorulnak, akkor onnantól kezdve lehet, hogy mindent a gépek fognak írni, és talán teljesen mindegy lesz majd, hogy kié volt bármi is eredetileg", tette hozzá a bizonytalanságokra utalva.

FORRÁS: ORMÓS ZOLTÁN

ORMÓS ZOLTÁN INTERNETJOGÁSZ

Iparági szakértők egyébként azt jósolják, hogy közeleg a szintetikus szövegek kora – egyfajta szintetikus szingularitás – mikor az MI már nem hallucinál majd ennyit, hanem képes lesz olyan szövegeket írni, mint egy ember. Innen talán már nem is lesz szükség emberi írókra. Vállalati oldalon ugyanakkor mintha több felelősségvállalást is elbírna az OpenAI a kimenetek jogtisztaságáért is felelősséget vállalva.

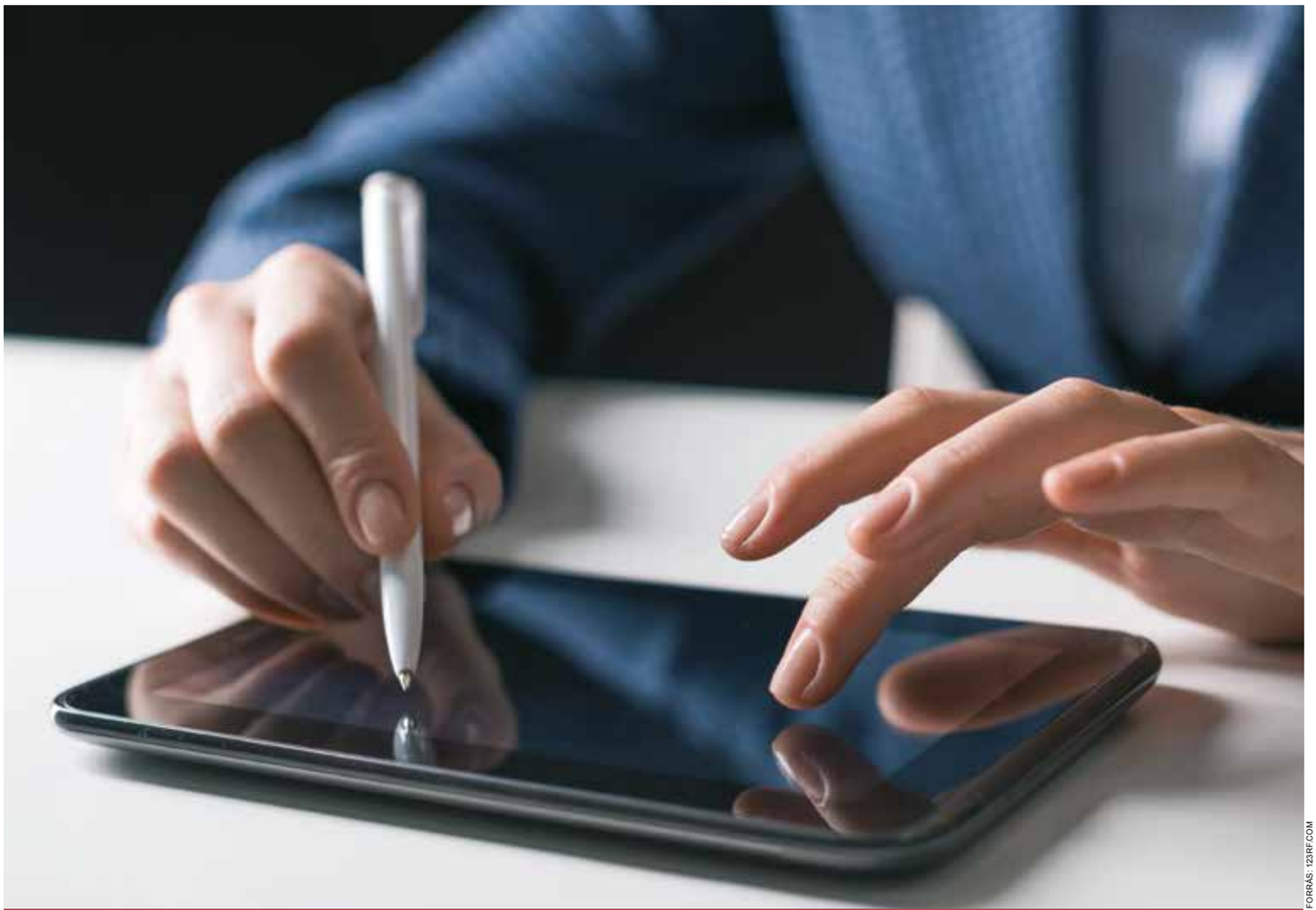
Vállalati MI-jogkörnyezet

A vállalati előfizetéseknél a cégek adatkészletéről, adatvagyonáról van szó, amely más megítélés alá kell essen, mint a szerzői művek. Minden vállalatra igaz, hogy az adatvagyona az, ami miatt valamely szempontból a vállalat igazán sikeres tud lenni, ezért rendkívül fontos, hogy azt hogyan kezeli, és hogyan védi.

„Ebből a szempontból azért én technikai értelemben konzervatív maradnék, tehát azt mondanám, hogy eljöhet esetleg azoknak az MI-szoftvereknek a dominanciája, amelyek nem a felhőben futnak, és egy kisebb, saját adathalmazon tanulnak. A 'sziget' típusú izolált adatkezelés biztonságot tud teremteni", mondta Ormós Zoltán.

Az MI-re visszatérve tegyük azt azért mellé, hogy minden új technológiának van egy jellemző életciklus görbéje, ami először nagyon felugrik, aztán nagyon visszaesik, és valahol a középen fog beállni egy normál szintre. „Ma még az MI-görbe a plató környékén jár, és hat a cégek körében FOMO (a kimaradástól való félelem) is, de ez jelentősen vissza fog esni. Rájönnek majd, hogy az MI egy csomó dologra nem úgy használható, ahogy az elején elképzelték, és halmozódnak a biztonsági kockázatok is", zárta gondolatait az internetjogász.

Justin Viktor



FORRÁS: 123RF.COM

ÁTALAKULÓ E-INGATLANNYILVÁNTARTÁS

Kötelező lesz az elektronikus aláírás

Nagyot fejlődött az elektronikus dokumentumkezelés és az ügyintézés, de egy kritikus ponton általában megbicsaklik a folyamat – ez pedig a hitelesítés. Legyen szó magánszemélyek hivatali vagy szolgáltatói ügyintézéséről, esetleg két vállalkozás közötti üzleti szerződésről, a legtöbb esetben a teljesen digitalizált folyamat egy pontján belép az analóg világ: amikor a dokumentumokat kézzel írják alá az érintett felek. Hamarosan azonban komoly változás várható.

Hogyan is néz ki ezért ma egy szerződési folyamat? A dokumentum elektronikusan születik meg – megírják egy számítógépen, a tervezeteket emailen küldözgetik, míg elő nem áll a végleges verzió. Akkor aztán kinyomtatják sok oldalon és sok-sok példányban, hogy minden érintett fél aláírhassa kézzel. Majd az aláírt példányokat beszkennelik, így újra elektronikus dokumentum születik belőlük, az eredetieket pedig elteszik az irattárba, hogy jó esetben soha elő ne vegyék őket. „Nyilvánvaló, hogy mennyivel egyszerűbb, gyorsabb, környezetbarátabb és nem utolsósorban olcsóbb lenne, ha ezeket az iratokat nem kellene kinyomtatni és visszaszkennelni, hanem a folyamat végéig megmaradhatnának elektronikusnak”, hangsúlyozza *Dr. Kósa Ferenc* ügyvéd, a Magyar Elektronikus Aláírás Szövetség (MELASZ) elnöke.

A ragaszkodás a papírhoz azért is érthetetlen, mert a jogi keretek régóta adottak. Magyarországon már 2001-ben megszületett az elektronikus aláírásról szóló első törvény, az első ügymenet, amelyet pedig kizárólag elektronikusan lehet intézni, 2008-as – azóta csak ilyen formában

lehet cégbejegyzési és változási kérelmet benyújtani a Cégbíróságra. „Ez azt is jelenti”, teszi hozzá Dr. Kósa Ferenc, „hogy az ügyvédeknek 2008 óta rendelkezniük kell elektronikus aláírással, ha cégügyeket akarnak intézni. 2016 óta minden gazdálkodó szervezet számára kötelező az elektronikus kapcsolattartás a hatóságokkal, bíróságokkal.”

Ingyen is kaphatnak

Magánszemélyek számára is viszonylag könnyen elérhetők az e-aláírások. Az elektronikus személyi igazolványba integrált chip (egyéb adatok mellett) minősített elektronikus aláírás tanúsítványt is tartalmazhat, ha azt az állampolgár a személyi kiváltása során kérte. Mobiltelefonnal beolvasható a tanúsítvány, és másodpercek alatt aláírható vele egy elektronikus dokumentum. Két piaci szolgáltató, a Netlock és a Microsec is kínál magánszemélyeknek ingyenes, szintén mobillal is használható elektronikus aláírást.

Egy másik módszer a magyarorszag.hu-n, ügyfélkapus bejelentkezés után igénybe vehető AVDH (azonosításra visszavezetett dokumentumhitelesítés), amely mindenki számára ingyenesen elérhető, akinek van ügyfélkapuja. A feltöltött dokumentumokat az AVDH révén lehet elektronikus aláírással ellátni. „Egyfelől nagyon örülök, hogy létezik ez a lehetőség, mert tényleg széles körben elérhető. Ugyanakkor ismerjük a mindennapi gyakorlatot, hogy cégvezetők milyen gyakran osztják meg az ügyfélkapus bejelentkezési adataikat akár az asszisztenseikkel, akár a könyvelővel. Ez nemcsak az eljárást, hanem a visszaélést is megkönnyíti”, mondja erről az ügyvéd.

További probléma az AVDH-val, hogy a hitelesítés során az így „aláírt” dokumentumhoz csatolva lesznek az aláíró ügyne-

FORRÁS: MELASZ

DR. KÓSA FERENC ÜGYVÉD,
A MAGYAR ELEKTRONIKUS ALÁÍRÁS SZÖVETSÉG ELNÖKE

Adni-venni továbbra is lehet papíron

Érdekes csavar a szabályozásban, hogy magát az ingatlan adásvételi szerződését továbbra is lehet papíron aláírni és utólag digitalizálni, szkennelni, az ügyvédi meghatalmazást és a bejegyzési engedélyt viszont kizárólag elektronikusan lehet létrehozni. Ennek oka feltehetően az, hogy egy közel tízéves jogszabály szerint csak 50 millió forintig lehet pénzügyi kötelezettséget vállalni e-személyivel – ebbe az összeghatárba viszont már lassan egy budapesti panellakás ára sem fér bele.

vezett „négy T”, azaz természetes azonosítói: név, születési név, az anya neve, születési hely és idő. Ezek az adatok a hitelesített dokumentummal együtt mennek tovább. „Különösen bírósági eljárásokban kényes ügy ez, hiszen így adott esetben a gyanúsított is megismerheti a felperes vagy az áldozat, de akár az eljáró ügyvéd személyes adatait is”, teszi hozzá Dr. Kósa Ferenc.

Mobilapp is lesz

Most azonban komolyabb változás várható az e-aláírás használatában. Az ingatlan-nyilvántartási eljárásokban tervezett módosítások szerint már nemcsak az ügyvédek, hanem az ügyfelek (magánszemélyek) számára is kötelező lesz az elektronikus aláírás használata az ügyvédi meghatalmazás és az úgynevezett bejegyzési engedély aláírására. Ehhez a korábbi módszereken kívül a Digitális Állampolgárság Program (DÁP) keretében megvalósuló mobilappot, illetve annak e-aláírási funkcióját is lehet majd használni. A tervek szerint az alkalmazás használatára július elejétől lehet előregisztrálni, az éles üzem pedig a tervek szerint szeptemberben indul.

Hogyan működik majd ez a gyakorlatban? Ahogy Dr. Kósa Ferenc elmeséli, az elektronikus ingatlan-nyilvántartásnak lesz egy webes felülete *(https://landing.eing.foldhivatal.hu/),* ahova vagy a DÁP mobilappal vagy az ügyfélkapun keresztül, de kétfaktoros azonosítást követően lehet bejelentkezni. A fent hivatkozott dokumentumokat ezen a felületen kell előállítani, az ügyfélnek és az ügyvédnek egyaránt hitelesítenie kell elektronikusan, majd a rendszeren keresztül beküldhetők az iratok.

