informatikáról üzleti döntéshozóknak XX. évfolyam 5. szám 2022. május 3. Ára: 2990 Ft www.itbusiness.hu

ITBUSINESS

A Clico csapata

A CIO ÉS CISO EGYÜTT GARANTÁLJÁK A VÁLLALAT BIZTONSÁGÁT

ÉPÍTSÜNK ERŐS REZILIENCIÁT A KIBERBIZTONSÁG TERÜLETÉN!

ITBUSINESS előfizetés

Kedves Olvasó!

Ha úgy érzi, hogy értékes és hiteles szakmai tartalmakat talál magazinunkban, és a jövőben is szeretné kézhez kapni a havi szakmai olvasnivalót, szívesen vesszük előfizetési igényét.

Előfizethető a kiadó ügyfélszolgálatán: *elofizetes@itbusiness.hu*

Az ITBUSINESS magazin egy éves (12 havi) előfizetésének díja: 19 900 Ft + áfa

(Ajánlatunk csak belföldi kézbesítésre érvényes.)

ITBUSINESS

FORRÁS: 123RF.COM

Mindenkinek Mohács kell?

A veszély, a fenyegetettség érzése evolúciós okokból rendkívül erős hajtóerő mindenféle azonnali cselekvéshez. Minél közelebbi és minél húsbavágóbb a veszély, annál nagyobb a hajtóerő, annál hevesebb a reakció és annál nagyobb a veszély elhárítására fordított erőforrás. (Az oroszlánfalka által kergetett zebra nagyon-nagyon gyorsan tud futni…) Ezzel együtt a fenyegetettség érzését is meg lehet szokni, különösen, ha a kockázat egyszer sem jár káros következményekkel. A madárijesztő az első nap még meghátrálásra készteti a seregélyeket, de ha amúgy nem történik semmi, pár nap múlva boldogan pihen meg rajta az egész csapat, ha már eltelt a szőlővel.

Nem, nem tévedt el a kedves olvasó, nem egy természeti ismeretterjesztő magazint olvas, hanem valóban az ITBUSINESS májusi számát. A téma pedig úgy kerül ezekre a hasábokra, hogy a fent említett mechanizmus nemcsak az állatvilágban és nemcsak az életveszély elhárítása esetén működik – hanem például az IT-biztonság terén is. Az információbiztonsági szakemberek (és velük kórusban a szakmai újságok, újságírók) időtlen idők óta figyelmeztetnek a kibertámadások veszélyére. Talán túlságosan régóta is. Bár a kockázat tényleg valós, saját bőrükön (informatikai infrastruktúrájukon, adataikon, pénztárcájukon) viszonylag kevesen érezték meg, hogy milyen következményekkel jár egy komoly hackercsapás. A tényleges következmények nélküli riogatás pedig sokak érzékenységét eltompította. „Talán nem is akkora a veszély, mint mondják, és fölöslegesen költök olyan sokat az IT-biztonságra”, gondolhatta a CEO, a CFO – rosszabb esetben a CIO.

Az orosz-ukrán háború és annak kibertérben vívott ága viszont olyan kézzelfogható közelségbe hozta a veszélyt, mint eddig semmi más. Amikor a hackerek tevékenysége már a tömegmédiában is vezető hírnek számít, az áldozat pedig nem egy távoli ország soha nem hallott cége, hanem Oroszország nemzeti bankja vagy egy belorusz fegyvergyár (hogy a többiről ne is beszéljünk), a nyilvánosságra került bizalmas adatok mennyisége pedig már terabájtokban mérhető, a mégoly nyugodt vállalatvezető szeme is felnyílik, és ösztönei ismét veszélyt jeleznek. Ha ők prédául eshetnek, akkor mi sem vagyunk biztonságban! A (végre) felismert veszély pedig cselekvésre sarkallja – feltámad benne az érdeklődés a kockázatok elemzése, a megfelelő védekezés és általában, a szervezet biztonságtudatosságának növelése iránt. Ha pedig így jár el, az már fél siker, hiszen ha a szándék megvan, a védelem kiépítése nem akkora ördöngösség.

„Nekünk Mohács kell!” – utal a régi mondás arra, hogy a többség csak a katasztrófa után kap észbe. A szomszédunkban most egyszerre sok Mohács zajlik, tanuljon mindenki azokból, ne várja meg, amíg a nyakába szakad a saját Mohácsa. A katasztrófa elkerüléséhez pedig mostani lapszámunkból is kellő muníciót szerezhet mindenki.

SCHOPP ATTILA,
FŐSZERKESZTŐ

ITBUSINESS

COVER STORY

STRATEGY

ICT-MARKET

TECHNOLOGY

ITEXEC

HUMAN

CLICO MELLÉKLET

#696. ITBUSINESS 2022. május

SZERKESZTŐSÉG
Főszerkesztő
Schopp Attila – aschopp@itbusiness.hu

Felelős szerkesztő
Kiss Franciska – fkiss@itbusiness.hu

Vezető szerkesztő
Kenczler Mihály – mkenczler@itbusiness.hu

Szerkesztők
Kalocsai Zoltán – zkalocsai@itbusiness.hu
Vass Enikő – evass@itbusiness.hu

Tervezőszerkesztő
Papp Gyula – gypapp@itbusiness.hu

Fotó
Teszár Ákos – texakos.foto@gmail.com

ITEXEC üzletág-igazgató
Mester Sándor – smester@itbusiness.hu

Sales igazgató
Bakos Gergely – gbakos@itbusiness.hu

Event manager
Kardos Beatrix – bkardos@itbusiness.hu

Sales
sales@itbusiness.hu

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

Kiadóvezető: Klenner Linda – lindaklenner@itbusiness.hu

ISSN 1589-3464

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

Előfizetési díjak
Egyéves (12 lapszám): 19 900 Ft + áfa
Továbbá előfizetésben terjeszti a Magyar Posta Zrt.
hirlapelofizetes@posta.hu

Digitális előfizetés
ugyfelszolgalat@digitalstand.hu
ugyfelszolgalat@dimag.hu

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

1139 Budapest,
Frangepán utca 7.

Az ITB kiadói feladataihoz a MiniCRM ügyfélkezelő rendszert használja, amelyet a szoftver fejlesztője és forgalmazója, a MiniCRM Zrt. biztosít számunkra.

ITBUSINESS

A CIO ÉS CISO EGYÜTT GARANTÁLJÁK A VÁLLALAT BIZTONSÁGÁT

Építsünk erős rezilienciát a kiberbiztonság területén!

A zsarolóvírusos és a DDoS-támadások jelentik a vállalatok számára a legnagyobb kiberbiztonsági fenyegetést, ezek a támadások örökzöld slágerként az előttünk álló időszakot is meghatározzák. A vállalatok felismerték, hogy az IT-infrastruktúra és a vállalati adatvagyon érték, amelyet védeni kell, azonban sok esetben az IT biztonsági szakemberhiány mindezt megnehezíti. *Csinos Tamás,* a CLICO Magyarország country managere szerint a CIO-nak és a CISO-nak vállvetve, egyforma erőfeszítéssel kell figyelnie a szervezet IT biztonságára. A kiberbiztonsággal foglalkozó vállalatok felelőssége megmutatni a cégeknek, hogyan tudják bölcsen elkölteni a védekezésre szánt összegeket.

FORRÁS: 123RF.COM

– Milyen trendek határozzák meg kiberbiztonság területén az előttünk álló évet?

– A két örökzöld trend, a zsarolóvírusos támadások és a DDoS-támadások idén is meghatározzák a kiberbiztonság területét. Ezek a fenyegetések mostanra eléggé összetett támadási formává értek. A hagyományos támadási módszerekről elég régóta beszél a szakma. Szerencsére a vállalatokhoz is eljutott az üzenet, így már ismertek a védekezési technikák is. A szervezetek azt is tudják, hogy a vírusvédelem és a tűzfal önmagában nem elég a hatékony védelemhez, hajlandóak más technológiákba is invesztálni.

A másik örökzöld támadási forma, a szolgáltatások ellehetetlenítése, megtagadása, vagyis a DDoS, gyakran a ransomware-támadásokat felerősítve jelentkezik. A bűnözők egy alacsonyabb intenzitású DDoS-támadással sebzik meg a vállalatot, majd jelzik, hogy a váltságdíj elmaradása esetén egy nagyobb lökéshullámmal teljesen ellehetetlenítik a szervezetet. Egyre több potenciális célpont, főleg az üzleti szférából, ismeri fel, hogy az ilyen támadásokra is fel kell készülni. Szerencsére a magyar piacon is megjelentek az előremutató védekezési törekvések. A vállalatok egyre gyakrabban nem attól az infrastruktúra-szolgáltatótól vásárolnak védelmet, amelynek az infrastruktúráján keresztül egyébként is érkezne a támadás, hanem egy független, felhő alapú biztonsági szolgáltatást vesznek igénybe.

– Hogyan befolyásolja ezeket a trendeket az orosz-ukrán konfliktus?

– Sajnos, azt kell mondani, hogy mindkét fél önkéntesek ezreit mozgósította sikeresen, akik egymás IT-infrastruktúráját kóstolgatják és támadják. Nemcsak Oroszország vagy Ukrajna területéről érkeznek ezek az önkéntesek, hanem szinte a világ minden pontjáról harcolnak egyik vagy másik oldalon. A háborúnak egyszer vége lesz. Nem tudjuk, hogy ebben a virtuális harcban megedzett és leszerelt „katonák” a harc végén mire és hogyan fogják képességeiket felhasználni. A fehér vagy a fekete oldalra állnak át? Egy ilyen tömeg megjelenése a kiberbűnözői oldalon plusz kockázatot jelenthet a vállalatok biztonsága szempontjából.

FORRÁS: CLICO MAGYARORSZÁG

CSINOS TAMÁS, CLICO

– Az említett slágertámadások egyben a leggyakrabban előforduló fenyegetettségek is?

– Majdnem minden más támadási technika és eszköz gyakorlatilag a zsarolóvírusos és a DDoS-támadásokat készíti elő. Az általános hadászatból is ismert Kill Chain szerint egy kibertámadásnak is több fázisa van: az első a felderítő üzemmód, ahol körbetapogatják a célpontot,

> Magyarországon nincs olyan jellegű szabályozás, amely egyértelműen kötelezővé tenné a vállalatoknak, hogy a támadásokat széles nyilvánosságra hozzák

majd bejutnak a rendszerekbe, kiépítik az oda-vissza menő kommunikációs kapcsolatokat, megtalálják az aranytelért, vagyis a védett vállalati adatokat, majd a command és control központ felé kilopják ezeket adatokat. A különböző fázisokban különböző támadási technikákat használnak a kiberbűnözők. Majdnem minden incidens végső soron zsarolóvírusos támadásban vagy DDoS támadásban ér véget, hiszen a bűnözők ezekkel tudnak pénzt keresni.