A háttér is változik

Az ingatlan-nyilvántartás és az alapjául szolgáló térképek egyébként jó húsz éve digitalizáltak, csak az eljárás volt hagyományos. Ugyanakkor szükség volt komoly adattisztításra, például az ismeretlen tulajdonos birtokában lévő termőföldek esetében, illetve végrehajtottak egy adatmigrációt is, amelynek során a régi nyilvántartásból áttöltötték az adatokat az új elektronikus nyilvántartásba. Egyes földhivatalokban már májustól használni fogják az új nyilvántartást, ami azt jelenti, hogy a friss változásokat mind a két változatban átvezetik – vagyis a back-office hamarabb áttér az új módszerre, mint front-office, azaz az ügyfelek és az ügyvédek, tekintettel arra, hogy az új törvény hatálybalépését követően a személyes ügyfélfogadás megszűnik a földhivatalokban.

Mindezzel párhuzamosan némiképp változik az ingatlanjog intézménye is (ennek részleteibe itt nem érdemes belemenni), viszont ennek következménye az lesz, hogy csak azok az ügyvédek intézhetnek ingatlanügyeket, akik levizsgáztak az elméletből, emlékeztet Dr. Kósa Ferenc. Emellett kiegészítő 50 millió forintos felelősségbiztosítást kell kötniük, kifejezetten ingatlan-nyilvántartási ügyintézésre. Ezt követően kell kérelmezniük a kamaránál, hogy jogosultságukat bejegyezzék az ügyvédi nyilvántartásba, és amikor ez megtörtént, onnantól már intézhetnek ingatlanügyeket. ■

AZ INTERNETES SABLONOK NEM MŰKÖDNEK

Lehet rövid szerződést írni, de nem érdemes

A Havas-Sághy és Társai Ügyvédi Iroda az alábbiakban foglalja össze tapasztalatait a szoftverfejlesztési szerződésekkel kapcsolatos elvárásokról – és a realitásról.

FORRÁS: HAVAS-SÁGHY ÉS TÁRSAI ÜGYVÉDI IRODA

HAVAS-SÁGHY GÁBOR,
HAVAS-SÁGHY ÉS TÁRSAI ÜGYVÉDI IRODA

A szerződéstől minden fél elvárja, hogy érdekeit minél jobban védje. Legyen áttekinthető – de az érdekek alapos védelmét csak egyértelműen kifejtett feltételekkel lehet biztosítani. Az egyértelműség pedig megköveteli a részletek kidolgozását, ráadásul az egyedi fejlesztések egyedi megközelítést igényelnek. Az internetes sablonok nem ilyenek. Az alábbiakban összefoglaljuk a szerződés kritikus elemeinek jellegzetességeit.

A **fejlesztési specifikációk** határozzák meg a szoftverrel kapcsolatos alapvető elvárásokat, ez a fejezet vagy melléklet kiemelkedő fontosságú. Ennek kellően hosszúnak és részletesnek kell lennie.

A **teljesítés ellenőrzése, igazolása,** valamint ezekhez kapcsolódóan a díjazás, a számlázás és a megszüntetés feltételeinek rögzítése elengedhetetlen. Tapasztalataink szerint a legtöbb vitát e részek hanyag kidolgozása eredményezi. Bár a szakma több hatékony megoldást is alkalmaz, mégis gyakori hiba, hogy a szerződésben nem kellően részletes, vagy nem az adott projektre szabott elszámolási mechanizmus szerepel.

Tapasztalatunk szerint **a szellemi tulajdonjog (IP),** a titoktartás és a szavatossági kérdések kidolgozására általában szintén nem szentelnek elég figyelmet. Márpedig a szoftver hasznosítását ezen fejezetek határozzák meg, így üzleti oldalról nem mellőzhetők.

Ritka (és örömteli), amikor a fentiek mellett **hírnév- és üzleti érdekvédelmi, versenykorlátozási, joghatósági, vagy lehetetlenülési klauzulákkal** is találkozunk. Általában ezek szükségességére nekünk kell felhívnunk a figyelmet, és ezek kidolgozását is irodánk szokta elvégezni.

A szerződés költségei eltörpülnek még egy kisebb applikáció fejlesztéséhez képest, ezzel szemben az alapossággal és rutinnal kidolgozott szerződés előnyei gazdaságilag is jelentős értékűek. ■

Dr. Novák Anett
konzultáns

Mindenképpen foglalkozni kell a NIS2-vel

Kicsit úgy vagyunk a jelenlegi szabályozásokkal, mint a Római Birodalom légióival: egyszer elér minket, talán le is rohannak minket, nekünk meg túl kell élni valahogyan, és meg kell oldani az együttélést. Nos, a NIS2 elkészült, mind az Európai Uniós, mind a hazai szabályozás (bár cikkünk 2024 májusi megjelenésekor még várjuk a végleges kiegészítő szabályozásokat), ki is hirdették, és ha már első sokk után magunkhoz tértünk, és megtörtént a (mentális) lerohanás, akkor próbálunk vele együtt élni, és versenyt futni az idővel, hogy mindennek meg tudjunk felelni.

Maga a szabályozás – főleg, amikor túljutunk az olvasás fázisán – nem könnyű olvasmány, főleg akkor, ha megpróbáljuk beazonosítani magunkat, és elhelyezni az érintetti körbe. Ehhez a Szabályozott Tevékenységek Felügyeleti Hatóságának (SZTFH) a prezentációi és előadásai nagyban segítséget nyújtanak a szervezeteknek. Két dologról ellenben kevés szó esik.

Vessük pillantásunkat a cégjegyzékre

Az egyik az, ha már tudjuk, hogy méretileg vagy bevétel alapján – talán – a hatálya alá tartozunk, mit kell még figyelembe venni, ha még mindig nem vagyunk biztosak abban, hogy a jogszabály ránk is vonatkozik-e? A TEÁOR és a NACE kód szintén segítség abban, hogy meggyőződhessünk arról, hogy beleesünk-e az érintettek körébe.

A cégjegyzékben a szervezet tevékenységi kódjai közel 100%-os biztossággal megmutatják azt, hogy indulhat-e a vesszőfutásuk az idővel vagy sem. Szintén ide kapcsolódik az is, hogyha valamelyik hatóság nyilvántartásába be kellett kerülnie a szervezetnek (pl. NMHH, NÉBIH stb.), akkor már teljesen biztos lesz az is, hogy a NIS2 érvényes lesz ránk, és az első nehéz és fájó lépést is meg kell tenni, be kell jelentkezni a hatóságnál, mint NIS2 alany.

Hosszú csata ez – nem, nem háború, hiszen azt majd akkor tudjuk megnyerni, ha már leszerződtünk egy auditor céggel, akik bevizsgálják a szervezetet és megtörténik az első kötelező audit - lezárásának ideje és a paktum megkötése: 2024. június 30.-ig. De mindenekelőtt meg kell keresni azokat az információkat a cégen belül, amelyeket be kell jelenteni az SZTFH felé (pl.: információbiztonsági felelős meg- és kijelölése, szervezet által használt domain nevek összeírása, IP-címek (fix), partner és beszállítói adatok stb.)

FORRÁS: WIKIPEDIA

Már elkéstünk a létszámcsökkentéssel

A másik tényező azokat fogja kellemetlenül érinteni, akik úgy döntöttek, hogy inkább a létszám-leépítés, illetve „egyéb átszervezés” mellett voksolnak, és 50 fő alatti foglalkoztatotti létszámúvá alakulnak. Költséghatékonyság szempontjából biztosan jó döntés volt, ellenben az SZTFH az utolsó kettő lezárt évi cégadatokat fogja figyelembe venni; aki így próbálja meg, hogy elkerülje a lehetetlent, annak csak idő kérdése, hogy a hatóság látókörébe kerüljön, és akkor nemcsak a bírsággal kell szembenéznie, de a megfelelőség miatt is fájni fog a feje.

Figyeljünk arra, hogy elsősorban magunkat megvédjük az esetleges incidens esetén, továbbá, ha ez bekövetkezik, akkor az esetleges hiba, mulasztás, károsodás, felelősség és egyéb esetkörökben egy letisztultabb felelősségi rendszerben lehessen kezelni a felmerült eseményeket, amely meg tudja azt mutatni, hogy kinek a hibájából, illetve hol következett be az incidens.

A cseresznye a tortán, hogy a beszállítók és partnerek listájának összeállítása és az után, hogy felmértük, milyen kockázati értékkel, lehetőségekkel rendelkeznek, akkor újraírhatjuk vagy kiegészíthetjük a már meglévő szerződéseinket, az új ügyfelek számára pedig már a (IT-, információbiztonsági-, cyber security-) biztonsági, védelmi specifikumokat is tartalmazó szerződéseket tudjuk átnyújtani.

Amikor mindezeknek eleget teszünk, és azt hisszük, már nem jöhet olyan szabályozás (invázió), amely kihatna további életünkre, akkor az AI Act is lassan (de biztosan) berobban az életünkbe, és a „lerohanás” újra kezdődik. ■

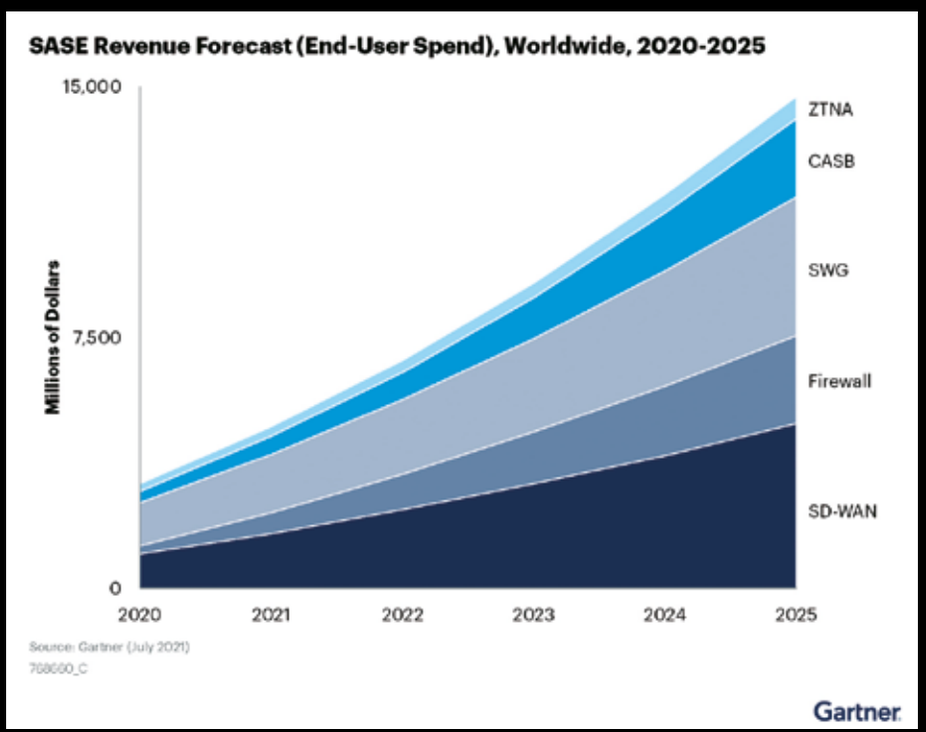
Kamarás Bálint
security architect

SD-WAN-tól a SASE-ig

Az infrastruktúráért és üzemeltetésért felelős szakemberek, valamint az IT-biztonsági szervezetek számára a hagyományos architektúrákról a modern, Zero-Trust alapokra történő átállás korántsem jelent egyszerű feladatot. Ezek a szervezetek gyakran szembesülnek a különböző gyártók eltérő érettségi szintű heterogén környezeteiben komoly nehézségekkel már az üzemeltetés és fejlesztés területén is. Ettől nagyságrenddel komplexebb kérdéskört vet fel a rendszerek modernizálási igénye.

A Gartner jóslata alapján, 2025-re a ZTNA-t (Zero Trust Network Access) alkalmazó szervezetek 70 százaléka vagy a SASE (Secure Access Service Edge) vagy az SSE (Secure Service Edge) irányt választja a ZTNA megvalósítására. De hogyan jutunk el egy SASE-komponens bevezetésétől, jelen esetben egy SD-WAN-tól (amely általában elsősorban hálózatos, üzletfolytonossági és felhasználói szempontból érkező igény) egy akár komplett SASE Platform-ig?