Például ahhoz, hogy bejussanak a rendszereinkbe, sok esetben adathalász támadást indítanak a támadók. Zárójelben jegyzem meg, hogy a phishing támadások ellen a magyar felhasználók a támadók nyelvi nehézségei miatt korábban védettek voltak, a rossz magyarsággal megírt levélnek kevesen dőltek be. Azonban ennek a kornak is vége, a mostani adathalász-támadásokban magyar anyanyelvűek segítségével tökéletesen megfogalmazott csalilevelek születnek.

– Kevés Magyarországon a kibertámadás vagy csak nem hallunk róluk?

– Sajnos, a hazai vállalatokat is ugyanolyan intenzitással érik a kibertámadások, mint a külföldi cégeket. Azonban itthon nincs olyan jellegű szabályozás, amely egyértelműen kötelezővé tenné a vállalatoknak, hogy a támadásokat nyilvánosságra hozzák. Sok szabályozó testülethez, még több hivatalhoz kell bejelenteniük a támadás, adatszivárgás tényét a szervezeteknek, de a fogyasztókkal, ügyfelekkel vagy partnerekkel mindezeket nem közlik. Senki sem éli meg vállalata büszke pillanataként azt a percet, mikor sikeres zsarolóvírusos támadások áldozataivá váltak.

– Hogyan változna meg az IT-biztonság, ha amerikai példára itthon is nyilvánosságra kellene hozni ezeket?

– Az biztos, hogy a kibervédelemmel foglalkozók munkáját nagyban segítené. Sok esetben küzdünk azzal, hogy a vállalatok nem ismerik fel, vagy csak későn, hogy szükségük van IT-biztonságra, IT-védelemre. A nyilvánosság abban is segítene, hogy több fiatal fordulna az IT-biztonság terü-

lete felé, és választaná ezt szakmájává. Szerintem az IT-nek globálisan is az egyik legnagyobb kihívása az elkövetkező tíz évben, hogy nincs és nem is lesz megfelelő mennyiségű IT-biztonsági szakember.

– Van elegendő pénzük a vállalatoknak a kibertámadások elleni védekezésre?

– Azzal már tisztában vannak a vállalatok, milyen értéket jelent az IT és az adatok. Nincs, vagy nagyon kevés az olyan hazai vállalat, amelynek ne lenne valamilyen szintű IT-infrastruktúrája, az ácsnak vagy a burkolónak is van legalább egy weboldala vagy email-címe. A digitális eszközök olcsó és hatékony munkavégzést, kommunikációt tesznek lehetővé.

A digitalizáció az üzletmenet része. A cégvezetők elgondolkodtak, milyen értéket teremtenek az IT-eszközök és hogy ezek kiesése milyen mértékű kockázatot jelent a szervezetnek. Mérettől függetlenül, mindenhol foglalkoznak a témával, már egy mikrovállalatnál sem meglepő, ha tűzfalra van szüksége.

Mindenképp üdvözlendő, hogy kezd valamilyen szintű tudatosság kialakulni IT-biztonság kapcsán. Hogy ez milyen minőségű védelmi intézkedéseket hoz magával, mennyire mélyrehatóan, az cégméret- meg vertikumfüggő. Más a kockázati szintje a burkolással foglalkozó cégnek és annak a pénzügyi szervezetnek, amely most jelentette be, hogy neobankot indít. Minden vállalatnak kockázatarányosan érdemes a kiberbiztonsággal foglalkoznia, a kockázatok mértékének megfelelően kell erre a területre pénzt költenie.

– Bölcsen költik el ezeket az összegeket a cégek?

– A hozzánk hasonló, kiberbiztonsági termékekkel foglalkozó vállalatok felelőssége is egyben, hogy bölcsen tudják ezeket a pénzeket elkölteni a szervezetek. Nemcsak termékekkel, hanem tapasztalattal is kereskedünk, ez nem titok. Noha disztribútorként nem állunk közvetlen kereskedelmi kapcsolatban a végfelhasználókkal, nagyon sokszor beszélünk viszonteladó partnereink ügyfeleivel. Tanácsadóként fölmérjük az igényeket, beszélgetünk a fájdalmaikról, a problémáikról, a kockázataikról. Sok esetben azonban a kiválasztott megoldásról le kell beszélnünk az ügyfelet. Megértjük, hogy a kiválasztott védelemre ténylegesen szükség lenne, és rendkívül jó megoldást adna az adott problémára. Viszont azt is látjuk, hogy az ügyfél szervezete egyszerűen nem elég érett a kiválasztott technológiára és megoldásra, nincsenek meg azok a folyamatok és az az emberállomány, minőségben és mennyiségben egyaránt, amelyek ezeknek az eszközrendszereknek az üzemeltetésére kellenének.

A nyilvánosság a munkerőhiányon is segíthetne, lehet, hogy több fiatal fordulna az IT-biztonság területe felé, és választaná ezt szakmájává

A bölcsességbe az is beletartozik, hogy a saját kapacitásait is fel tudja mérni az ügyfél. Kiberbiztonsággal foglalkozó cégként a mi feladatunk minderre rávezetni őket.

Korábban már említettem, de hangsúlyoznom kell: a kiberbiztonsági beruházások fogaskerekei között a szakemberhiány az egyik ék. Imádunk új védelmi eszközöket eladni, hiszen ebből élünk. Azonban ha azt látjuk, az ügyfél HR-oldalon nincs a beruházás üzemeltetésére felkészülve, akkor inkább nemet mondunk. Megfelelő szakértelem hiányában sikertelenségre van ítélve a projekt. Nem szeretnénk az a szállító lenni a piacon, amely ehhez a nevét adja. Vannak, akik emiatt megsértődnek, de előbb-utóbb beismerik és elfogadják az általunk kínált megoldást.

A kiberbiztonság területén fellépő szakemberhiány sok területet érint. Például itthon talán a pénzügyi szektor a legszabályozottabb IT-biztonság szempontjából, eszközök tekintetében ők vannak a legjobban ellátva. De őket is ugyanúgy sújtja a szakemberhiány, ami a biztonságtudatosságot is komolyan befolyásolja.

– A biztonságtudatosság kiépítése is HR-kérdés, ezen a területen hogy állnak a vállalatok és a cégvezetők?

– Azt tapasztaljuk, iparágfüggő, hogy a vállalatok hogyan is viszonyulnak a biztonságtudatossághoz. Vannak olyan iparágak, ahol a vállalatvezetők szerintem elég biztonságtudatosak, pontosan és jól becsülik vagy becsültetik fel saját kockázataikat. Hogy utána mennyire tudnak védelmi intézkedésekre költeni, vagy hogy ezeknek a kockázatbecsléseknek milyen védelmi megoldás szintű megvalósulásai vannak, az megint egy másik történet. Mindezt a technológia szállítója tudja pozitív irányba befolyásolni.

A vezetők szintjén a biztonságtudatosság már megvan. Azt látjuk, sok helyen a CISO-t kiveszik a CIO alól, és az informatikai vezetővel egyenrangú félként a legfelsőbb vezetőnek közvetlenül jelent. Az IT-biztonság kérdésköre van annyira fontos, hogy valamilyen szinten az informatikát is felügyelje. Nem tartom jónak, ha a CIO és CISO között alá-, fölérendeltségi viszony van. Ideális esetben ez a két vezető egyenrangú fél, hiszen a két területnek vállvetve, egyforma erőfeszítéssel kell dolgoznia a vállalat IT-biztonságán.

Miután a vezetők szintjén már létezik biztonságtudatosság, az alkalmazottak szintjét kell erősíteni. Ezzel ugyancsak kockázatarányosan kell foglalkozniuk a vállalatoknak. Ennek egyik összetevője a vezetők példamutatása, de rengeteg új megoldás és technológia létezik, amelyek teszteléssel, oktatással vagy játékosan növelik a kollégák biztonságtudatosságát. A HR-nek a CISO-nak együtt kell kidolgoznia az alkalmazottak számára leghatékonyabb programokat.

– Aranyszabály nem létezik, de hogyan védekezzenek a vállalatok a kibertérben?

– Erős rezilienciát kell kiépíteni kiberbiztonság területén, amit a kockázatarányos védelmi technológia és biztonságtudatosság szinten tartásával érhetünk el. Elképzelhető, hogy letapogatják a támadók a rendszerünket, megnézik, hogy milyen megoldásaink vannak. Amikor azonban látják, hogy milyen kiberbiztonsági rezilienciát építettünk ki, akkor könnyen elképzelhető, hogy a kisebb erőfeszítéssel bevehető célpontok felé fordulnak.

IT-rendszereink legyenek naprakészek, a folyamatokat az IT-biztonságot szem előtt tartva építsük ki. Legyen tisztában a szervezet azzal, hogy pontosan hogyan is kell a támadások ellen védekezni. Lehetőség szerint használjon a vállalat olyan új technológiájú védelmi rendszereket, amelyek fel vannak készülve a modern támadási formákra. A 15 évvel ezelőtt kitalált védekező eszközöket érdemes lecserélni az azóta többszörösen átalakult és megújult rendszerekkel, amelyek sokkal hatékonyabban veszik fel a harcot az ismeretlen fenyegetettségekkel szemben is. A már említett biztonságtudatosságra is érdemes időt és pénz szánni, hiszen ha csak egy adathalász levélre nem kattint az alkalmazott, máris megtérült a befektetés.

Vass Enikő

DIGITÁLIS SIVATAG

240 milliárd dollár tűnhet el az ICT-piacról a háború miatt

FORRÁS: 123RF.COM

Egyelőre felbecsülni is nehéz, hogy mekkora kárt okoz az egész világnak az orosz-ukrán háború. Az IDC szerint a globális ICT-piac még akkor is 240 milliárd dolláros kieséssel számolhat, ha egy éven belül befejeződnek a harcok. Az oroszok támadása és a nyomában járó szankciók miatt a technológiai szektorból is számos cég döntött úgy, hogy kivonul Oroszországból, és ez, valamint az ukrán IT-szakemberek kiesése azt eredményezte, hogy rövid idő alatt több százezer szoftvermérnök tűnt le a piacról. Pótlásuk várhatóan kemény árversenyt hoz majd, még nagyobb globalizációra és a szoftverfejlesztési projektek és IT-szolgáltatások további drágulására kell felkészülni.

Napjainkra már igencsak kitartónak kell lennie annak, aki végig szeretné böngészni az orosz piacot teljesen elhagyó, vagy ottani tevékenységét jelentősen csökkentő globális nagyvállalatok listáját. Több, folyamatosan frissülő összesítést is készítenek világszerte, amelyek alapján az látszik, hogy már jóval 700 fölött lehet az így döntő társaságok száma. Az orosz-ukrán háborúra adott reakciót egyrészt az agresszorral szembeni szankciók, másrészt a fogyasztók elvárásai váltották ki, illetve néhány cég esetében maguk az orosz hatóságok tiltása vezetett a szakításhoz.

Fókuszba kerül a biztonság

Cikkünk írásakor nem voltak arra utaló jelek, hogy a harcok belátható időn belül véget érnek, így értelemszerűen a kutatócégek, tanácsadó vállalatok dolga is rendkívül nehéz, ha megpróbálják felbecsülni, milyen hatásai lehetnek a háborúnak. Az IDC április elején megfogalmazott egy prognózist az európai és a globális infokommunikációs piacra vonatkozóan, az anyagban „rövid háborúval" számoltak, vagyis azzal, hogy a harcok 3-12 hónapig tartanak majd. Az elemzés szerint, ha ez a forgatókönyv valósul meg, akkor a 2022 és 2025 közötti időszakban az európai ICT-piacon a költéseket 143 milliárd, míg globális szinten 240 milliárd dollárral csökkenti a háború. Ez jelentősen lefékezi a szektor fejlődését. A kutatócég szakértői azzal számolnak, hogy az európai ICT-költések idén 2 százalékkal bővülnek majd, és elérik az 1052 milliárd dollárt. A háború előtt kiadott előrejelzésben még ennél jóval nagyobb mértékű, 3,7 százalékos fejlődés szerepelt.

A helyzet egyébként nem érinti egyformán az ICT-piac egyes szegmenseit. A kutatócég várakozásai szerint az üzleti szektorban jelentősen visszafogják majd az eszközbeszerzéseket, kevesebb számítógépet és okostelefont vásárolnak, így ezen a területen idén akár 6 százalékos csökkenés is lehet. A vállalati szoftverek esetében viszont továbbra is komoly keresletre számítanak az IDC-nél és alaposan megdobhatja a kiberbiztonsági alkalmazások, szolgáltatások és eszközök iránti keresletet a háború.

Bár a korábban várt kemény összecsapás a kibertérben eddig elmaradni látszik – legalábbis a nyilvánosságot elérő információk alapján –, mind az üzleti szektor, mind a kormányzati szféra igyekszik bebiztosítani magát Európában, és frissíteni, ellenállóbbá tenni a védelmi megoldásait. Az IDC várakozásai szerint, ha valóban nem tart tovább egy évnél a háború, akkor 2023-ban már ismét komolyabb bővülés jöhet az európai infokommunikációs piacon, amelynek mértéke elérheti a 4,7 százalékot is.

Egységes reakció

Érthető módon Ukrajna és Oroszország ICT-piaca kapja a legnagyobb ütést a háború miatt. Azt egyelőre csak találgatják a szakértők, hogy az orosz fejlődést mennyivel veti majd vissza a nyugati világ reakciója, a szankciók sorozata és az, hogy rengeteg cég kivonult az országból, de a már most is komoly infláció mellett gazdasági visszaesés is várható az országban. A legnagyobb technológiai cégek egyébként meglehetősen egységesen reagáltak, és ha nem is azonnal hagytak fel az oroszországi tevékenységükkel, de folyamatosan érkeznek a hírek arról, hogy elhagyják azt a piacot, nem szállítanak oda, illetve bezárják ottani érdekeltségeiket.

Mivel Oroszországból a valós helyzetet bemutató hírek nem nagyon jutnak el hozzánk, azt is nehéz felmérni, hogy milyen hatása lehet ott annak, hogy a nagy, nemzetközi technológiai vállalatok beszüntetik tevékenységüket. Az mindenesetre jelzésértékű, hogy például az SAP – amely egyébként csak április közepén döntött úgy, hogy teljesen elhagyja a piacot – néhány éve még a 100 legnagyobb forgalmú orosz társaság mintegy felével üzleti kapcsolatban állt. Vagyis aktívan használták a németországi központú cég szoftvereit, igaz, új termékekhez és szolgáltatásokhoz már március eleje óta nem juthattak hozzá. A helyben telepített megoldások egyébként az SAP képviselője szerint továbbra is működnek majd, de frissítések, új verziók nyilván nem érkeznek, ahogy a legmodernebb, felhőalapú rendszerek sem állnak majd rendelkezésre.

> Csak az európai az ICT-költést 143 milliárd dollárral csökkentheti a háború 2022 és 2025 között

A népszerű globális közösségimédia-platformok, videómegosztók eltűnése az orosz piacról tovább szűkítik a vállalkozások lehetőségeit, hiszen elég csak abba belegondolni, hogy itthon a digitális hirdetési piac két legnagyobb szereplőjének már a Facebook és az Alphabet számít. Az Amazon már a háború elején bejelentette, hogy nem szállít az országba termékeket, de ami talán még fontosabb, hogy az AWS (Amazon Web Services) felhőszolgáltatása is elérhetetlenné vált az orosz cégek számára. Nyilván igyekeznek majd

saját megoldásokkal pótolni a kieső technológiákat, szoftvereket és szolgáltatásokat, azonban kérdéses, hogy az évtizedes tapasztalatokra és globális erőforrásokra építő társaságok által fejlesztett megoldások mennyire lesznek majd pótolhatók, azaz sikerül-e elkerülni, hogy digitális sivataggá váljon az ország.

Chipes kérdések

A globális hatások kapcsán érdemes kiemelni egy területet, amely az elmúlt években is komoly nehézségekkel küzdött és a háború miatt újabb ütést kaphat. A Covid-járvány kirobbanásának egyik gyakran emlegetett hatása volt az ellátási láncokban keletkezett zavar, és talán a legtöbbször a chipgyártást hozták fel ennek illusztrálására. Természetesen a gyárak leállása mellett a chiphiányban az is szerepet játszik, hogy egyre nagyobb az igény az intelligens berendezésekre, hiszen ma már a számítástechnikai eszközök mellett autókban, háztartási gépekben, ipari berendezésekben egyaránt szükség van ezekre. Az orosz-ukrán háború kirobbanását követően rögtön felvetődött a kérdés, hogy vajon hogyan hat a kialakult helyzet a globális chipellátásra. A piac meghatározó szereplői igyekeztek megnyugtatni a nyilvánosságot, hogy rendelkeznek készletekkel alapanyagokból, nem okoz majd komolyabb fennakadást a háború.

Márciusban viszont a Techcet nevű tanácsadócég arra hívta fel a figyelmet, hogy az egyik fontos alapanyagból, a neonból igenis hiány lehet. A társaság ugyanis rámutatott, hogy a chipgyártás során globálisan használt neongáz mintegy fele Ukrajnából származik, ahol a helyi és oroszországi acélgyártás melléktermékéből állítják elő az Intel, a Samsung, vagy az AMD üzemeiben használt gázt. Ez a forrás február 24-e után érthető módon megszűnt, vagyis nagy kérdés, hogy vajon mennyi tartalékkal rendelkeznek a nagy gyártók, illetve a másik nagy neongáz-szállító, Kína képes-e nagyobb menyniséget szállítani a piacra. Az mindenesetre árulkodó jel, hogy Dél-Korea úgy döntött, hogy áprilistól három, a chipgyártásnál is használt nemesgáz – neon, xenon és kripton – esetében részlegesen megszünteti a korábban alkalmazott importvámot.

Állással segítenek

Speciális toborzási programot jelentett be az SAP, hogy az Ukrajnából érkező menekülteknek a globális irodahálózatán keresztül álláslehetőséget biztosítson. A kezdeményezés célja, hogy az Ukrajnából származó képzett menekülteknek megfelelő munkalehetőséget kínáljanak a cégnél Németországban, Csehországban, Magyarországon, Bulgáriában, Romániában, Lengyelországban vagy Szlovákiában.

A felkínált állások többek között a szoftverfejlesztés, az értékesítés, a tanácsadás, valamint az operációt támogató funkciók – például a HR és a pénzügy – területéről származnak. A németországi állásoknál lehetőség van részmunkaidős, illetve határozott időtartamú szerződéses munkaviszony választására is.

A háború miatt lakóhelyüket elhagyni kényszerülő ukrán alkalmazottak a felkínált állás mellett a beilleszkedést segítő anyanyelvi mentorálást, egészségügyi és lelki segélynyújtást, nyelvoktatást, és szükség esetén gyermekgondozási támogatást is kaphatnak, országonként változóan. Bizonyos esetekben pedig munkabér-előleg is kérhető.

Élesedik az árverseny

Az orosz-ukrán háború komoly hatással lehet a szoftverfejlesztési, illetve az IT-szolgáltatási piacra is *Zséger Ádám,* az Attrecto vezetője szerint. „Több százezer szoftvermérnök tűnt el a piacról szinte egyik pillanatról a másikra. Mivel az

FORRÁS: 123RF.COM

amerikai és nyugat-európai vállalatok kivonultak az orosz piacról, az eddig nekik dolgozó szakembereket elveszítették, az ukrán fejlesztők pedig vagy harcolni mentek – például az ukrán sereg kiberbiztonsági részlegébe –, vagy egyéb okok miatt váltak elérhetetlenné. Az érintett cégek természetesen igyekeznek pótolni a kieső szaktudást és kapacitást, ez pedig a már amúgy is meglehetősen komoly inflációs nyomást tovább növeli a piacon. Már az év elején, a háborútól függetlenül megfigyelhető volt áremelkedés a projekteknél, szolgáltatásoknál, azonban a most kialakult helyzet további drágulást hoz a szoftverfejlesztés, IT-szolgáltatások esetében. Árfelhajtó hatása van annak is, hogy még komolyabb árverseny indul be a szakemberek megszerzéséért, és tovább emelkednek a szoftverfejlesztési és IT-szolgáltatási költségek. Ráadásul a Covid-járvány hatalmas változást hozott a távmunka vállalati

ZSÉGER ÁDÁM, ATTRECTO

FORRÁS: ITBUSINESS

megítélésében. Fel kell készülni arra, hogy globális szinten kell versenyezni a tehetségekért. Ez a gyakorlatban pedig azt jelenti, hogy a hazai ICT-cégeknek például német, vagy amerikai társaságok ajánlatait kellene felülmúlni, vagy valami olyat kínálni, amit ők nem tudnak”, vázolta a helyzetet Zséger Ádám.

Beszámolója szerint a háború kirobbanására nagyon gyorsan reagált az informatikai piac, nagyjából egy hét után több olyan megkeresés is befutott hozzájuk, amelyek az oroszországi, illetve az ukrajnai fejlesztői csapatok áthelyezésére, esetleg egész projektek átszervezésére vonatkozott. Hasonlóan a Covid-járvány kitöréséhez az első időszak a gyors reakciókról szólt, de a jelek szerint néhány hét alatt sokan találtak valamilyen megoldást, mert azóta csökkent a megkeresések intenzitása.