Ez a feladat korántsem olyan nehéz, mint amilyennek első látásra gondolnánk. Először is kellően pontosan meg kell határozni az elérni kívánt célokat. Ezt követően a különböző gyártók tengerében szükséges megvizsgálni, hogy az eltérő víziók közül melyek állnak a mi igényeinkhez közelebb. Az első döntési ponton hazánkban jellemző, hogy elsősorban hálózat- és nem biztonság-orientált a projekt lelke. Ebben az esetben mindenképp a hosszútávú tervezés legyen a szempont. Ha elköteleződünk egy SD-WAN gyártó felé, akkor az előbb-utóbb biztosan megjelenő biztonsági igényeket csak a kiválasztott gyártó megoldására építve tudjuk majd megoldani.



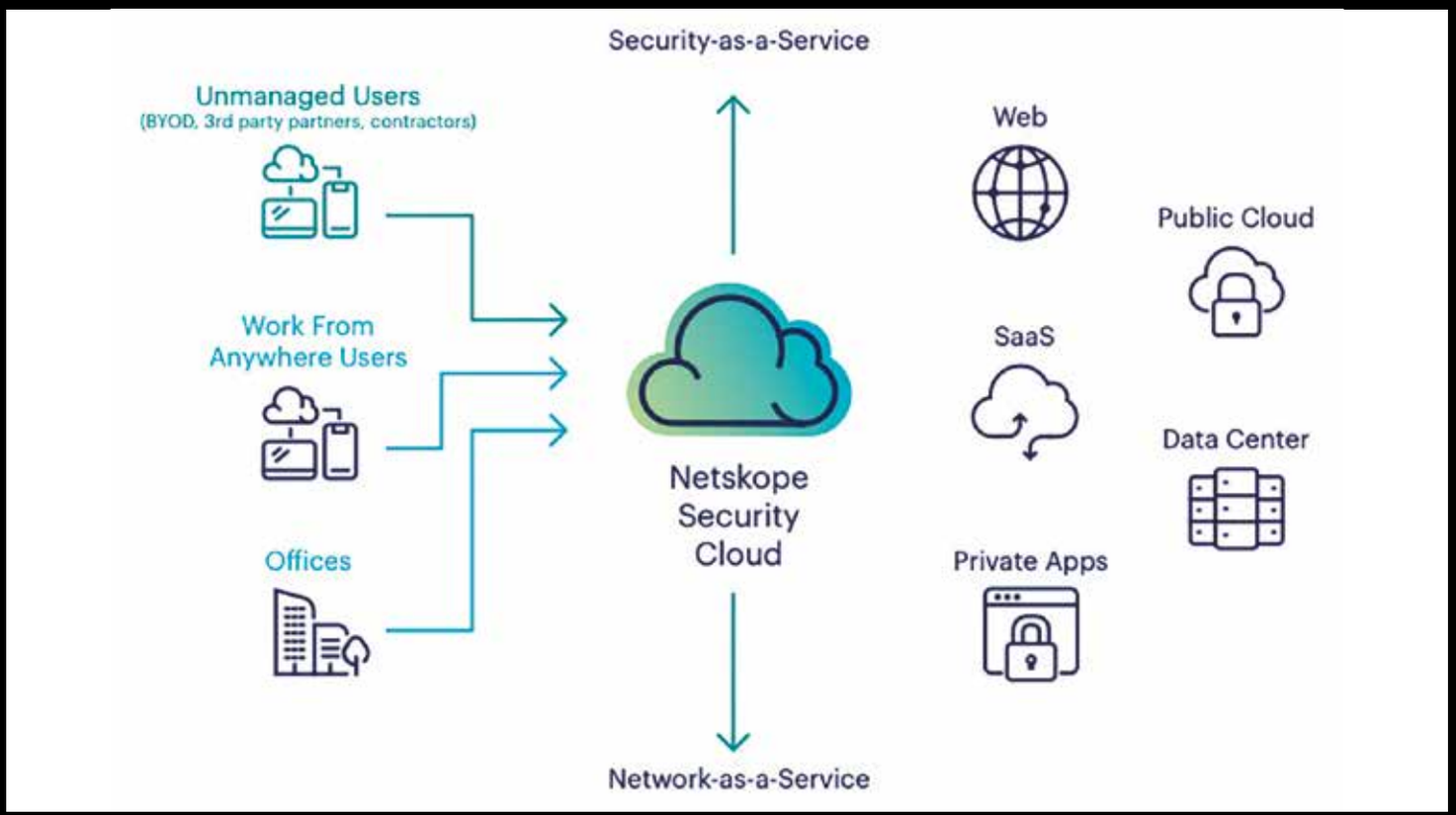
Bonyolítja a helyzetet, hogy a legtöbb esetben nem egy új környezet felépítése a feladat. A SASE akkor is rugalmas megoldást nyújt az igényekre, amikor egy meglévő ökoszisztémába kívánunk becsatlakoztatni új biztonsági elemekkel vagy bővülünk. Vagyis egy új telephely, egy új szervezeti egység kialakítása esetén nincs megkötve a kezünk. De a meglévő biztonsági architektúránk újragondolása esetén is kiváló döntés lehet ez az irány.

A végcél az, hogy a felhasználók elérjék ugyanazokat az erőforrásokat és rendszereket, amelyek a munkájukhoz szükségesek a lehető legmagasabb biztonsággal. Arról nem is beszélve, hogy egy homogén környezet üzemeltetése sokkal egyszerűbb és általában költséghatékonyabb is.

Piaci háttér

A Netskope az egyik első azon gyártók körében, akik kifejezetten a SSE-vel, mint technológiai megoldáscsomaggal léptek a piacra. A 2012-ben alakult cég 2015-ben állt elő először azzal a platformmal, melyet ma – követve a trendeket –, nemes egyszerűséggel csak Netskope One-nak hív (korábban Security Cloud Platform volt) és alapjában véve a felhős szolgáltatások alkalmazásalapú kezelésére (CASB-ra, Cloud Access Security Brokerre) épül. A Gartner SSE-kvadránsában 2024-ben immáron harmadik alkalommal értékeli igen előkelő vezető helyen a Leaders kategóriában.

2023 augusztusában vásárolta fel a Netskope a Infiot-ot, így az addig hiányzó elem, egy Borderless SD-WAN megoldás is sebesen integrálódott a platformba, így garantáltan a „Single-Vendor SASE” kategóriában is előkelő helyre kerülhet a Palo Alto Networks mellett a soron következő új riportban.



Mindezek mellett a cég alapítói, befektetőinek egy része, valamint vezető mérnökei szinte kivétel nélkül a különböző konkurenciáktól érkeztek az évek során. Nem csoda, hogy a stabil háttérrel rendelkező cég szakmai vonalon is több mint 10 éve bizonyít a világ különböző piacain. Az igazán ínyenceknek kötelező a „Critical Capabilities for Security Service Edge" kódnév alatt futó Gartner-elemzés, amelyben többek között négy kiemelt felhasználási mód (1. Secure Web and Cloud Usage, 2. Detect and Mitigate Threats, 3. Connect and Secure Remote Workers, 4. Identify and Protect Sensitive Information) mentén kerülnek besorolásra a gyártók. A Netskope-ot a négyből két esetben első, két esetben második helyre értékelték.

Választási gondolatok

A fentieket végiggondolva nehéz olyan gyártót választani, amely minden tekintetben már első ránézésre erősebb, de menjünk egy kicsit mélyebbre. Csak néhány példa, amelyek számtalanszor felmerülnek a különböző ügyféligények során: felhős alkalmazásokban történő adatszivárgás, felhasználói élmény monitorozás és szabályozás, távoli munkavégzés, külsős beszállítók felügyelete stb. Egy azonban mindben közös: az adat, és annak mozgása a szervezeten belül és főleg azon kívül.

Ezen a téren nyújt teljes körű szolgáltatást egy igazán jó SASE platform. Mindent lefedhetünk, ami SaaS, IaaS, nem menedzselt szolgáltatások, saját alkalmazások, szinte a létező összes szükséges biztonsági funkcióval (Threat Protection, titkosítás, FWaaS, Cloud SWG, DLP, UEBA, OCR, RBI „és még sokan mások"). Nem beszélve a különféle analitikákról és a számos natív integrációs irányról (XDR/SIEM/SOAR stb.), ha ennél még többre lenne szükség.

Akár laikusként is végig gondolva, ha ilyen szintű biztonsági funkcionalitást szeretnénk, az nem tűnik kis feladatnak. Egy SD-WAN bevezetést követően, melyek a prioritások? Mik lesznek a következő lépések? ZTNA? VPN kiváltás? SWG funkcionalitás? Ezeket kell alaposan végiggondolni előre. Arról már korábban is esett szó, hogy egy ilyen jellegű fejlesztés a megszokottnál alaposabb tervezést követel meg, ami viszont az implementáció fázisában kifizetődik. Ez a kulcsa a jövő hálózatainak. Sokkal-sokkal alaposabban és hosszabb távra kell tervezni.

Összefoglalás

A vállalatoknak előbb-utóbb elkerülhetetlenül nyitniuk kell az új technológia irányába az üzleti igények miatt. Csak így tarthatnak lépést a fejlődés adta lehetőségek mentén a megkövetelt biztonsági szinttel. Létfontosságú, hogy ez igaz akkor is, ha főként hálózatot érintő projektről van szó.

Figyelembe KELL venni a biztonsági aspektust, mert ennek hiányában sem közép-, sem hosszútávon nem fogunk tudni tovább építkezni, és komoly lépéshátrányba kerülünk. Sokszor olyannyira, hogy a meglévő konstelláció szinte teljes újragondolása lesz szükséges. Tekintettel arra, hogy nincs két egyforma környezet, kulcsfontosságú a tényleges professzionális fejlesztési tervek készítése, még akkor is, ha ezt időről időre igazítani kell a változó igényekhez.

A gyártók startra készen várják ezeket az igényeket, itt az idő, hogy az ügyfelek nyissanak, az implementációs szakértők pedig felnőjenek a feladathoz. ■

Foki Tamás
senior system engineer

Thales és Imperva összeolvadás – Better Together

A számtalan IT-biztonsági felvásárlás-összeolvadás közül kiemelkedik a nekünk egyik legfontosabb: a Thales és az Imperva ügye. Mivel mindkét cégnek évek óta regionális disztribútorai vagyunk, így egészen közelről figyelhetjük, hogy hogyan fogja kiegészíteni és erősíteni egymást a két vezető, IT-biztonsági cég adatbázis-védelmi portfóliója.

Leginkább az adatbázis-biztonsági területre vagyunk kíváncsiak, ahol mindkét gyártónak vannak megoldásai. Úgy érzem, hogy ez a terület a fontosságához képest továbbra is kisebb figyelmet kap, és kevesen foglalkoznak a szervezetük által használt, birtokolt adatbázisokban tárolt érzékeny adatvagyon felmérésével és védelmével, direkt erre a területre szánt, célzott megoldásokkal.

Egyértelmű, 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 az esetlegesen nem megfelelően kezelt és védett személyes adatok miatt.

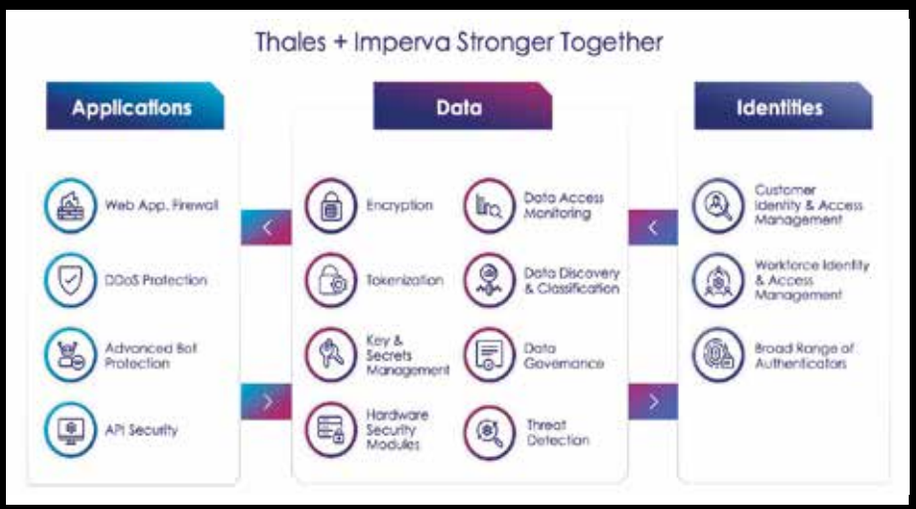
A **Thales** portfólióját a **CipherTrust Data Security Platform** erősíti, amelynek fontos része az adatvagyont feltérképező és értékelő modul, amely strukturált (adatbázisok) és strukturálatlan adatokban (dokumentumokban, ömlesztett fájlokban, archivált tartalmakban) is képes keresni. Felderíti az érzékeny adatokat a 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.