A társaság IT-szolgáltatásokat kínál, webes és mobiltechnológiákban egyedi szoftverfejlesztést végez ügyfeleinek, illetve outsourcing szolgáltatásokat is nyújtanak. A kialakulóban lévő helyzet miatt a hasonló portfólióval rendelkező cégek várhatóan keresettebbek lesznek majd a piacon. „Jelenleg Győrben és Budapesten van egy-egy irodánk, összesen 70 fős a csapatunk. Szakmailag és létszámban is folyamatosan fejlődünk. Elsősorban szakmailag magas színvonalú, igényes szolgáltatásokat, megoldásokat nyújtunk ügyfeleinknek. A piaci hatások, mint például a fluktuáció minket is érint. De úgy gondolom, hogy erős a munkaerőpiaci pozíciónk, több olyan kezdeményezésünk van, ami vonzó munkáltatóvá tesz minket, erősíti a csapatunkat, így meg tudjuk majd oldani a növekedést”, fűzte hozzá Zséger Ádám.

Kalocsai Zoltán

ALKALMAZÁS KIS DARABOKBÓL

Konténerbe vele, de azonnal!?

Az online térben való jelenlét megkerülhetetlen, de önmagában már nem elég. A piaci igényekre való gyors reagálás napjaink felgyorsult világában minden cég számára elengedhetetlen. Vajon a meglévő IT rendszereink és működésünk támogatja az üzlet ilyen gyors változását?

FORRÁS: REVDEBUG.COM

Ha az agilis módszertanok, konténerizáció, Dev(Sec)Ops régi jó ismerősök, akkor már ön is találkozott a problémával, és kezeli a kérdést. Ha ön is ebbe a csoportba tartozik, bátran ugorjon az utolsó bekezdésre. Ha még most ismerkedik, a következő bekezdések megerősítik abban, hogy belevágjanak, mert az ma már nem kérdés, hogy érdemes.

A sokoldalú konténer

Nagyon leegyszerűsítve a konténerizáció egy, az infrastruktúránál magasabb szintű virtualizációs technológia, amely az alkalmazásunk kódját és a futásához szükséges szoftvereket egy futtatható csomaggá, úgynevezett konténerré építi. A kódból telepített alkalmazássá válás folyamatát CI/CD pipeline-nak nevezzük. Ez a felépítés és a hozzá szorosan kötődő folyamat rengeteg előnnyel jár, mondja *Richter Elek,* az NKS üzletfejlesztési vezetője.

A konténerizált alkalmazások könnyen és gyorsan mozgathatók a fejlesztői, teszt- és éles környezetek között. Ha jól építettük fel a folyamatot, egy hibajavítás vagy új funkció egy gombnyomásra, percek alatt végigrobog, és már élesben is működik. Nincs levelezés az üzemeltetéssel, megszűnik a fejlesztői, teszt- és éles környezetek eltérésének örök problémája, és jelentősen leredukálódik a mindenki által hallott örök klasszikus „nálam még működött” felbukkanása.

A funkciók szétválasztásával egy esetleges hiba nem a teljes alkalmazásunkat teszi használhatatlanná, hanem csak az adott funkciót. Az automatizált biztonsági tesztek és az integrált biztonsági elemző eszközök azonos biztonsági szintet garantálnak, függetlenül a fejlesztő tudásától.

A kicsi, önmagában elindítható, leállítható, mozgatható konténer kisebb fajlagos üzemeltetési költséget jelent az alkalmazásoknál, és könnyen lekövethető velük a terhelés változása.

Konténerizáljunk mindent?

Az előnyök ellenére nem mindent lehet vagy érdemes konténerizálni. Dobozos termékeket, ahol a licenc nem teszi lehetővé, vagy nagy méretű, komplex alkalmazásokat, amilyen egy CRM- vagy ERP-rendszer, nem érdemes konténerbe kényszeríteni. Egy új, IT által még nem támogatott üzleti igény megjelenésekor azonban már mindenképpen érdemes számításba venni ezt az architektúrát, figyelmeztet Richter Elek.

Ennek is több módja lehet, attól függően, mi áll a rendelkezésünkre.

– Ha van infrastruktúra (szerverteremtől a hálózaton át a mentésig), folyamatok (fejlesztési, üzemeltetési, biztonsági) és humán erőforrás (fejlesztő, DevOps mérnök), akkor akár házon belül is bátran felépíthető egy on-premise környezet.
– Ha az infrastruktúra megvan, de sem folyamatokban, sem megfelelő mérnökökben nem dúskál a cég, akkor érdemes a teljes fejlesztési és DevOps folyamatot, feladatokat kiszervezni. Így az adat megmarad házon belül, viszont a tapasztalt szakemberekkel az üzlet gyorsan kap megoldást.
– Fejlesztőcsapatokban az üzleti tudás és a DevOps Dev része erős: ők olyan platformszolgáltatást keressenek, ahol az infrastruktúrán túl megfelelő DevOps támogatást is kapnak.
– Ha pedig csak az infrastruktúra hiányzik (mint a startupoknál), logikus irány a felhő. Lehet publikus, privát, nemzetközi vagy itthoni. A választás többnyire az ismertségen, a meglévő tapasztalatokon, illetve a szabályozási vagy a biztonsági igényeken múlik.

Az elmúlt hetek háborús eseményei és az azt követő szankciók felvetik még a nemzetközi publikus felhők rendelkezésre állási kérdését, azaz vajon mikor vágja le magát egy ország a nemzetközi internetről, vagy korlátozza a hozzáférést az adott országból egy nemzetközi cég. Ha ilyen kétely merül fel bárkiben, úgy érdemes inkább magyarországi szolgáltatót választania. ■

RÖGZÍTSÜNK, DE OKOSAN!

A szó nem száll el

Óriási potenciál rejlik a vállalatok és az ügyfeleik közötti kommunikáció elemzésében. A tartalmi és érzelmi mintázatok felismerése rendkívül értékes tudással látja el a döntéshozókat.

FORRÁS: TC&C

DR. JUHÁSZ CSABA, TC&C

Az ügyfélszolgálati központokban minőségbiztosítási szempontból már régóta rögzítik a bejövő hívásokat, amelyekben hatalmas, kihasználatlan adatvagyon rejlik. A beszélgetések érzelmi töltetéből következtetni lehet az ügyfél elégedettségére, az ügyintéző munkájának minőségére, de adott esetben egy-egy termék vagy szolgáltatás fogadtatására is. Mivel pedig a contact centerek eszköztárába a telefonhívás mellett már bevonult a chat és a videó is, olyan rendszerre van szükség, amely mindhárom csatornán képes automatikusan, valós időben detektálni és kiértékelni az érzelmeket.

Árulkodó érzelmek

„Közel két évtizede foglalkozunk IP alapú telefonrendszerekhez kapcsolható hangrögzítési megoldásokkal, így jól érzékeltük ezt az ügyféligényt. Elhatároztuk, hogy mesterséges intelligencia (MI) alapú okos rögzítővel fejlesztjük tovább CARIN rendszerünket, a projektre pedig a NKFIH-tól 177,7 millió forintos támogatást is elnyertünk”, mesél a múltról és a jelenről *Dr. Juhász Csaba,* a TC&C ügyvezető igazgatója.

Általában hat emberi alapérzelmet szoktak megkülönböztetni, a projekt és a rendszer céljaihoz viszont elegendő annak megállapítása, hogy az ügyfél elégedett, elégedetlen vagy éppen semleges hozzáállású. Ehhez felhasználják a mimikát (összeráncolt homlokot, összehúzott szemöldököt, mosolygó szájat), a hangot (hangerőt, intonációt, egymás szavába vágást). A beszélgetés folyamán készült leiratot a szövegelemző segítségével lehet kiértékelni, például indulatszavakra.

A TC&C okos rögzítőjének egyik újítása éppen abban áll majd, hogy a három csatornán egymástól függetlenül, de egyszerre vizsgálják az érzelmeket. A különböző forrásokból származó elemzéseket egy további mesterséges neurális hálózat összesíti, ami garantálja a nagy megbízhatóságú eredményt.

Újrahasznosítható tudás

„A jövő őszre befejeződő fejlesztés során egy nagy pontossággal működő, többnyelvű, nemzetközi környezetben is alkalmazható megoldást állítunk elő. Ilyen rendszer jelenleg még nincs a világon, és akkor sem igen lesz, amikorra mi elkészülünk vele, éppen ezért komoly piaci potenciált látunk benne”, állítja Juhász Csaba. A contact center üzemeltetők számára az egyik legfontosabb előny, hogy a kritikus hívások automatikusan megjelennek értékelésre, felülvizsgálatra, nem utólag kell kikeresni ezeket a felvételeket

A fejlesztés során megszerzett tudást ugyanakkor egészen más területeken is hasznosítani kívánja a TC&C. A CARIN-ban alkalmazott gépi tanulásos módszerek más, Big Data jellegű tudásbázis (hívásnaplók, email archívumok) elemzésére is felhasználhatók. Ennek révén például fel lehet térképezni, hogyan áramlik az információ a cég egyes osztályai, csoportjai között, illetve milyen a vállalat kommunikációs hálója a partnerei, ügyfelei felé – említ néhány lehetőséget Juhász Csaba. ■

Odafigyelve az adatvédelemre

A közelmúltban 250 millió forintos GDPR-bírságot szabott ki a NAIH egy bankra, amely mesterséges intelligencia alapú szoftverrel értékelte a call centeres hívásokat, az ügyfelek érzelmeit is elemezve.

„A NAIH határozatai ebben a tárgykörben (még) nem publikusak”, mondta *dr. Ormós Zoltán,* az Ormós Ügyvédi Iroda vezetője. Az ügy rövid összefoglalójából az látszik, hogy a hatóság nem a hívások MI általi elemzését „ítéli halálra”, hanem a konkrét pénzintézet konkrét megközelítését tartja jogszerűtlennek. Ha a pénzintézet módosítja adatkezelési gyakorlatát úgy, hogy az megfeleljen az általános adatvédelmi rendeletnek – például biztosítja az érintetteknek a megfelelő tájékoztatást és a tiltakozás jogát –, akkor nincs akadálya a hívások szoftveres elemzésének.

BEKÖSZÖNTÖTT A „DIGITAL FIRST" KORSZAK

A digitális játszótéren az együttműködés a fontos

Az ügyvezető igazgatók digitális eszközökhöz nyúlnak a világ kockázatainak kezelésére. A „digital first" világban a know-how megszerzésére, a bevételt növelő technológiákra és a digitális szolgáltatások ökoszisztémájának kialakítására van szükség. Ki fog alakulni a digitális szolgáltatások ökoszisztémája, ahol sokan sokaknak kínálnak szolgáltatásokat. Ebben a modellben a tegnapi ügyfél ma partner, holnap pedig versenytársunk lehet.

FORRÁS: 123RF.COM

„A digitális átalakulás korszakából a »digital first« periódusba lépünk”, mondta 2022. márciusi előadásában *Philip Carter,* az IDC kutatási alelnöke. A világ, a vállalatok és az emberek felébredtek az elmúlt két év digitális hibernálásából, és a világ kockázatainak kezelésére elsősorban digitális eszközökhöz nyúlnak. Az IDC tanulmánya szerint (amelyet 398 vállalati CEO megkérdezésével készített kutatásra alapoznak, címe: „The CEO imperative in the digital first world”), a vezetők 88 százaléka növeli vagy az előző évhez hasonló szinten tartja majd technológiai jellegű kiadásait – ez is jelzi a digitális elsőbbség iránti elköteleződésüket.

A digital first világa érkezik

Az elemzés szerint a digitális átalakulás korszaka után a digitális üzleti korszak érkezik 2023-tól. *(Lásd a „Digitálisnak számító költés” című ábrát!)* Azért ettől az évtől, mert a szakemberek előrejelzése szerint fordulópontot jelent majd: a vállalatok több pénzt költenek IT-re, mint más területekre a szervezeten belül.

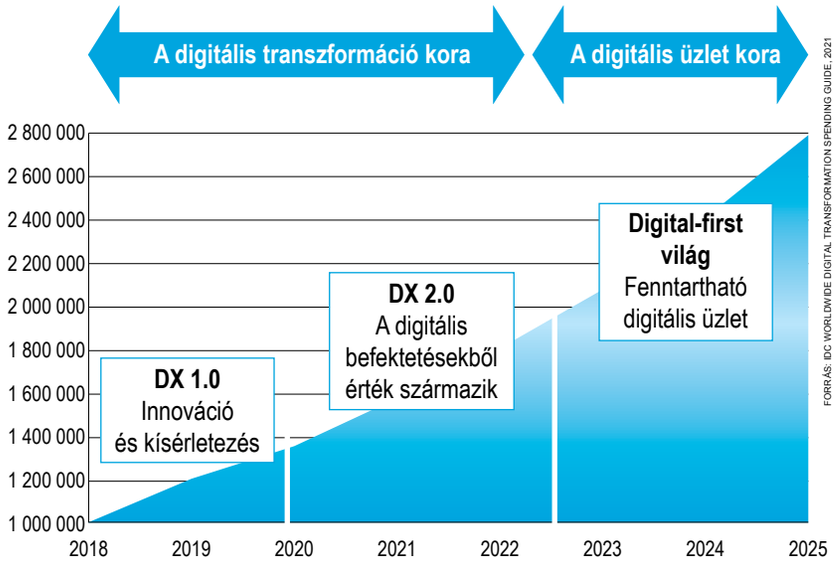
A digitális transzformáció korának két szakaszát különböztetik meg: a DX 1.0 2020-ig tartott, ezt a szakaszt az innováció és a kísérletezés jellemezte. Ebben a szakaszban a sikeres pilotprogramok nagy léptékű megvalósítása kihívást jelentett a vállalatoknak, csupán 26 százalékuknak térült meg ez irányú befektetése. A második szakaszban, a DX 2.0-ben a vállalatok igyekeznek a digitális befektetéseket nyereségessé tenni, úgy tűnik, jó úton haladnak a cél felé. A digitális üzleti korszak hajnalán az első szakasz a „digital first” világ lesz, amikor az ügyvezető igazgatók fenntartható digitális vállalatok igyekeznek kialakítani. Idén a digitális know-how megszerzésére, a digitális üzlet fejlesztésére kell összpontosítsanak az ügyvezető igazgatóknak ahhoz, hogy a „digital first” világába sikeresen bevezessék szervezetüket. Az elemző cég szerint a látványos és nagy mértékű befektetések ellenére a CEO-knak nem szabad rövid távú sikerekben gondolkodniuk, a cél a hosszú távon fenntartható digitális üzlet megteremtése.

A technológia növelje a bevételt

A vállalat kutatása azt is feltárta, hogy minden második vezetőnek segítségre van szüksége ebben az utazásban, ezért nem meglepő, hogy a vezetők 48 százaléka a bevételek növelését célzó technológiákban bízik. De pontosan mit is jelent, vagyis hogyan néz ki? A kutatás a bevételt növelő technológiák négy ismérvét sorolja fel:

– kizárólag felhő alapú, reziliens, több szereplős architektúrát követ,
– „API first” szemléletmódra vált szervezet, ahol újradefiniálják az integráció, automatizáció témaköreit,
– olyan technológiai környezetet kell megteremteni, ahol nem egy központi adattárház generálja az adatokat és jelentéseket, hanem az érdekelt felek a saját adataikat behozhatják a rendszerbe
– az ügyfél, alkalmazott, partner határozza meg azt a csatornát, amelyen keresztül a digitális élményben részesül.

Digitálisnak számító költés (millió dollár)



Változnak a felelősségi körök is az IDC szerint. A vállalatok az üzleti eredményekre összpontosítanak, amikor millió vagy milliárd dollárokat költenek technológiai fejlesztésekre. Egy multinacionális autógyár példájával élve: ez a gyár azt várja el technológiai szállítójától, hogy a megoldások 30 százalékos produktivitást eredményezzenek, 30 százalékkal csökkenjenek a gyártási költségek és 1 milliárd eurós költségmegtakarítást érjenek el az ellátási láncban. Az eredmények eléréséhez pedig a technológiai szállító vállal garanciát a szerződés szerint.

A digitális üzlet alapja a felhő, ezt is tartalmazzák a szerződések. Így nem meglepő, hogy a „digital first” világban a CEO legfontosabb, stratégiai technológiai partnere a nyilvános felhőszolgáltató lesz, őt követi a technológiai tanácsadó partner, a harmadik az ERP-szolgáltató. A felhőszolgáltató partnerben látják a vezetők a garanciát arra, hogy az eredmények kerülnek fókuszba.

Digitális szolgáltatások összefonódása

A IDC szerint a vezetők olyan partnereket keressenek, akikkel közösen az eredményekre tudnak összpontosítani. Ez a fenntartható digitális modell lényeges változást jelent a korábbi modellekhez képest. A 2010-es évek előtti világ tranzakcióközpontú volt, ahol a termék és annak értékesítése volt a középpontban. A mai világ ehhez képest a fogyasztás serkentésére összpontosít, ahol egy szolgáltató többeknek kínál megoldásokat a gondjaikra „as a service” konstrukcióban.

Azonban a „digital first” világban kialakul a digitális szolgáltatások ökoszisztémája, ahol sokan sokaknak kínálnak szolgáltatásokat. Ez a modell azt jelenti, hogy bármely szervezet, amely tegnap még az ügyfelünk volt, holnap potenciális partnerünkké, és elképzelhető, hogy a jövőben pedig versenytársunkká válik. A már említett autóipari szereplőre vetítve: az IT-megoldásokat vásárló ügyfél a jövőben versenytársa lehet az IT-szolgáltató cégnek, hiszen felépített infrastruktúráját kihasználva ők is indíthatnak felhőszolgáltatásokat a többi autóipari cég számára. Nem az lesz a fontos, hogy menynyire jól játszunk ezen a digitális játszótéren, hanem mennyire tudunk együttműködni másokkal az ökoszisztéma-modellben.

Az üzleti eredményekre való összpontosítás mellett a vezetőknek figyelniük a méretezésre is, amikor a technológiai architektúra üzleti architektúrává fejlődik. Azzal is számolniuk kell, hogy a digitális világ alapja és fizetőeszköze a bizalom lesz, amelynek kialakítása és megtartása közös erőfeszítés eredménye.

Vass Enikő

ALKALMAZKODNI A KISZÁMÍTHATATLANSÁGHOZ

Házhoz jön a felhő

A saját adatközpontnak és a felhőnek is megvannak az előnyei, amelyekről nem szívesen mondanak le a vállalatok. Szerencsére van lehetőség arra is, hogy úgy élvezzék a felhő rugalmasságát és költséghatékonyságát, hogy nem kell publikus szolgáltatást igénybe venni.

Kiszámíthatatlanság – leginkább ezzel a szóval lehetne jellemezni az ügyfelek, a piac legfőbb problémáját. A nagymértékű változások hirtelen és váratlanul követik egymást, amire válaszul az üzleti igények egyik napról a másikra vehetnek gyökeresen új irányt. Alig tanultak meg együtt élni a vállalatok a Covid-járvánnyal, illetve annak hosszú távú hatásaival, kirobbant az orosz-ukrán háború, és ismét új körülményekhez kellett alkalmazkodni.

A méretezés korlátai

Az üzleti körülmények változása az infokommunikációs infrastruktúrára is rányomja a bélyegét. A járvány egyes vállalatoknál (például szállítmányozók, futárcégek) olyan hirtelen növekedést hozott, amelyet előre nem tudtak betervezni. Amikor pedig próbálták a működés fenntartásához szükséges rendszereket beszerezni és üzembe állítani, azt kellett tapasztalniuk, hogy mire a beszerzési eljárás végigfutott a cégen, már ismét újra kellett tárgyalni az igényelt kapacitást, konfigurációt, említ egy tipikus példát *Marton Balázs,* az EURO ONE Számítástechnikai Zrt. HPE GreenLake rangere.
Idén pedig a háború húzta keresztül számos vállalat elképzeléseit. Az Oroszországgal vagy Ukrajnával komolyabb üzletet lebonyolító cégek azon találták magukat, hogy a korábban egy összegben, egyszerre megvásárolt erőforrások a visszaeső volumen miatt kihasználatlanul állnak. Pénzügyi szempontból nagyon rosszul jártak, mert az előre megvett kapacitások gyakorlatilag kidobott pénzt jelentenek.

Almát az almával

Nem mindig egyszerű összehasonlítani egy használat alapú, több éves szolgáltatási szerződés költségeit egy egyszeri beruházásával. Bizonyos költségelemek sokszor rejtve maradnak, ami óhatatlanul torzítja a valós képet, figyelmeztet *Marton Balázs,* az EURO ONE Számítástechnikai Zrt. HPE GreenLake rangere.
Nem szabad például mechanikusan összevetni az egyszeri beruházás költségeit a HPE GreenLake szolgáltatásért 4-5 év alatt kifizetett összegekkel. Utóbbi esetében a költségek nem kis hányada csak évek múltán jelentkezik, ezért lényeges jelenérték-számítást végezni diszkontrátával. Bele kell venni az egyenletbe az inflációs rátát (ami jelenleg nem elhanyagolható), az IT-eszközök és az informatikai szolgáltatások éves árnövekedését is.
Ami pedig még nehezebben számszerűsíthető, az a kiszámíthatóbb informatikai és üzleti környezet kínálta biztonság, a működési kockázatok csökkenése.