További fontos szolgáltatásai ennek a platformnak az adatok biztonságát védő titkosítási megoldások (transzparens titkosítás a legkülönbözőbb adatbázisokhoz on-prem és felhős környezetekben is), és a statikus/dinamikus adatmaszkolási lehetőségek az érzékeny adatok kezelésére, valamint a titkosítási kulcsok kezelését és biztonságos tárolását segítő kulcsmanagement és HSM megoldások.

Az **Imperva** az ún. **Data Security Fabric**-ot fejleszti ezen a területen. Ez az egyik első on-prem, multicloud és hibrid környezetben is egyaránt használható, egységes átfogó adatvédelmi megoldás, amelynek a legnagyobb előnye, hogy a legkülönbözőbb helyen lévő adatbázisokban képes ellenőrizni az összes adatbázist érintő tevékenységet, legyen az hagyományos adatbázisokban, felhőalapú (cloud native) tárolókban, big data platformokon, támogatja a legújabb technológiákat is, például a NoSQL adatbázisokat, Kubernetes konténeres környezeteket is.

Szintén képes az adatokat feltérképezni és osztályozni, legyenek azok bármilyen adatbázisban, és ezekről segít egységes képet adni, hogy hol és milyen típusú adatok vannak tárolva. A Imperva Data Security Fabric nagy segítséget nyújt testre szabható adatvédelmi szabályok és házirendek meghatározásához és azok érvényesítéséhez.

Nagy erőssége az adatbázis monitoring és hozzáférésvédelem. Finomra hangolható szabályok mentén képes észlelni és figyelmeztetni gyanús viselkedések, anomáliás tevékenységek és meghatározott házirendek megsértésének bekövetkezése esetén.



Másik nagy erőssége a platformnak az ún. Data Risk Analytics modul, amely az adatbázis-védelmi megoldásokból érkező logokat egy helyen dolgozza fel. Fejlett analitikával, korrelációs szabályokkal dolgozik, sok ezer logbejegyzésből incidenseket generál részletes leírásokkal. Ez az eszköz nagy segítséget tud nyújtani az incidensek priorizálásában, a hibás pozitív riasztások számának csökkentésében, valamint nagyban növeli az aktív támadások felismerésének lehetőségét (például a ransomware-támadásokat).

THALES

Almási Zsolt
CISSP,
Engineering team lead

Van jó kiberhírszerzési eszköztár

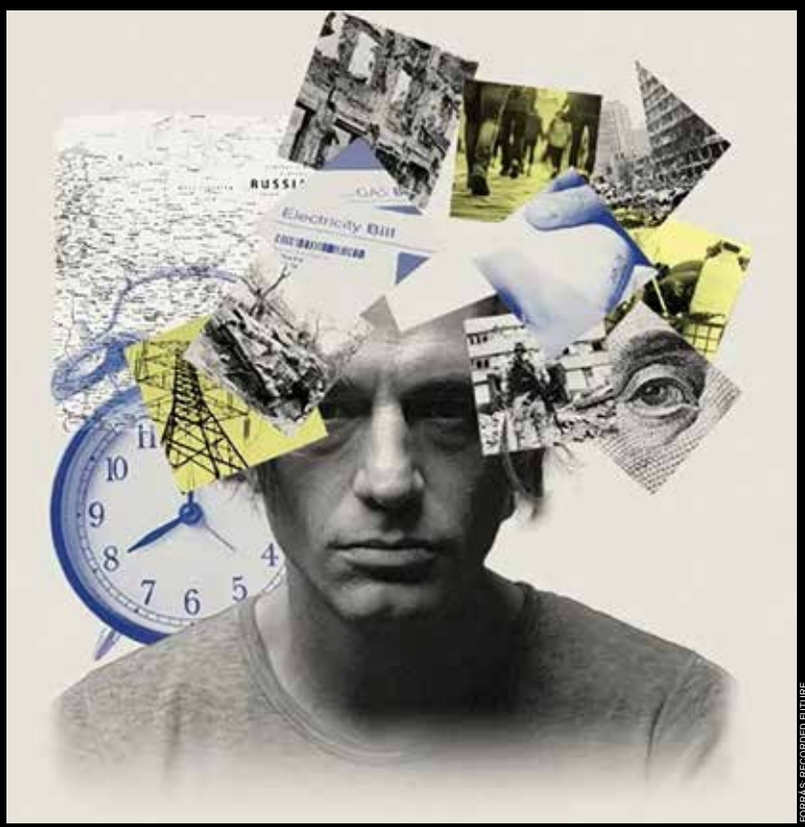
A CTI- (Cyber Threat Intelligence) platformok használata egyre inkább nélkülözhetetlen a cégek számára. Ha visszatekintünk az elmúlt év kiberbiztonsági eseményeire, láthatjuk, hogy a támadások száma folyamatosan növekszik. Az ismert sérülékenységek (CVE-k) listája is egyre csak bővül, ezzel párhuzamosan pedig olyan exploitok látnak napvilágot, amelyek használatával már nemcsak az elavult, és/vagy kis rendszerekbe lehetséges a behatolás.

2022-ben több, mint 25 ezer (25081) sérülékenységet találtak a különféle környezetekben, ami ijesztően magas szám, viszont a 2023-as év statisztikái ezt is felülmúlták - ekkor 29065 darab sérülékenységet regisztráltak. Ha a számok mögé nézünk, felismerhetjük, hogy a legnagyobb gyártók legbiztonságosabbnak ítélt megoldásainak esetében sem lehetünk teljesen nyugodtak, mivel az operációs rendszeren és a tűzfalakon át a céges IT-infrastruktúra bármely komponense célpont lehet.

Az általános patchelési folyamatok fejlesztésén felül a szabályozás szempontjából is hasznos lehet a legtöbb szervezet számára egy CTI-megoldás. Jelentősen növelhetjük az IT biztonsági csapatunk hatékonyságát, ha nem csak hírekre, illetve a gyártók tájékoztatásaira hagyatkozva dolgoznak, hanem egy független CTI megoldás is támogatja őket. Az egyik ilyen piacvezető megoldás a **Recorded Future,** amely több, mint egymillió forrásból szerzi be a különféle információkat, és segít azok értelmezésében is.

Szintén említésre méltó, hogy a generatív MI-megoldások elterjedésével az elmúlt években viszonylag könnyen kiszűrhető phishing támadások lassan kezdik elérni a célzott támadásoknál látott színvonalat. Az ezek elleni védekezésben hatékonyan segíthet, ha tájékoztatjuk felhasználóinkat a jelenlegi phishing kampányokról, illetve támogatjuk elemző csapatunkat a Recorded Future által nyújtott IOC listákkal. (IOC: Indicators of Compromise, fenyegetettségi index.) Ezek fontos információkat szolgáltatnak a fenyegetések észleléséhez és a már bekövetkezett incidensekre való reagáláshoz.

Fontos tudni, hogy a támadók által használt környezetek nagyon gyorsan képesek lekövetni a változásokat, és észlelés után gyorsan új környezetbe költöztethetők. Többek között ez az oka annak is, hogy az identitás alapú visszaélések fénykorukat élik, és nagyon sok esetben a támadók valid felhasználói adatokkal jutnak be a céges környezetekbe. Ebből adódóan egyre többször találkozunk olyan támadásokkal, amelyeket jóval nehezebb észlelni, és ha nincs tudomásunk az esetlegesen kiszivárgott hozzáférési adatokról, a bejutást megakadályozni sokszor szinte lehetetlen. Az ilyen esetekben



FORRÁS: RECORDED FUTURE

a korábban említett IOC-listák mellett a Recorded Future identitás-védelme lehet segítségünkre, amely valós idejű információkra támaszkodva nyújt tájékoztatást a vállalatot érintő kompromittálódott felhasználókról, és képes kielégíteni az erős autentikációs igényeket.

Az említett példák mellett a Recorded Future CTI-platform számos más területen is tudja segíteni a szervezetek működését. A megoldás a geopolitikai információktól kezdve a banki visszaéléseken át teljes körűen lefedi a vállalati kiberhírszerzés felé támasztott igényeket, és a már meglévő (például SIEM, SOAR, XDR) rendszerekkel is integrálható. ■

Recorded Future®

Németh Mónika
senior system engineer

AI-Native hálózatok a Junipertől

Lassan már eljutunk oda, hogy a csapból is AI folyik. Tulajdonképpen az, hogy egy hálózat vagy szolgáltatás mesterséges intelligenciát használ, egyáltalán nem ritka, sőt, mindenki úgy hirdeti a megoldásait, hogy AI-alapú. De vajon hogyan tudjuk a rendszereinkben kihasználni a mesterséges intelligencia nyújtotta előnyöket? Miben és hogyan tud a mesterséges intelligencia segíteni? Mitől lehet az egyik megoldás jobb, mint a másik?

A kérdésekre a választ ott kaphatjuk meg, hogy melyik az a rendszer, amelynek az elemei a legtöbb valós idejű, hasznos információt (például eszközteljesítmény-mutatókat, hálózathasználati statisztikákat, biztonsági naplókat, valós idejű wireless felhasználói állapotokat, routerek/switchek/tűzfalak telemetrikus adatait) tudják az AI-motor felé elküldeni. Ez az egésznek a lelke, hiszen az AI és a gépi tanulás abban tud nagy mértékben segíteni, hogy a rendelkezésre álló adatáradatból sokkal könnyebben tud használható információt nyújtani arról, hogy melyek azok a dolgok, amelyek nem az elvárt szintnek, igénynek megfelelően működnek a hálózatunkban.

Itt jön a nagy különbség. Nem mindegy, hogy a rendszer építőköveinek számító berendezések alapból képesek-e a szükséges információ küldésére, vagy utólagos barkácsolással „vették rá” azokat, hogy dobjanak adatokat az AI felé, amelyeket az feldolgozhat. Az a legjobb, ha az eszközöket úgy fejlesztették ki, hogy ezt a képességet már eleve beléjük integrálták. A **Juniper** által kínál **AI-Native Networking** erre az opcióra épül, vagyis a platformba beépíthető switchek, routerek, tűzfalak, AP-k, stb, már eredendően úgy „születnek”, hogy a mesterséges intelligenciával történő integrálhatóságra képesek. Ezért hívja a Juniper a saját megoldását AI-Native Networkingnek.

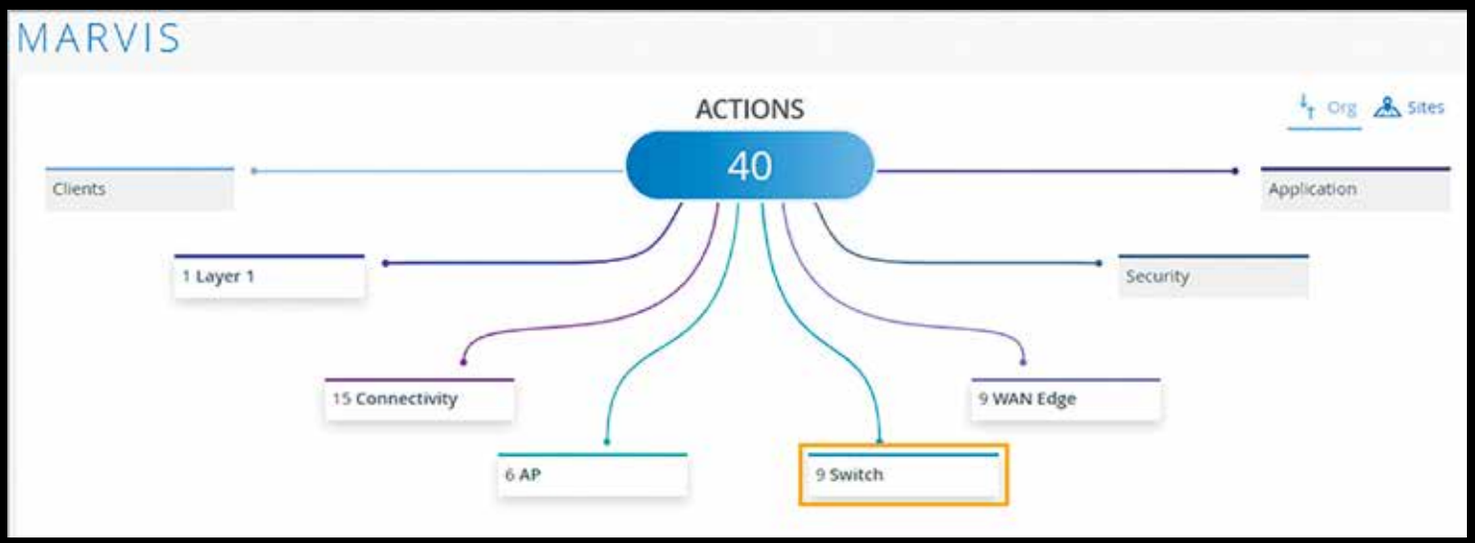
Hogyan működik?