Kézenfekvő választásnak tűnne a számítási felhő igénybe vétele. Számos olyan vállalat van azonban, amely számára ez nem járható út, akár a szabályozói környezet, akár belső szabályok, akár adatbiztonsági megfontolások miatt.

On-premise telepített, mégis rugalmas

A kiszámíthatatlanság ellensúlyozására az ügyfelek olyan infrastruktúrát szeretnének, amelyek ötvözik a felhő alapú és a saját adatközpontban működtetett megoldások összes előnyét, azok hátrányai nélkül, összegzi a piaci igényeket Marton Balázs.
Vagyis ne kelljen újraírni az alkalmazásokat, ne legyen szükség drága migrációs projektre és ne fenyegessen a „vendor lock-in”, vagyis az egy szállítótól való függés veszélye, mint a felhős megoldásoknál.
Ugyanakkor ne is kelljen egyszerre nagy költséggel felállítani egy olyan infrastruktúrát, amely csak hónapok alatt állítható üzembe, miközben az életciklusa kezdetén a feleslegesen betervezett kapacitás kihasználatlanul áll, hogy aztán amikor az igények a várnál nagyobb mértékben nőnek, csak nehézkesen lehessen utólag bővíteni, ahogy ez a saját adatközpontban történni szokott.
Erre nyújt megoldást a HPE GreenLake, amely gyakorlatilag a felhőt hozza el az ügyfél saját adatközpontjába. A konstrukció lényege, hogy a szükséges erőforrásokat (szervereket, tárolókat, hálózati eszközöket, a hozzájuk szükséges virtualizációs, szerver operációs vagy akár 3rd party szoftverekkel) a HPE szállítja le és helyezi üzembe a felhasználó adatközpontjában, partnerei bevonásával.
„Természetesen arra is van lehetőség, hogy az implementáció után az adatok migrálásban vagy az adatbázisok beállításában segítsünk. Alapesetben ezeket a rendszereket az ügyfél üzemelteti, de arra is van lehetőség, hogy ezeket az EURO ONE Számítástechnikai Zrt. teljes mértékben kiszervezze. Az EURO ONE Számítástechnikai Zrt. integrátor HPE partnerként az adatközponti hardver réteg üzemeltetése fölött a teljes környezet támogatási tevékenységeit képes elvégezni a méretezéstől, tervezéstől, az üzemeltetési tevékenységek ellátásán át. Legyen szó a virtualizációs, alkalmazás-, vagy adatbázisrétegről, vagy az azon futó szolgáltatásoktól, üzemeltetéstámogató szakembereink képesek az igények hatékony lefedésére. A hatékony erőforrás-felhasználást központi IT monitoring megoldásunk segítségével támogatjuk annak érdekében, hogy ügyfeleink a rendelkezésre álló erőforrásokat

FORRÁS: ITBUSINESS

MARTON BALÁZS, EURO ONE SZÁMÍTÁSTECHNIKAI ZRT.

optimálisan tudják felhasználni. Modern alkalmazások esetén támogatjuk a hibrid (felhő-on prem) működést, akár konténerizációs alapokon is", teszi hozzá Marton Balázs.

A csavar ott van a dologban, hogy az eszközök a HPE tulajdonában maradnak, az ügyfél azokért a használattal arányos havi díjat fizet, mintha csak egy felhőszolgáltatótól venné meg a kapacitást.

A HPE GreenLake a felhő egyik másik nagy előnyét, a rugalmasságot, gyors skálázhatóságot is kínálja. A titok abban rejlik, hogy nagyobb kapacitást szállítanak le, mint amennyire az ügyfélnek kezdetben szüksége van, magyarázza a konstrukció egy fontos elemét Marton Balázs. Ez a plusz kapacitás ott rejlik az infrastruktúrában, de addig nem kell érte fizetni, amíg a vállalat használni nem kezdi azt. Ám ha hirtelen felmerül az igény, és villámgyorsan kell még több számítási teljesítmény vagy háttértár, az néhány kattintással (vagy akár automatikusan is) aktiválható és használatba vehető. És mielőtt a tartalék még teljesen elfogyna, tovább lehet bővíteni a rendszert, hogy megmaradjon a mozgástér.

Csak annyit, csak akkor

A fentiekből következik, hogy igen fontos a letelepítendő rendszer méretezése és az igények későbbi alakulásának tervezése. „Az IT egyik legnagyobb problémája a kapacitások túltervezése, ügyfeleink manapság nagyjából 50 százalékkal nagyobb szerverteljesítményt és tárhelyet vásárolnak, csak hogy biztosra menjenek. Ezt elkerülendő jól kell belőni, hogy milyen erőforrásokra van pillanatnyilag szükség, és hogy összességében milyen növekedéssel számol a vállalat a szerződés 4-5 éves időtartama alatt. Ehhez az IT-n kívül természetesen szükség van az üzleti területek képviselőire és a pénzügyi vezetőre. Itt jön képbe az EURO ONE Számítástechnikai Zrt. szakértelme és közel három évtizedes tapasztalata is, hiszen „Magyarországon tavaly mi helyeztük üzembe a legtöbb HPE GreenLake rendszert. Varázsgömbünk nincs, de épp elég tudást halmoztunk fel különféle vertikumokban, hogy ne tévedjünk nagyot", hangsúlyozza Marton Balázs.

Az elszámolás havonta történik, a felhasznált kapacitás függvényében. Többféle mérőszám is elképzelhető a fogyasztásra (szerver, CPU, memória, virtuális gép, háttértár). Ezeket már a tervezés során számba veszik, és a különféle lehetőségek közül úgy választanak, hogy az leginkább megfeleljen az ügyfél igényeinek. A fogyasztást folyamatosan látja az ügyfél, az EURO ONE Számítástechnikai Zrt. és a HPE is, így a költségek mindig előre tervezhetőek, a partner pedig fel tud készülni a kapacitások szükségessé váló növelésére.

Zsebben maradó forintok

Mind az informatikai, mind a pénzügyi vezetőnek számos előnyt kínál a HPE GreenLake. Előbbi az infrastruktúrával együtt számos szoftverhez (akár harmadik felek szoftvereihez) és üzemeltetési szolgáltatáshoz is hozzájuthat, akár a HPE, akár a partner jóvoltából, szintén havi díj ellenében. A rendszer elemei követik a technológiai változásokat, a fejlődést, így a CIO-nak nem kell aggódnia az avulás miatt. Egyszerűsödik számára a rendszermenedzsment is, hiszen a HPE a partnerével karöltve gondoskodik az igények szabott 7×24 órás felügyeletről, a rendszerek monitorozásáról, a firmware-ek és alapszoftverek frissítéséről, hibajavításáról. „Természetesen tudunk segíteni az implementációban, az adatmigrálásban vagy akár az adatbiztonsági szolgáltatásokban is", teszi hozzá Marton Balázs.

A CFO számára igen lényeges, hogy elkerülheti az egyszeri, nagy beruházások költségét, illetve a szükséges kapacitások túltervezését és ezzel a felesleges kiadásokat. A használat alapú árazás csökkentheti, egyúttal tervezhetővé teszi az informatikai infrastruktúra költségeit, és kedvezőbb lehet a cash-flow menedzsment is. *(X)*

EURO ONE Számítástechnikai Zrt.

Hewlett Packard Enterprise

MAGASABB FOKOZATBA KAPCSOLT A FELHŐ

Ezermilliárd dolláros üzleti lehetőség

FORRÁS: 123RF.COM

Három szabadságot kínál a felhőtechnológia a vállalatoknak: szabadon kísérletezhetnek, szabadon hibázhatnak és szabadon lehetnek agilisak. Ennek ellenére a vállalatok még csak a lehetőségek felszínét kezdték el kapargatni a felhőtechnológia lehetőségeinek, de négy év múlva az IT-büdzsék szinte felét a nyilvános felhő technológiára költik el. A vállalatok a költségek csökkentéséért és az alkalmazottak produktivitásának növekedéséért fordulnak a felhőhöz.

Még a koronavírus járvány előtt határozott úgy *Stéphane Bancel,* a Moderna vezérigazgatója, hogy az mRNA kutatás-fejlesztési platformjukat felhő alapokra helyezi. A felhő a terápiás felfedezések és fejlesztések eszközévé vált. A járvány kitörésekor érezhették ennek a stratégiának az előnyét: a vállalat „Drug Design Studio" nevű felhős megoldásának segítségével gyorsan és hatékonyan elemezték az mRNA szekvenciákat.
A tudósok és mérnökök a felhő alapú adattárház-szolgáltatásokat használva több, párhuzamosan futó kísérlet eredményeit elemezhették, így gyorsan meg tudták tervezni, majd finomhangolni a gyártási folyamatokat. Vagyis részben a felhőtechnológiának is köszönhetjük, hogy a vírus első szekvenálása után 42 nappal már kérvényezhették az oltás első körös kísérleti tesztjét, mert nem kellett mindent az első lépéstől kitalálniuk.

Már jól látják a CxO-k a felhőt

A McKinsey szerint a felhőnek az internet 1990-es és az okostelefonok 2000-es megjelenéséhez hasonlóan komoly átalakító hatása van társadalmunkra. A technológiának két értékjavaslata van: IT-korszerűsítés plusz a digitális innováció és felfedezés gyorsítása. A bevezetőben említett szabadságok együttesen olyan környezetet teremtenek, melyben az innováció otthon érzi magát.
A legtöbb vállalat csak most kezdi el felfedezni a felhő valós értékét, noha a szakemberek régóta dicsérték az innovációt és digitális átalakulást lehetővé tevő technológiát. A McKinsey szerint a vállalatok egyelőre még csak a lehetőségek felszínét kezdték el kapargatni. Komplex számításaik szerint a Fortune 500 vállalatok számára a felhő 1 ezer milliárd dollár értékű üzleti lehetőséget jelent 2030-ig EBIDTA-ban. A szám inkább csak becslés és nem előrejelzés, hiszen megvalósulásához a vállalatoknak kiemelten kell foglalkozniuk a felhő adta lehetőségekkel – ne feledjük, hogy a korai felhasználók nagyobb mértékű részesedést szerezhetnek ebből az üzleti lehetőségekből.
A Gartner szerint a felhőszolgáltatásokra fordított globális kiadások 2022-ben várhatóan meghaladják a 482 milliárd dollárt, szemben a 2020-as 313 milliárd dollárral. 2026-ra a vállalatok teljes informatikai költésük több mint 45 százalékát már nyilvános felhőre fogják fordítani, de világszerte gyorsan nő a hibrid – vagyis a publikus és privát felhő előnyeit ötvöző – és a több felhős (multicloud) megoldások népszerűsége is.