Az AI-natív hálózati rendszereket, mint minden modern AI-rendszert, úgy tervezték meg, hogy tanuljanak a hozzájuk eljutott adatokból, alkalmazkodjanak az új helyzetekhez és fejlődjenek. A folyamatos tanulási képesség alapvető jellemző, amely lehetővé teszi a rendszer hatékonyabbá és eredményesebbé válását, hiszen folyamatosan több adatot és tapasztalatot gyűjt össze.

A megfelelő módon betanított, tesztelt és alkalmazott, mesterségesintelligencia-alapú hálózatok, amilyen a **Juniper Mist** megoldása is, előre látják a problémákat, és proaktívan léphetnek fel a hibák megelőzése érdekében, még mielőtt azokat az üzemeltető vagy a végfelhasználó észrevehetné. Ez időt és erőforrást takarít meg az informatikai és a hálózatos csapatok számára, miközben javítja a működési hatékonyságot és az általános felhasználói élményt.

Például az AI-alapú algoritmusok optimalizálhatják a hálózati forgalmi útvonalakat, képesek a sávszélesség-kiosztás kezelésére, és csökkenthetik a késleltetést. Ennek eredményeképpen megbízhatóbb hálózati teljesítményt kapunk, amely a nagy sávszélességet igénylő alkalmazások számára különösen előnyös. Vagy, ahogy már korábban is írtuk, az

FORRÁS: JUNIPER



AI-natív hálózatok képesek a problémákat előre jelezni, így a karbantartást is proaktív módon tudjuk ütemezni, csökkentve a váratlan állásidőt, és a hibákat még azelőtt ki tudjuk javítani, mielőtt azok a végfelhasználókat érintenék.

De az AI-natív hálózatok képesek a biztonság támogatására is, hiszen a hatalmas mennyiségű hálózati adat valós idejű elemzése lehetővé teszi az anomáliák és a potenciális biztonsági fenyegetések korai felismerését, így a kibertámadások meghiúsításához és az érzékeny adatok védelméhez is jelentős segítséget kaphatunk.

A Juniper AI-natív networking megoldása

Az egész „történet” egy stratégiai fordulattal kezdődött, amikor is áthelyeződött a hangsúly arra, hogy kerüljön az ügyfélélmény az első helyre ahelyett, hogy annyival „megnyugtatnánk” a felhasználót, hogy de hát tudott az AP-hez kapcsolódni. A megfelelő élmények nyújtásához szükséges képesség három alapvető pillérre épül:

- megfelelő adatok,
- megfelelő valós idejű válaszok,
- megfelelő infrastruktúra.

A Juniper a megfelelő kérdések feltevésével kezdi a megfelelő adatok rögzítését, amelyek az egyes felhasználók és munkamenetek szintjéig leásva értékelik a hálózatot. A robosztus algoritmusok és az összes hálózati felhasználó és eszköz valós idejű telemetriája pontos információkat biztosít az IT számára, valamint az üzemeltetők valós idejű válaszokat kapnak a hálózati kérdéseikre.

Marvis, a Juniper rendszerébe integrált virtuális hálózati asszisztens, természetes nyelven válaszol az informatikai kérdésekre, ahogy egy ember is tenné, így nagy mértékben segíti az IT-üzemeltetők hálózattal történő interakcióját. Az eszközök tekintetében a Juniper már évekkel ezelőtt lerakta az AI-natív networking platform alapjait, amikor elkezdett olyan berendezéseket gyártani, amelyek lehetővé teszik a gazdag hálózati adatok kinyerését. Azzal pedig, hogy ezeket az adatokat arra használja fel, hogy jobb üzemeltetői és végfelhasználói élményt nyújtson, új iparági mércét állított fel.

Marvis, segíts!

Ahogy korábban már olvashattuk, a hálózat és az IT-csapat közti kapocs a „Marvis” névre hallgat. Igazából akár úgy is tekinthetünk rá, mint egy élő kollégára, aki mást sem csinál, csak állandóan a hálózat állapotát vizslatja, és segít a hatékony hálózatüzemeltetésben.

Az egyik ilyen funkció, amelyet megtalálhatunk a Juniper megoldásában, az a **„Marvis Actions”.** Segítségével proaktívan azonosíthatjuk a WLAN-, LAN- és WAN-környezetekben előforduló hálózati problémák kiváltó okait. Még a konkrét hiba érzékelése előtt tudomást szerezhetünk például arról, ha valahol hiányzik egy VLAN, rossz kábelek vagy túlterhelt áramkörök vannak.

> Az AI-alapú algoritmusok optimalizálhatják a hálózati forgalmi útvonalakat, képesek a sávszélesség-kiosztás kezelésére, és csökkenthetik a késleltetést.

Újdonságként találkozhatunk a **„Marvis Minis”** funkcióval, amely a hálózati felhasználókat tudja szimulálni, és a felhasználók jelenléte nélkül is észleli azokat a problémákat, amelyek később a valódi felhasználók esetében is bekövetkeznének. Egy másik újdonság, hogy a Juniper kibővítette Marvis társalgási felületét a ChatGPT-vel, így még több, az emberi kommunikációhoz hasonló beszélgetési képességet biztosít. Az integráció következtében különösen nagy segítséget kaphatunk dokumentációs és támogatási kérdések megválaszolásában is.

Ez csak pár példa, további érdekességekről kérdezzük meg inkább Marvist! 😊

■ Juniper driven by Mist AI

Almási Zsolt
CISSP, Engineering team lead

A termelésirányítás digitális biztonsága: TXOne + Forescout

Az elmúlt években egyre többször hangzik el az ipari szakemberek körében egy „démoni” szófordulat, az „IT/OT konvergencia”. A kifejezés nem megfelelő használatával egy füst alatt két terület informatikai szakembergárdáját is magunkra haragíthatjuk. Gyakran azt láthatjuk, hogy az OT-környezeteket hagyományos IT-security eszközökkel próbálják megvédeni a terület biztonságáért felelős szakemberek. Ez egyfelől érthető lehet, de árnyalja a képet, ha megvizsgáljuk az adott komponensek funkcióját és működésének kritikusságát, illetve a rendelkezésre álló erőforrásokat.

Sokszor egy hagyományos tűzfal, vagy végpontvédelmi megoldás beillesztése már olyan mértékben késlelteti egy ipari „process” lefutását, amivel az már nem képes megbirkózni. Egy rossz helyre illesztett, túl szigorú megoldás fizikai kárt, vagy akár személyi sérülést is okozhat. A védelem elengedhetetlen, érdemes tehát körbejárni, milyen lehetőségeink vannak, ha kifejezetten ipari, gyártástechnológiai környezetek (az operational technology, OT) védelmére szeretnénk megoldást választani.

Nyilván olyan védelmi megoldást kell keresnünk, amelyet kifejezetten ilyen körülményekre optimalizáltak: minimális késleltetést visz a folyamatokba, és alacsony az erőforrásigénye. Szerteágazó kérdéskör ez, mert az ilyen megoldások nemcsak egy területet fed(het)nek le, hanem beszélhetünk aktív, passzív eszközökről, illetve hálózati és végponti védelemről is (továbbá még ezer más területről).

Egy passzív megoldás

Általánosságban nagyobb támogatásnak örvend az OT területén, mi magunk is korábban többször bemutattuk a Clico portfóliójában belül a **Forescout EyeInspect** megoldását, amely a hálózati forgalom elemzése alapján képes megjeleníteni az adott környezetekben fellelhető eszközöket. Megtudhatjuk milyen verziójú szoftver/firmware fut rajtuk, és milyen sérülékenységek jellemzik az egyes eszközöket, milyen kommunikáció zajlik a talált eszközök között, és adott esetben segít felderíteni a nem biztonságos protokollok használatát is – mindezt passzív módon. Jelentős előrelépés a gyakran tapasztalható információhiány kezelésében, és mivel elsősorban a tükrözött forgalomból dolgozik a rendszer, nem nyúlunk az eszközökhöz, kivéve olyan esetekben, amikor ez kifejezetten preferált.

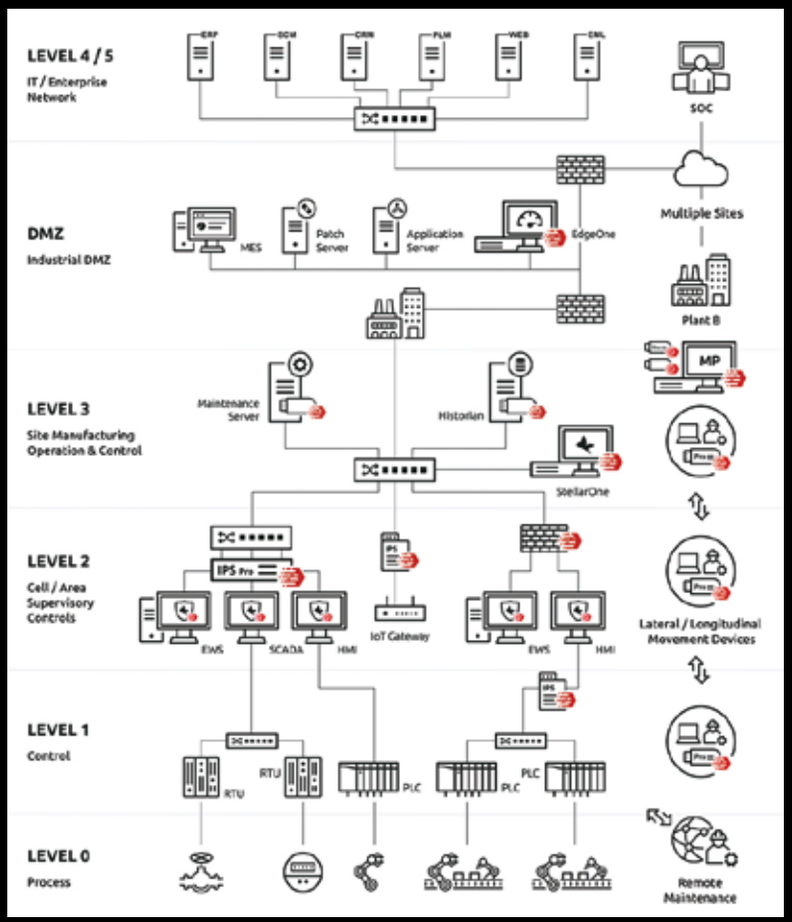
Igény esetén a Forescout megoldását integrálni lehet a gyártó NAC-megoldásával, és ezen keresztül egyéb security eszközökkel is. Maga az EyeInspect akár kétrétegű, központi menedzsmentkonzollal is elérhető, így a különböző telephelyek vagy üzemek rendelkezhetnek saját helyi, illetve egy összesített központi menedzsment konzollal is.

A FORESCOUT MEGOLDÁSA KORÁBBAN „SILENTDEFENSE” NÉVEN VOLT ISMERT. A SECURITYMATTERS NEVŰ, OT-BIZTONSÁG FÓKUSZÚ CÉG FELVÁSÁRLÁSÁVAL VÁLT A FORESCOUT PLAFTORM RÉSZÉVÉ

Be kell avatkozni

Ha a vizibilitás már adott, vagy rögtön olyan eszközt keresünk, amely képes valós időben beavatkozni, akkor az aktív megoldások felé érdemes fordulni. Az OT-specifikus megoldások között találunk egy viszonylag új gyártót, a **TXOne**-t, amely 2019 óta van a piacon. A TXOne a „zero trust” architektúra ipari környezetekre való kiterjesztését tűzte ki célul. A startup jelenleg több, mint 3600 ügyféllel rendelkezik, és mögötte nem kisebb cégek állnak, mint a TrendMicro és a MOXA.

A cél eléréséhez az első lépésünk a beszédes nevű EdgeIPS, IPS-funkciót ellátó megoldások beillesztése a hálózatba. Ezek az eszközök segítenek a hagyományosan lapos és szegmentáció nélküli környezetek mikroszegmentációjában, legyen szó akár egy-két szegmensről/eszközről, vagy akár 48 különböző szegmensről egy eszközön belül. A speciálisan erre a célra gyártott eszközök már a legkisebb modellek esetén is rendelkez-



nek beépített bypass modullal, és redundáns tápellátással, hogy egy esetleges eszköz meghibásodása esetén ne legyen kimaradás.

Fontos jellemzőjük, hogy a hálózati címzés módosítása nélkül 500 µs-nál rövidebb késleltetéssel transzparens módon beilleszthetők a környezetbe. Szükség esetén képesek akár passzívan, monitor módban is működni. A beépített automatikus tanulás használatával pedig a szabályrendszerek megalkotása és a környezetek felderítése is nagyban leegyszerűsíthető.

Az eszközök tulajdonságait és a támogatott protokollokat a gyártástechnológiai (OT-) környezetek sajátosságainak előtérbe helyezésével fejlesztették ki. Ilyen képesség például az ipari környezetek esetén hírhedten elavult szoftverekben található sérülékenységek virtuális patchelése, amivel leállás és frissítés nélkül tudjuk befoltozni a sérülékeny eszközöket. Ezenfelül az OT-specifikus protokollok esetén Layer7-es (művelet szintű) beavatkozási képességgel rendelkeznek. Több eszköz használata esetén az EdgeOne központi menedzsment megoldáson keresztül egy helyen, könnyen használható grafikus felületen keresztül tudjuk elvégezni a különféle beállításokat.

Védjük az öregeket!

Ha az ipari környezetben több legacy Windows-kliens, vagy -szerver alapú eszköz is lapul, akkor érdemes ezek védelméről is gondoskodni, már végpont szinten is. Ezekben a környezetekben a hosszabb életciklusnak köszönhetően az eszközök általában régebbi operációs rendszert futtatnak (esetenként frissítések nélkül), és sokszor minimális szabad erőforrással rendelkeznek. Ezért fontos, hogy speciálisan egy ilyen környezetre kifejlesztett megoldás nyújtson védelmet számukra.

A TXOne portfóliójában ez a **„Stellar”,** amelyet a gyártó a Cyber-Physical System Detection and Response (CPSDR-) kategóriába sorol, ez gyakorlatilag az OT-környezetek EDR-megoldásait takarja. Az agent képes több, mint 8000 különféle OT-specifikus alkalmazás, eszköz és tanúsítvány felismerésére, és akár régi Windows 2000 és XP rendszerek védelmét is képes ellátni. A „hagyományos” támadások mellett fel tudja ismerni az ipari környezettel összefüggő programok és a rendszer elemeinek módosításaira tett kísérleteket, illetve viselkedés alapú védelmet is nyújt. Használatával jól körbebástyázott végpontokat kapunk, akár teljesen elszigetelt (air-gapped) hálózatok esetén is, on-prem működéssel.

Szoftverügynök nélkül is lehet

Ha bizonyos eszközökre nem tudunk, vagy nem szeretnénk végponti agentet telepíteni, akkor érdemes megvizsgálni az **„Element”** termékcsaládot. Akkor is optimális választás lehet, ha csupán egy általunk megbízhatónak ítélt vizsgálatot szeretnénk lefuttatni a környezetünkbe bekerülő eszközöket érintően. Az „Element” családba tartozó eszközök telepítés nélkül futtathatók, USB vizsgáló eszközként használhatók.

A vírusok elleni vizsgálat mellett felmérik az eszközökön található alkalmazásokat, frissítéseket, és ezt képesek megjeleníteni egy központi konzolon keresztül. A „Pro” sorozatú eszközök esetén a képességek még titkosított, és security szempontból átvizsgált tárhellyel is kiegészülnek. A portable inspector kifejezetten hasznos tud lenni például külső karbantartók felügyeletére, de akár a legyártott eszközök szállítás előtti átvizsgálására is használható. Az megoldás a Stellar agenthez hasonlóan akár Windows 2000 (SP3/SP4) vagy XP (SP1) esetén is használható, sőt, Linux-rendszereket is támogat.

Záró gondolatként azt szeretném hangsúlyozni, hogy bár sok esetben a fő prioritás az ipari környezetek üzembiztonsága, nem szabad elhanyagolni a biztonságos működést sem. Javasolt a nagyobb egységeket, amelyek közt a kommunikáció megengedi, robusztusabb védelemmel ellátni, míg a kisebb egységek esetében legalább a vizibilitásra törekedni. ■

txOne networks

Werner Obring
cloud security architect

Cyberark Conjur a biztonságos kulcskezelésért

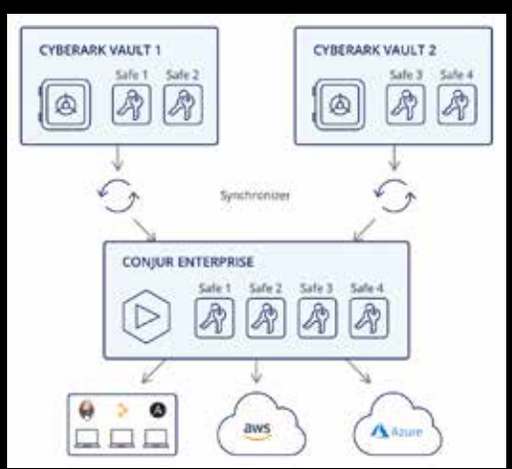
A mai modern DevOps (fejlesztési folyamatok) velejárója, hogy időről időre kiszivárognak érzékeny információk a fejlesztési ciklusban. Ha a fejlesztő nem kellően körültekintő, vagy időnyomás alatt kell teljesítenie, előfordulhat, hogy a kódban felejti a kulcsokat, tanúsítványokat. Ez súlyos adatszivárgás, kritikus applikációkhoz, adatbázisokhoz férhetnek hozzá a támadók.

A GitHub public repository-k jelentős részében lehet ilyen „ottfelejtett" adatokra, API-kulcsokra, jelszavakra bukkanni, sokszor kritikus infrastruktúrához, üzletileg kritikus applikációkhoz biztosítva hozzáférést ezzel a behatolóknak. A GitHub évről évre ellenőrzi, hány „secretet" találnak publikus repository-kban, text formátumban. 2023-ban ez a szám elérte a 2 milliót. Erre az egyre súlyosbodó problémára kínál megoldást a **CyberArk Conjur Secrets Management.**

De hogyan?

Először is fontos megérteni, miért érdemes egy központi kulcskezelési platformot használni. A "secret sprawl" nevű jelenséget így könnyen elkerülhetjük, tehát kiküszöböljük azt a lehetőséget, hogy kulcsaink, jelszavaink és tanúsítványaink össze-vissza, az adott automatizációs eszköz platformján, text formátumban legyenek tárolva. Ez azért fontos, mert így nem adunk lehetőséget a támadóknak arra, hogy hozzáférhessenek nem titkosított kulcsokhoz a környezetünkben, mivel nem is így tároljuk azokat.

A CyberArk Conjur egy automatizált kulcskezelési platform, amely lehetővé teszi a szervezetek számára, hogy biztonságosan kezeljék és oszthassák meg az érzékeny információkat, például jelszavakat, API-kulcsokat és tanúsítványokat. Az alkalmazások, szolgáltatások és konténerek dinamikus környezetében a Conjur segítségével a szervezetek hatékonyan tudják kezelni és védeni a kulcsaikat. Az egyik fő előnye az automatizált kulcskezelés.



A platform lehetővé teszi a felhasználók számára, hogy irányelvek (policy-k) definiálják és vezéreljék, hogy ki, mikor és milyen körülmények között férhet hozzá az adatokhoz. Ezáltal minimalizálja az emberi hibák és a behatolások kockázatát, miközben növeli a kulcsok biztonságát és a megfelelőséget. Titkosítja is a kulcsokat, ezzel elkerülve a text formátumban való tárolást.

Integráció és előnyei

A Conjur széles körű integrációs lehetőségeket kínál olyan népszerű fejlesztési eszközökkel és platformokkal, mint például Kubernetes, Docker, Ansible, Terraform stb. Ezáltal könnyen integrálható a meglévő fejlesztési és DevOps-folyamatokba anélkül, hogy megbontaná azokat. A fejlesztési folyamatok nem lassulnak, a szoftverfejlesztők továbbra is használhatják eddig meglévő kulcstárhelyüket, legyen ez egy Azure Key Vault, Amazon Secrets Manager, vagy egyéb más felhőszolgáltató megoldása. A CyberArk Conjur megoldásának igazi értéke ebben rejlik, teljes átláthatóságot nyújt a környezet meglévő kulcsairól legyen az on-prem, hibrid, vagy felhős környezetben. A fejlesztőnek nem szükséges foglalkoznia azzal, hogy külön a Conjurba helyezze a kulcsot, nem befolyásolja a megszokott fejlesztési folyamatát. A CyberArk emellett számos fejlesztési folyamatot meggyorsító úgynevezett „acceleratort" kínál például Kubernetes kulcsokhoz. (*https://github.com/conjurdemos/Accelerator-K8s-External-Secrets*)

Az adatok felügyeletének központosítása kulcsfontosságú a modern IT-környezetekben, ahol a különféle alkalmazások és rendszerek dinamikusan változnak. A Conjur segítségével a szervezetek egységes, centralizált helyről kezelhetik és monitorozhatják az összes kulcsot, csökkentve ezzel a kockázatokat és növelve az adatbiztonságot. Az automatizált kulcskezelés és a központosított felügyelet mellett a Conjur erős auditálási képességeket is kínál. Ez lehetővé teszi a szervezetek számára, hogy nyomon kövessék és ellenőrizzék, hogy ki és mikor hozzáférést kapott adatokhoz, valamint, hogy milyen tevékenységeket hajtott végre ezekkel az adatokkal. A Conjur naplózza ezeket a tevékenységeket, ezáltal könnyen visszaellenőrizhető milyen esetleges visszaélések történtek, vagy történhettek volna.

A CyberArk Conjur Secrets Management kiváló megoldás a kulcsok hatékony és biztonságos kezelésére. A platform számos előnyt kínál a szervezeteknek, beleértve az automatizált kulcskezelést, a széles körű integrációs lehetőségeket, a centralizált felügyeletet és az erős auditálási képességeket. Ennek eredményeként a Conjur segítségével a szervezetek képesek minimalizálni az adatbiztonsági kockázatokat és javítani az adatvédelmet, miközben megfelelnek a szigorú szabályozási követelményeknek is. ■

CYBERARK®

Almási Zsolt
CISSP,
Engineering team lead

SentinelOne Singularity Platform

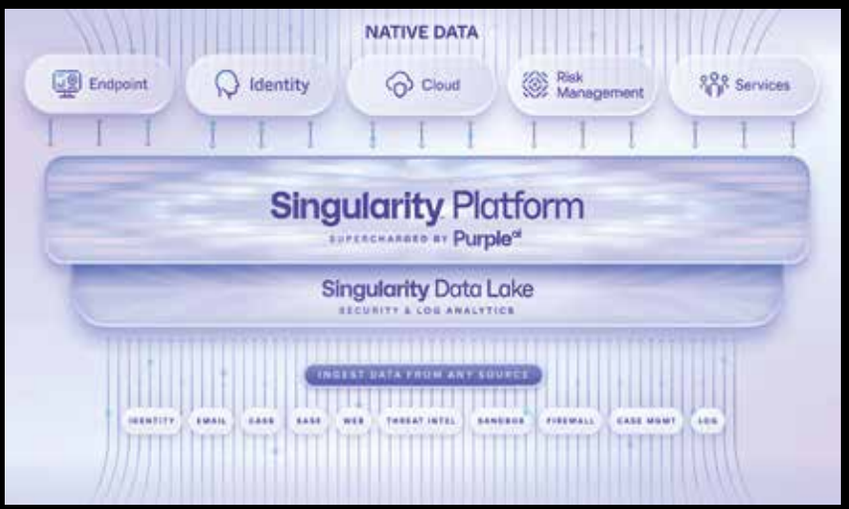
A kaliforniai székhelyű kiberbiztonsági vállalat, a SentinelOne kapcsán állandó vitatéma, hogy miért jobb az XDR, mint egy klasszikus, „old school" végpontvédelem vagy egy EDR/EPP megoldás. Legalább ennyire megosztó kérdés az is, hogy egyáltalán létezik-e az a követelményszint, amelyet minden megoldásnak teljesítenie kell, mielőtt XDR-nek hívnák.

A különféle gyártók megoldásait a saját portfóliójukban már elérhető termékek mentén alakítják ki XDR-jellegű megközelítéseiket. Találkozhatunk hagyományosan NDR, EDR, de akár SIEM vonalról érkező megoldásokkal is – a közös bennük általában az, hogy egy központi konzolon jeleníthetünk meg riasztásokat és egyéb információkat. Megvizsgáljuk, mire képes egy olyan megoldás, amely a folyamatos fejlődést és a mesterséges intelligencia (AI), valamint a gépi tanulás (ML) alapú működést tűzte ki céljául.