A legfontosabb növekedési területek

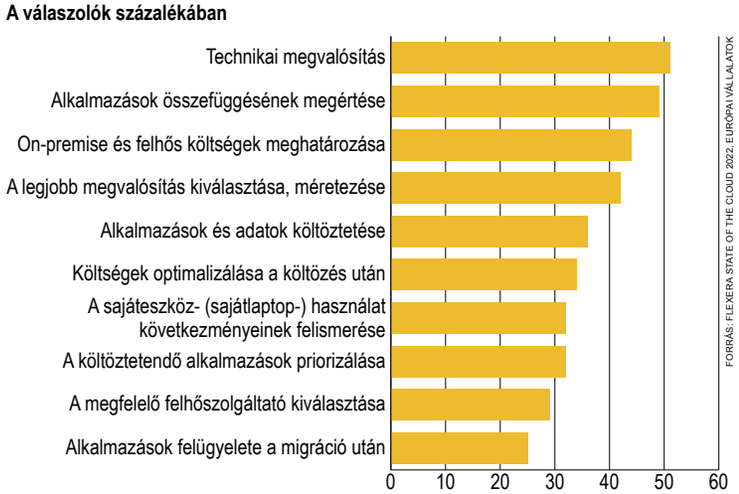
(válaszadók százalékában)

1. Software-as-a-Service – 52%
2. Platform-as-a-Service – 38%
3. Security-as-a-Service – 37%

FORRÁS: FOUNDRY: CLOUD COMPUTING STUDY 2022

A legnagyobb kihívások Top 10-es listája

A válaszolók százalékában



FORRÁS: FLEXERA STATE OF THE CLOUD 2022, EURÓPAI VÁLLALATOK

Egyre inkább a fősodorba kerül a felhő

Magasabb fokozatba kapcsolt a „cloud first" infrastruktúra fejlődése a távoli munkavégzés masszív elterjedése miatt, ezt mindenki érezte az elmúlt két évben. A Foundry (volt IDG) Cloud Computing Study 2022 tanulmánya számokat is társít a vélt gyorsuláshoz. A vállalatok 69 százalékánál gyorsult a felhőbe költözés az elmúlt 12 hónapban. Az ezután következő 18 hónapban azon vállalatok aránya is növekszik, amelyeknél már csak felhő infrastruktúra érhető el, de mindenképp az a domináns: a mai 41 százalékról 63 százalékra.
A 850 IT-döntéshozó megkérdezésével készített kutatás szerint a megkérdezettek közel kétharmada (72 százalék) fejlesztéskor vagy új technikai készségek vásárlásakor egyértelműen a felhő felé fordulnak. Egy kicsit aprólékosabban megvizsgálva, a vállalatok egyharmada (32 százalék) a munkafolyamatokat és alkalmazásokat a felhőben építi fel újra cloud migráció esetén.
A vállalatok egyharmada (33 százalék) kicsit óvatosabb megkö-

Konzervatív területeken is terjed a felhő

„Az olyan ultrakonzervatív iparág is, mint a bankszektor, mostanra komoly felhőtechnológia-felhasználóvá vált", mondja *Révész Róbert,* a TC2 ügyvezetője. Tisztán látható, hogy ha üzletileg rugalmasan akar változni a szervezet, költségoptimalizáltan, biztonságos módon, akkor ennek az egyik válasza biztosan a felhő. A pénzügyi szektorban is fontos, hogy az alkalmazásokat és a rendszereket igény szerint tudják méretezni: ha több felhasználó van, akkor is ügyfélbarát módon lehessen használni, ha viszont kevesebben vannak, akkor a költsége is legyen kevesebb.
„A pénzintézetek első körben az ügyféloldali alkalmazásokkal léptek, de most már ott tartunk, hogy a frontend mellett a backend is átkerült felhőbe", mondja az ügyvezető. Nyilván ehhez arra is szükség volt, hogy szabályozói oldalról egy sor kérdést megnyugtatóan rendeztek, az MNB ajánlásokkal segíti a felhőszolgáltatók és a pénzügyi szervezetek munkáját egyaránt.
Ennek hatására a különböző auditokra is sokkal jobban fel tudnak készülni a pénzügyi vállalatok. A felhőben is kritikus adatokkal dolgozik a szervezet, ahol szintén kockázati alapon kell kezelni a tevékenységet, mindezt egy sor IT-biztonsági előírásnak és compliance-elvárásnak megfelelően – ezeknek egy nagy részét a technológiával együtt a cégek megkapják szinte készen a felhőből. „Szolgáltatóként mi is egyre jobban értjük, hogy mit kell tennie az ügyfeleinknek, az ügyfelek pedig az üzleti céljaik könnyebb megvalósíthatóságán túl egyre jobban tudják, mit vár el tőlük a szabályozó, hogy megfeleljenek az egyes felülvizsgálatokon", fejezte be Révész Róbert.

FORRÁS: ITBUSINESS

RÉVÉSZ RÓBERT, TC2

zelítéssel a saját on-premise alkalmazásaikat nyújtják a felhőbe a core alkalmazások felhőbe költöztetésével, így ők a hibrid megközelítés hívei. A cégek közel egynegyede (23 százalék) apróbb lépésekben pár célzott alkalmazást egyetlen felhőszolgáltatónál próbálnak ki. A fennmaradó 6-6 százalék még nem döntött arról, milyen IT modernizációs stratégiát követ vagy nincs egyáltalán felhő migrációs tervük.
A Flexera „State of the Cloud 2022" tanulmánya hasonlóképpen azt látja, hogy globálisan növekedett a felhőtechnológia terjedése a járvány miatt. Az európai vállalatok esetében azonban sokkal nagyobb mértékű volt ez a növekedés, mint az amerikai cégeknél. A kutatás alátámasztja, hogy az európai szervezetek esetében is a felhő mainstream technológiává vált, 58 százalékuk erőteljes felhőhasználatról számol be, igaz, ez 4 százalékponttal marad el a globális aránytól.

Nem sétagalopp a migráció

A vállalatokat változatos okok vezetik a felhő technológiai felé. A Foundry tanulmányában megkérdezettek 40 százaléka a katasztrófatűrési képességek erősítése és az üzletmenet folytonossága miatt vásároltak felhőtechnológiát, míg 39 százalékuk régi rendszereiket cserélték le felhő alapúra. A válaszadók több lehetőséget is megjelölhettek, így kiderült, hogy egyharmaduk (34 százalék) a TCO csökkentése miatt, 33 százalékuk az alkalmazottak produktivitásának növeléséért váltanak erre a technológiára. Ugyancsak egyharmaduk (32 százalék) azért fordult a cloud felé, hogy növelje rugalmasságát és reakcióképességét a gyorsan változó piaci feltételek között.
A Foundry adatai szerint a felhőtechnológiára való áttérés pozitívan befolyásolta a vállalatok bevételeit, a megkérdezettek 60 százalékának fenntartható módon nőtt a bevétele az elmúlt 12 hónapban. A nagyvállalatok esetében az arány magasabb volt, 64 százalék, míg a kisebb cégeknél csupán 58 százalék. A vállalatok IT-költségvetésük egyharmadát felhőtechnológiára költik.

Felhőmigrációs kezdeményezések az európai vállalatoknál (százalék)

Több munkafolyamat költöztetése a felhőbe	69
A meglévő felhő használat optimalizálása	68
„Cloud first" stratégia követése	47
On-premise szoftverek SaaS-ra költöztetése	44
A konténerek használatának bővítése	41
Jobb pénzügyi jelentések felhő költségekről	37
Automata szabályozások az irányításhoz	37
Felhőszoftver-licencek menedzselése	37
CI/CD felhős megvalósítása	33
A nyilvános IaaS/PaaS szolgáltatások használatának növelése	32
A nyilvános felhő használatának növelése	31
Annak biztosítása, hogy az IT-részleg igénybe vehessen felhőszolgáltatásokat	12
A felhő szolgáltatók használatának növelése	12
A cloud marketplace használatának növelése	6

FORRÁS: FLEXERA STATE OF THE CLOUD 2022

FORRÁS: 123RF

Azonban, mint minden technológiának, a felhőnek is vannak kihívásai. A legnagyobb kihívást talán a költségek menedzselése jelenti a felhőstratégia megvalósításakor. A megkérdezettek 36 százalékának akadtak problémái a felhő jelentette költségek ellenőrzésével, míg 25 százalékuk az adatok felhőbe, illetve a felhőszolgáltatók közötti költöztetésének költsége miatt panaszkodtak. De a biztonsági kihívásokba is beletörik egyes vállalatoknak a bicskája: egyharmaduk adatbiztonsági és adatvédelmi problémákkal küzd. Gondot jelent a cloud biztonsági szakértelem hiánya is, ahogy a cloud erőforrások védelme és biztonsága is az esetek 34, illetve 25 százalékában.

A felhőmigráció sem mindig a legsikeresebb, a megkérdezettek 79 százaléka találkozott jelentős problémával. A multicloud migrációval kapcsolatos egyik leggyakoribb panasz, hogy rendkívül komplex (a megkérdezettek 48 százaléka szerint). A folyamatot hátráltatja a felhő menedzsment és biztonság miatt megnövekedett költségek (36 százalék) és a képzés és toborzás megnövekedett költsége (34 százalék).

A Flexera kutatása szerint a felhőre való átálláskor a technikai megvalósíthatóság felmérése jelenti a legnagyobb akadályt. Sok európai vállalatnak okoz álmatlan éjszakát költözéskor, hogy nem értik pontosan a különböző alkalmazások közötti összefüggéseket és nehezen tudják összehasonlítani az on-premise működés költségeit a felhő jelentette költségekkel. Foglalkoztatja őket az appok és adatok migrálásával kapcsolatos költségek, ahogy nehéz felmérniük, hogy pontosan milyen appokat is költöztessenek a felhőbe, milyen felhőszolgáltatót válasszanak.

Erős az optimizmus

Ezek a kihívások szerencsére még nem szegik a felhőbe költöző vállalatok kedvét, hiszen a szervezetek 69 százalékának az a legelső priori-

Konkrét megoldásokat keresnek

„A vállalatok levetkőzték a felhővel kapcsolatos ellenérzéseiket és félelmüket, és konkrét megoldásokat keresnek a cloudban”, mondja *Szabados Attila,* az Alef ügyvezető igazgatója. A döntés eléggé egyszerűsödött. Ahelyett, hogy a cég maga építse ki az IT-biztonsághoz vagy backuphoz szükséges hardver infrastruktúrát, a szolgáltató helyette találja ki és kínálja havidíjas konstrukcióban mindezt. A vállalatnak csak igénybe kell vennie. Ehhez konkrét és kézzel fogható, valós üzleti problémákra megoldást jelentő felhős szolgáltatásokat kell kitalálni és kínálni.