A **Singularity Platform** óriási előnye, hogy a központi menedzsmentkonzol több saját megoldást is tartalmaz az elérhető külső integrációkon felül. A SentinelOne legfőbb funkciója kétségkívül az új generációs végpontvédelem, amely operációs rendszertől (legyen az Windows, Linux, és/vagy macOS) függetlenül egységes védelmet biztosít egy központi konzolon keresztül.

Ezek a végpontok bármilyen környezetben futhatnak: lehet akár felhős, akár saját adatközpont is, sőt, a megoldás Kubernetes-környezeteket is képes megvédeni. A platformot könnyen kiegészíthetjük egy hálózati vizsgáló modullal, amely képes felismerni, milyen egyéb eszközök találhatók azokon a hálózatokon, ahol a telepített agenttel rendelkező eszköz is található.

A végpontvédelem egyszerűen kiterjeszthető akár (iOS, Android, ChromeOS) mobileszközökre is, így vállalatunk támadási felülete tovább csökkenthető. A mobil végpontvédelem elsőre nem tűnik kiemelt fontosságú pontnak, de ha belegondolunk, hányszor és hányféle kibertámadással és adathalász-SMS-sel találkozhattunk az elmúlt időszakban, gyorsan újraértékelhetjük a prioritási sorrendet.



Az identitásalapú támadások a ransomware-ektől kezdve egészen a legkülönfélébb célzott támadásokig előfordulhatnak. A Singularity Identity használatával jelentősen növelhetjük a biztonsági szintünket, mivel a modul képes észlelni a céges (AD/AzureAD/EntraID) címtárrendszert érintő támadásokat, illetve javaslatokat tesz a konfigurációs problémákra is. Továbbá képes szimulálni céges környezeteket is, úgynevezett „csali" (decoy, honeypot) rendszereket létrehozva, amelyek megtéveszthetik a támadókat, és megkönnyítik az észlelésüket.

A harmadik fő pillére a megoldásnak a felhős erőforrások és környezetek védelme. Ez egy cloud workload protection (CWPP) megoldásból áll, amely kiterjeszti az on-prem végpontok esetén már ismert és jól bevált védelmet a felhős környezetekre is. Ráadásul a SentinelOne az év elején felvásárolta a PingSafe nevű, teljes cloud security (CNAPP, cloud native application protection) csomagot fejlesztő céget, így hamarosan még több funkció lesz elérhető a platformon belül.

A gyártó egyedülálló módon beépített a megoldásába egy „Purple AI" elnevezésű, mesterséges intelligencia alapú virtuális segítőt, amely többféleképpen használható annak érdekében, hogy a kollégák hatékonyabban tudjanak koncentrálni a lényeges feladatokra. Ilyen többek között a keresések gyorsítása és a különböző találatok értelmezése.

Egyedi SentinelOne-megoldások

Cloud Data Security az S3 bucketek és Netapp tárolók védelmére
A Singularity Marketplace és a Data Lake révén bármilyen külső megoldással integrálható
Egy helyen lehetnek a logjaink és a riasztásaink, bizonyos megoldások esetén a kétoldalú integrációnak köszönhetően akár műveleteket is végrehajthatunk a partner megoldásokon keresztül

Hajabács Balázs
system engineer

Jól csak a Packet Brokerével lát az ember – Niagara Networks

Ahogy a hálózatainkban egyre több adatot tárolunk és mozgatunk egyre növekvő sávszélességi igény mellett, kulcsfontosságú, hogy mindezt hatékonyan tegyük és nem csak kiberbiztonsági szempontból. A hálózati vizibilitás nem boszorkányság; egyszerűen csak arról van szó, hogy minden adatmozgásról, ami a hálózatunkon keresztülmegy, tudomásunk legyen.

Egy komplex hálózati architektúra esetén a láthatóság létrehozása komoly feladat. A NetOps- és SecOps-csapatok hatékony együttműködésének, valamint az üzemeltetési költségek és a kiberbiztonsági kockázatok csökkentésének elengedhetetlen feltétele az átgondolt hálózati láthatóság kialakítása. „Hatékonyság" és „egyszerűség" a két kulcsszó, amely a portfóliónkba frissen bekerült gyártó, az amerikai székhelyű, kizárólag network visibility megoldásokra szakosodott Niagara Networks megoldásait jellemzi.

Network Packet Broker

A cél az, hogy a hálózati láthatóságot 100%-ra növeljük, Le kell választani a vizibilitással kapcsolatos funkciókat hálózatunk switching rétegéről, és létre kell hozni egy dedikált network visibility réteget. Ennek a láthatósági rétegnek a lelke a packet broker, amely egy olyan célhardver (vagy felhős környezetben szoftver), amely képes a network TAP-ekből és SPAN-portokból érkező tükrözött forgalom aggregálására, szűrésére és a megfelelő biztonsági vagy analitikai eszközeink számára történő továbbítására.

A Niagara Networks egyedi megoldása, hogy a packet brokerek extra funkciói a fő funkcióktól szeparáltan egy úgynevezett Packet Accelerator modullal érhetők el. Ez a modul a Packetron, amely lehetővé teszi, hogy az alap funkcióktól szeparáltan végezzük a számításigényes extra funkciókat (mint például packet slicing, packet deduplciation, header stripping, TLS/SSL decryption) ezzel is biztosítva az alapfunkciók zavartalan ellátását. Az extra forgalmi intelligenciák lehetővé teszik, hogy jelentős mértékben tudjuk csökkenteni biztonsági vagy analitikai eszközeink leterheltségét.

Open Visibility Platform

Ha már van Packetron modulunk az NPB-ben, akkor egy újabb Niagara Networks exkluzív funkció

FORRÁS: WIKIPEDIA

is elérhetővé válik: az OVP (Open Visibility Platform). Virtualizált környezetben futtathatunk bármilyen harmadik féltől származó security vagy analitikai szoftvert közvetlenül a Packetron modulon. Ezzel nemcsak egyszerűbbé tudjuk tenni új biztonsági megoldásaink bevezetését, de egyből közvetlen hozzáférést is biztosítunk a fejlett forgalmi intelligenciával szűrt forgalomhoz az adott, külső megoldás számára legyen az egy NDR, Anti-DDoS, WAF vagy éppen egy SIEM megoldás

A Niagara Networks portfóliójában a Network Visibility Layer minden alkotóeleme megtalálható, így aktív és passzív Network TAP-ek, Hybrid Bypass Switchek és felhős környezetekben működő virtuális Packet Brokerek és Network TAP-ek is. Természetesen nem lenne teljes a kép a minden részletre kiterjedő központi menedzsment felület nélkül, ahonnan intuitív módon néhány kattintással beállítható a láthatósági réteg minden alkotóeleme.

Nem elég látni; jól kell látni! Végül a jól implementált network visibility megoldásokkal a Niagara Networks nemcsak egy hatékonyabb és a SOC/NOC csapatok számára könnyebben érthető és kezelhető hálózathoz segít hozzá, de egyben biztonságosabbá és megbízhatóbakká is teszi azokat. ■

NIAGARA NETWORKS

Werner Obring
cloud security architect

Palo Alto Networks Prisma Cloud és Rapid7 InsightCloudSec

A felhőalapú technológiák térnyerése jelentős változásokat hozott az üzleti környezetben, ezzel együtt új kihívásokat is felvetett a biztonság terén. A vállalatoknak ma már nélkülözhetetlen a hatékony felhőbiztonsági megoldások alkalmazása, mivel az üzleti adatok és alkalmazások egyre nagyobb része kerül a felhőbe. Részletesen áttekintjük és összehasonlítjuk a Palo Alto Networks Prisma Cloud és a Rapid7 InsightCloudSec piacvezető felhőbiztonsági megoldásait, kiemelve jellemzőiket és funkcionalitásaikat.

A **Prisma Cloud** jelenleg a piacvezető felhőbiztonsági megoldás a Gartner szerint. A Palo Alto Networks felvásárlásokkal elérte, hogy gyakorlatilag „faltól-falig" felhőbiztonsági platformot kínál az ügyfelek számára. A Prisma Cloud fő elve az egyedülálló shift-left megközelítés: tegyük fel, hogy felhőbe fejlesztünk, ehhez pedig egy DevOps eszközt, egy úgynevezett automatizációs toolt használunk. A Prisma Cloud agentje gyakorlatilag a kód írásakor, még azelőtt, hogy azt futtatjuk, szkenneli a kódot. Nem kell kutakodni sérülékenységek, kódban felejtett kulcsok, félrekonfigurációk után egy produktív környezetben, a Prisma Cloud megteszi helyettünk – még a futtatás előtt. A fejlesztő pedig ebből semmit nem vesz észre, mivel egyáltalán nem lassítja a CI/CD folyamatot.

A Palo Alto Networks hírnevéhez hű marad, ugyanis teljes átláthatóságot nyújt a felhőben lévő hálózatainkról is. A konténerkörnyezetek védelméért a Twistlock felel, amelyet egyébként on-prem is hostolhatunk. Biztosítja a munkafolyamatokat, félrekonfigurációk esetén értesít, és javítási ajánlásokat kínál. Ha egy multicloud környezetet szeretnénk biztonságossá tenni, a Prisma Cloud lehet az ideális megoldás. Kiváló átláthatóságot nyújt a hozzáférésekről, legyen szó gépi vagy emberi jogosultságokról. Megakadályozza a túlzott hozzáféréseket beépített CIEM-megoldásának köszönhetően.

Felhőben futtatott eszköztárunk állapotáról is teljes képet ad, egyszerre nagyjából 4 milliárd eszközről. Több mint 1500 beépített iránymutatásának köszönhetően kiváló képet kapunk felhőkörnyezetünk konfigurációjának állapotáról. Kritikusság szempontjából osztályozza a sérülékenységeket, félrekonfigurációkat.

A legújabb frissítés, az úgynevezett Darwin-release óta a lekérdezési nyelv is megváltozott, a korábbi RQL helyett most már teljesen egyszerű parancsokkal kezelhető a platform. Mindezek a funkciók, a CSPM (Cloud Security Posture Management), a CIEM (Cloud Infrastructure Entitlement Management), a CWP (Cloud Workload Protection), a DSPM (Data Security Posture Management) egy platformban integrálva megtalálhatók. A megoldás képes úgynevezett compliance check-eket kikényszeríteni, olyan erőforrásokra, mint hostok, image-ek, clusterek, vagy akár teljes felhőkörnyezetek. Ezt az előre beépített szabályoknak köszönhetően tehetjük meg. Ha olyan erőforrás található felhőkörnyezetünkben, amelyre egyik szabály sem megfelelő, értesítést kapunk.

A Rapid7 felhőbiztonsági megoldása **Cloud Risk Complete** csomag. Tartalmazza az **InsightVM**-et, az **InsightCloudSec**-et és az **InsightAppSec**-et. Átfogó és erős megoldás ez is, talán a felülete nem annyira kiforrott, felhasználóbarát.

Ennél fontosabb, hogy az InsightCloudSec teljesen agentless, így az integrációja a különböző funkciói között harmonikusabb. A Prisma Cloudnál előfordulhatnak olyan esetek, amikor a mikroszegmentáció és a munkafolyamatok védelmének beállítása egy kicsit több konfigurációt igényel. A Rapid7 különös figyelmet fordít arra, hogy ne csak enterprise méretű környezetekre biztosítson megoldást, így felhőkörnyezetünk növekedésének ütemében skálázható, ami egy feltörekvő szervezet számára óriási előnyt. Az InsightCloudSec hasonlóan kínál CSPM, CIEM, CWP megoldást, tehát elmondhatjuk róla, hogy minden felhős erőforrást képesek vagyunk biztosítani vele.

Ennek a megoldásnak talán az a legjobb része, hogy a kockázatokat, fenyegetéseket valós időben, gyakorlatilag késleltetés nélkül felismeri. Ez teljesen egyedülálló a CNAPP megoldások körében. De ugyanúgy, ugyanazzal a hatékonysággal kezeljük a hozzáféréseinket multicloud vagy hibrid környezetben.

A CWP megoldás gondoskodik a fejlesztési folyamatok biztonságossá tételéről rengeteg integrációt biztosítva automatizációs eszközökhoz, legyen itt szó Terraformról, Ansibleről, vagy bármilyen más, a devopsos kollégák által kedvelt eszközről. A Kubernetes környezetekhez pedig az InsightCloudSec 175 előre beépített kontrolt kínál, ezek custom policykkel bővíthetőek, módosíthatóak.

Egy teljes CNAPP

(cloud native application protection platform)
A Prisma Cloud alkotóelemei:
– Twistlock,
– Redlock,
– Evident.io,
– Aporeto, PureSec,
– Dig Security.

Mindkét megoldás ténylegesen biztonságossá teszi a felhőkörnyezetet, és gondoskodik a megfelelőségi és szabályozási irányelvek betartásáról is. Legyen az a NIS2, DORA, vagy GDPR, ha Prisma Cloudot vagy InsightCloudSecet használunk, egy auditálható, biztonságos felhőkörnyezet tulajdonosai vagyunk. Mindkét megoldás mellett és ellen is szólnak érvek, de a nagy képet nézve mindig az adott környezet méretéhez, komplexitásához és az üzleti igényekhez igazítva választunk megoldást. Jelen állapotában a Rapid7 megoldása talán alkalmasabb lehet egy kisebb, de mégis multicloud környezetre, míg a Prisma Cloud igazi Enterpise környezetekre specializált platform. ■

Almási Zsolt
CISSP,
Engineering team lead

2024-es újdonságok a Palo Alto Networkstől

Az elmúlt időszakban, ha a Palo Alto Networks szóba került, a legtöbb estben az újdonságok és hírek főleg a felhőbiztonságról (a Prisma Cloudról), a SASE-ról (a Prisma SASE-ről) vagy esetleg a SOC-környezeteket támogató megoldásokról (Cortex XSOAR-ról, XSIAM-ról) szóltak. Azonban a mindennapokban még mindig azt tapasztaljuk, hogy a régióban a legnagyobb kereslet a piacvezető újgenerációs tűzfalakra és azokhoz kapcsolódó különféle licencekre van.

A Palo Alto Networks **tűzfal-portfóliója** immár teljesen lecserélődött, jelentősen ki is bővült. Ez amellett, hogy szemmel látható teljesítménynövekedést hozott minden tűzfalkategóriában, azzal a nem elhanyagolható extra előnnyel is jár, hogy az új modellek (és a hozzájuk tartozó „bundle" licencek) árai megérkeztek arra az szintre, amelyet a többi gyártótól a szegmensben már megszokhattunk.

Ha végiggondoljuk, ezzel gyakorlatilag már a kkv-szegmens számára is megfizethető tűzfalakat kapunk a korábban megszokott előnyökkel, mint például a valós idejű párhuzamos feldolgozási képesség az SP3 (Single Pass Parallel Processing) architektúrának köszönhetően, valamint a kiemelkedően jól működő alkalmazásfelismerés (AppID). Ez önmagában is üdvözlendő. Azonban fontos megemlíteni, hogy több speciális új modell is megjelent a portfólión belül.

PALO ALTO NETWORKS PA-450R HÁLÓZATI TŰZFAL

Az első ilyen például a **PA-450R** modell, amely a korábbi, kisebb teljesítményű PA-220R modellt váltja. Az új modell többek között rendelkezik IEC 61850-3 és IEEE 1613 tanúsítványokkal, illetve különféle környezeti behatások ellen (pl.: vibráció, extrém hőmérséklet) is tesztelt. A magas rendelkezésre állás szempontjából a gyártótól már megszokott dupla táp megléte szinte említést se érdemel, viszont a hálózati portok kapcsán fontos megemlíteni, hogy van rajta 2 combo SFP port is, illetve egy bypass port pár is, ami áramkimaradás esetén is képes továbbítani a hálózati forgalmat (ez ipari környezetek esetén kifejezetten hasznos lehet).

Ha tovább nézzük a portfoliót, szintén fontos pár szót ejteni a **PA-415-5G** modellről, amelynek a neve is mutatja különleges képességét: a beépített 5G-modemet, amellyel külső eszköz nélkül képes alternatív útvonal használatával áthidalni egy esetleges szolgáltatói kiesést. Ez a modell főleg kisebb fiókirodák, telephelyek esetén ideális, mivel az 5G-modemen felül még POE képességgel rendelkező portok is találhatóak rajta, amelyekhez például Wi-Fi AP-t vagy tápellátást igénylő IoT-eszközt (például kamerát) is csatlakoztathatunk.

A negyedik generációs eszközökről összességében érdemes tudni, hogy már mindegyiket felkészítették a jövő kihívásaira és támogatják a gyártó által fejlesztett legújabb, gépi tanuláson (ML-en) alapuló szolgáltatásokat, amelyekkel a támadások precízebben kiszűrhetők.

A szolgáltatások esetén is történt néhány, említésre méltó újítás. Megjelent a **„core security bundle"**: ez a licenccsomag költséghatékony módon egyben tartalmazza a legfontosabb biztonsági előfizetéseket, nem szükséges „a la carte" módon összeválogatni. Ezek: Advanced Threat Prevention, Advanced Wildfire, Advanced URL, DNS, SD-WAN.

A Palo Alto Networks elkötelezett amellett, hogy egy nagyobb IT-biztonsági platformot építsen ki, és egységes megoldást kínáljon, amely több különálló eszköz kiváltását tenné lehetővé. Ez az elmúlt időszakban nagy vihart kavart, például a tőzsdei körökben, ám a különféle elemzőcégek rendületlenül kitartanak a Palo Alto Networks vezető szerepe mellett.

Új, központi management-megoldás

A Strata Cloud Manager felhős központi felületet nyújt, ahol a gyártótól származó összes hálózatbiztonsági megoldásunkat (PA sorozatot, VM/CN sorozatot, Prisma SASE-t) egy helyen kezelhetjük. Az általánosan megszokott központi menedzsmentképességeken felül az AI-Ops is a részét képezi, amely alapvetően egy telemetriás adatokra és gyártói bevált javaslatokra építő megoldás. Az általa nyújtott, például konfigurációs javaslatokat is rögtön egy helyen láthatjuk.

Foki Tamás
senior system engineer

Vectra.AI XDR

Tavaly már bemutattuk a mesterséges intelligenciát hatékonyan használó NDR-gyártónkat, a Vectra céget. Akkor elmondtuk, a Vectra.AI-nak teljesen új a megközelítése a hálózati támadások észlelésére és kezelésére. Most szeretnénk a platform további képességeit és integrációs lehetőségeit is bemutatni.

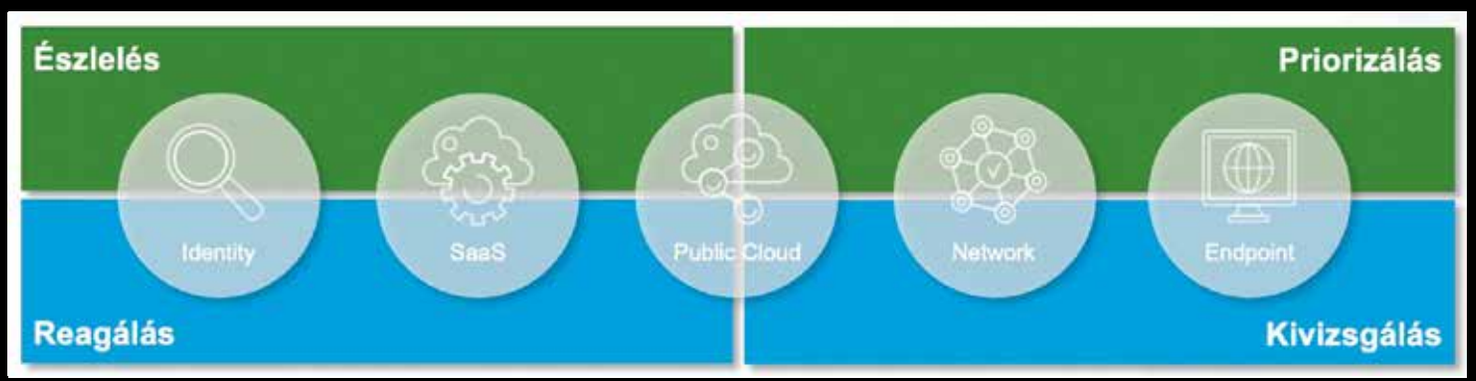
A Vectra legnagyobb különbsége a versenytársaihoz képest, hogy fejlett AI-technológiát használ, amely képes tanulni a hálózati viselkedésből, és folyamatosan karbantartott és fejlesztett modelleket használva felismeri az anomáliákat és támadási mintákat.
A titkosított kapcsolatok bontása nélkül is képes detektálni a nemkívánatos tevékenységek jeleit, mondhatni „átlát" a titkosításon, és bár a tényleges adattartalmat természetesen nem látja, de a kommunikációs mintázatokból felismeri a gyanús tevékenységeket. Ezáltal a hálózati forgalmak vizsgálatához megtakarítja a bonyolult és drága csomagbontási műveleteket. Az AI a detektáláson kívül a kockázatok alapján rangsorolja is a tevékenységeket, ezzel is csökkentve az elemzők terhelését.

A kiterjedt integrációs támogatásnak köszönhetően a Vectra is képes XDR funkcionalitás megvalósítására. Képes végpontvédelmi gyártók telemetriai adatait is beépíteni a saját, hálózati forgalmi észlelései mellé, de VMware felől, vagy akár felhős integrációk révén MS365-ből, AWS-ből, Azure-ból is képes adatokat fogadni, valamint címtárintegrációk (Active Directory, EntraID) is lehetségesek. Ebből a sokféle információból részletes, pontos észlelésekre képes. Ezeken az adatokon az elemzők kiterjedt nyomozásokat tudnak végezni, az egyes hálózati eseményekhez tartozó extra információkkal platformon belül képesek végponti eszközökön futó processeket, file server műveleteket, identity eseményeket, de akár felhős környezetekben történt változtatásokat (pl. egy AWS erőforrás konfigurációjának megváltoztatását) is összerendelni egyetlen incidens kapcsán. Ezekkel a képességekkel a korábbiaknál sokkal teljesebb képet tudnak alkotni az incidensek kivizsgálása során.

A másik integrációs lehetőség, amelyre szeretnénk felhívni a figyelmet, az a Niagara Networks megoldásaival kapcsolatos együttműködés. A Niagara Networks egy hálózati láthatósági megoldásokra specializálodott cég. Többek között hálózati TAP-eket, packet brokereket, és bypass switcheket fejleszt. A cég megoldásait használva nagy mértékben egyszerűsíthetjük a Vectra szenzorainak hálózati forgalommal való ellátását.

Egy packet broker használata nagy segítség lehet, főleg egy olyan környezetben, ahol több fajta eszközt is el kell látni a hálózati eszközök forgalmával. Itt érdemes egy komolyabb biztonsági infrastruktúrára gondolni, ahol például NDR mellett IPS, DLP, proxy (és sok más) megoldást is használnak, esetleg teljes hálózati forgalom rögzítését igénylik. Sok esetben ilyenkor egy packet broker rendszer bevezetésével jelentős költségmegtakarítást, a forgalmi torlódások elkerülését és nem utolsósorban a hálózati komplexitás csökkenését érhetjük el.

Az optimalizáció mellett figyelemre méltó a Niagara Networks Packetron platformja, amely egyetlen hardveren teszi lehetővé a packet broker funkcionalitást, valamint third party virtuális alkalmazások futattását. Használatával például egy Vectra vSensort is tudunk a Packetron eszközön futatni, amivel az infrastruktúra tovább egyszerűsíthető.



A most bemutatott XDR-funkcionalitás, illetve a Vectra.AI egyedi AI alapú működését figyelembe véve kijelenthető, hogy a megoldás használatával jelentősen csökkenthetjük a hálózati forgalom elemzésével járó terhelést az IT-biztonsági csapataink számára és nagyban növelhetjük a hatékonyságukat.

VECTRA®

CLICO

MAGYARORSZÁGI PORTFÓLIÓ:

ARISTA
ARMIS
COMMSCOPE® | RUCKUS®
CLOUDFLARE
CLOUDIAN®
cryptme
CYBERARK®
DIGI
exabeam
Fidelis Cybersecurity
Forcepoint
<) FORESCOUT
GREYCORTEX
imperva
Infinera
ivanti
JUNIPER driven by Mist AI
MICROSENS euromicron group
N CIPHER AN ENTRUST DATACARD COMPANY
netskope
nextsense
NIAGARA NETWORKS
opengear A DIGI COMPANY
paloalto NETWORKS
POINTSHARP
radware
RAPID7
Recorded Future®
rubrik
SailPoint
SCIRGE
SentinelOne
THALES
tufin
txOne networks
VECTRA®
XM Cyber
yubico

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

HUMANFIELD

EXECUTIVE SEARCH | SPECIALIST SEARCH

AZ IT-VEZETŐK ÉS SPECIALISTÁK FEJVADÁSZATÁNAK PIACVEZETŐ SZAKÉRTŐJE

WWW.HUMANFIELD.HU

ITBUSINESS

ITEXEC

DIGITALIZÁCIÓ I ADATELEMZÉS I MI I ÜGYFÉLÉLMÉNY

2024.05.30-31.

Thermal Hotel Visegrád