Az ügyvezető igazgató tapasztalata szerint dinamikusan növekszik ügyfeleik körében a felhő szolgáltatásokat vásárlók aránya, főként a versenyszférában. Az állami szektorban az adatvédelmi törvény miatt haboznak nem európai szolgáltatókra bízni adataikat, ott tapasztalata szerint nagyobb az ellenállás a felhő irányában.

FORRÁS: ALEF

SZABADOS ATTILA, ALEF

tása, hogy minél több munkafolyamatot költöztessen a felhőbe és optimalizálja a meglévő felhő infrastruktúra költségeit, ahogy a cloud-first stratégia követése is a top három prioritások egyike (bővebben lásd grafikonunkat).

A vállalatok nem nézik tétlenül a felmerülő problémákat a Foundry kutatása szerint sem. Új pozíciók megteremtésével és a szükséges készségek megvásárlásával próbálják kihozni a maximumot a befektetésből. A cégek 79 százaléka három új szerepkörbe vett fel embereket: felhő rendszer adminisztrátort, cloud architect és biztonsági architect, cloud rendszermérnök és cloud szoftver mérnök szerepkörökkel erősítettek.

Vass Enikő

NEMZETKÖZI TEREPEN IS PRÓBÁLKOZNAK AZ E-KERESKEDŐKET TÁMOGATÓ STARTUPOK

Virtuális kosarak

A járvány alaposan felpörgette az online forgalmat, itthon és világszerte is sokan próbálták ki az internetes vásárlást, ami nemcsak a kereskedőknek, de a számukra innovatív megoldásokat kínáló cégeknek is új lehetőségeket teremtett. A Webshippy Szlovákiában és Prágában terjeszkedik idén, a Recart pedig az amerikai jelenlétét erősíti a csapat bővítésével is.

FORRÁS: 123RF.COM

Jelentős fejlődést hozott a múlt év is a hazai e-kereskedelmi piacon, a webáruházak forgalma átlépte a bruttó 1200 milliárd forintot a GKI Digital és az Árukereső.hu közös elemzése szerint, az online csatorna részesedése pedig 10,4 százalék volt a teljes kiskereskedelemből. A pozitív trend komoly lehetőségeket hozott a szektort kiszolgáló innovatív cégek számára is, amelyek nemzetközi szinten is bizonyíthatnak.

Régiós tervek

„Május elején Pozsony mellett, a nyár végén pedig Prágában nyit új raktárat a Webshippy, a nemzetközi terjeszkedést pedig jövőre folytatná a cég, főként a közép-kelet-európai régióra fókuszálva", mondta el érdeklődésünkre *Perényi András,* a fulfillment logisztikai szolgáltatásokat kínáló társaság társalapítója. A vállalat számára komoly fejlődést hozott az elmúlt két év, az általuk havonta kezelt csomagok száma már 150-200 ezer között van, ami triplája a pandémia előttinek.

„A Covid-járvány hatalmas változást hozott az e-kereskedelemben. Az egyik ezek közül, hogy sok új belépő jelent meg a piacon, sok olyan kereskedő kezdte el az online értékesítést, aki korábban csak offline árulta termékeit. Miközben az internetes árusítás digitális része viszonylag könnyen megoldható, addig a logisztikai feladatokra ilyen rövid idő alatt megoldást találni nem lehetett volna partner nélkül.

A másik komoly változás, hogy sok ember kezdett el online vásárolni,

ami magával hozta azt is, hogy több innovatív szolgáltató jelent meg, és ez a csomagátvételi módok sokszínűségében is megnyilvánult. Számos csomagautomatát telepítettek az országban, csomagpontok nyíltak, megjelent a kényelmesebb átvételt biztosító időablakos kiszállítás, mi pedig például olyan szolgáltatást indítottunk, melynek keretében a megrendelt termékeket még aznap este kiszállítjuk Budapest területén. De érdemes megemlíteni azt is, hogy olyan piaci szereplők is nyitottak más területek felé, mint például az ételkiszállításban érdekelt Wolt a non-food szegmens felé. Velük közösen hoztunk létre olyan belvárosi raktárakat, amelyekből 60 percen belül megvalósítható a kiszállítás", számolt be a változásokról Perényi András.

A Webshippy a járvány kitörése előtt vette birtokba új bázisát, a 10 ezer négyzetméteres robotizált raktárban közel 3000 webáruház teljes rendeléskiszolgálása zajlik, és a kiszállított csomagok által generált árbevétel az elmúlt egy évben több mint 11 milliárd forintot tett ki. Az utóbbi két év fejlődése a csapat növekedését is magával hozta, már nagyjából kétszázan dolgoznak a cégnél.

A Pozsony mellett, illetve Prágában nyíló raktárbázisok az induláskor 3000 négyzetméteresek lesznek és Perényi András szerint a magyar, szlovák és cseh e-kereskedőknek is lehetőséget kínálnak arra, hogy gyorsabban érjék el ezeket a piacokat. Azt egyelőre nem döntötték el a társaságnál, hogy merre folytatják majd a régióban a terjeszkedést, a társalapító közlése szerint azonban 3 éven belül szeretnék teljesen lefedni a közép-kelet-európai térséget.

Felültek a hullámvasútra

Hullámvasúthoz hasonlította az e-kereskedelmi piac történéseit az elmúlt bő két évben *Tóth Soma,* a Recart alapító-ügyvezetője. Az online kereskedők és a fogyasztók közötti kommunikációt hatékonyabbá tevő, a mobil platformra fókuszáló szolgáltatást kínáló startup vezetőjének tapasztalatai szerint a Covid-járvány kitörése utáni néhány hét pánikhangulatot hozott, nagyot fékezett az e-kereskedelmi piac is, ezt követően viszont látványos felfutás indult, mivel az emberek rákényszerültek arra, hogy online vásároljanak, sokan először próbálták ki ezt a lehetőséget. A múlt év második fele ehhez képest megtorpanást hozott, érezhető volt, hogy az emberek

Az öt legnagyobb e-kereskedelmi szektor 2021-ben

Szektor	Bruttó forgalom (milliárd forint)	Bruttó átlagos kosárérték (forint)
Műszaki cikk	270	30 900
Ruházat, divat és sport	196	13 617
Játék és kultúra	140	15 004
FMCG	118	20 374
Számítás-technika	113	23 202

FORRÁS: GKI DIGITAL ÁRUKERESŐ.HU

FORRÁS: WEBSHIPPY

PERÉNYI ANDRÁS, WEBSHIPPY

FORRÁS: RECART

TÓTH SOMA, RECART

örültek annak, hogy visszatérhetnek a hagyományos üzletekbe. Azonban az elmúlt pár hónapban ismét úgy néz ki, hogy visszatér a gyorsabb fejlődés, ami Tóth Soma szerint annak is köszönhető, hogy akik a korlátozások idején kipróbálták az internetes vásárlást, időről időre visszatérnek ehhez.

A Recart szolgáltatása iránti kereslet csak részben követte le a piaci trendet, a pandémia kitörése utáni időszakban, ha kis számban is, de veszítettek ügyfeleket, majd komoly növekedésnek indult a piac, ami náluk is éreztette hatását. „A negatív hullám minket kevésbé érint, mert mi kifejezetten hatékony marketingeszközöket kínálunk, amelyek magas megtérülést hoznak. Az SMS-sekkel, Facebook-, Messenger-üzenetekkel a márkák hatékonyabban tudnak kommunikálni a fogyasztókkal, mint más megoldásokkal, ezért az utolsók között vágnák vissza az erre szánt költségvetést. Az értékesítés hatékony támogatása azért is kulcsfontosságú, mert a költségek sokszorozódtak az elmúlt időszakban az e-kereskedelemben,

3 éven belül szeretnék teljesen lefedni a közép-kelet-európai térséget

sokkal intenzívebb inflációt tapasztalnak a vállalkozások, mint amit a fogyasztók érzékelnek. Elég csak annyit mondani, hogy a Facebook-hirdetések átlagára 2,5-szeresére emelkedett, míg annak a költsége, hogy a kínai Sencsenből Los Angelesbe elszállíttassanak egy konténernyi árut, a hétszeresére emelkedett. Mi új vásárlót ugyan nem tudunk hozni, viszont abban nagyon hatékonyak vagyunk, hogy a meglévő figyelmet fogyasztássá változtassuk, és ezt értékelik az ügyfeleink", vázolta a helyzetet Tóth Soma.

A budapesti mellett New York-i irodát is működtető cég tavaly nyáron kapott 3,5 millió dolláros befektetést, ami egyelőre fedezi a további növekedési terveiket. A jelenleg mintegy 40 fős csapat túlnyomó többsége, több mint 30 ember a termékek fejlesztésével foglalkozik, így a következő időszakban az értékesítésre, a marketingre fókuszálnak. Főként az amerikai piacon igyekeznek erősíteni, bár már most is az ügyfeleik 80-85 százaléka az Egyesült Államokból van, de szeretnék jelentősen növelni a számukat. „10-15 fővel tervezzük bővíteni az amerikai csapatot, a fejlesztés ugyanakkor marad a budapesti központban, ahova szintén tervezik néhány további munkatárs felvételét", mondta el Tóth Soma.

Kalocsai Zoltán

MEGTÖRT A LENDÜLET A BEFEKTETÉSEKNÉL

A kiberbiztonság és a védelmi ipar felé mozdulhat a tőke

FORRÁS: 123RF.COM

Az idei első negyedévben megtört az elmúlt időszakban tapasztalt lendület a kockázatitőke-befektetések területén, de még így is minden idők ötödik legjobb három hónapos periódusán vagyunk túl. Az orosz-ukrán háború és az energiaválság egyelőre csak mérsékelten hat a piacra, de hosszabb távon komoly átrendeződést hozhat, ha a kiberbiztonsági és védelmi megoldásokat fejlesztő innovatív cégek felé fordul a befektetők figyelme.

Különleges év volt 2021 a kockázatitőke-befektetések esetében, hiszen minden negyedévben megdőlt az összegrekord. A KPMG legfrissebb, az idei első negyedévről szóló „Venture Pulse” elemzése alapján azonban ez a lendület 2022 elején megtört. Az idén január-márciusi időszakban 144,8 milliárd dollárt fektettek be világszerte a kockázatitőke-cégek innovatív vállalkozásokba, ez 8,2 milliárd dollárral maradt el az egy évvel korábbi értéktől és 47 milliárd dollárral a múlt év utolsó három hónapjának eredményétől. A csökkenés ellenére 2022Q1 egyáltalán nem volt rossz negyedév a befektetett összegeket vizsgálva.

Nincs kiszállás

A járvány lassan két és fél éve van velünk, és ahogy a tavalyi befektetési aktivitás mutatta, ezzel már megtanult együtt élni a piac. Azonban a múlt év második felében felpörgő infláció, majd a februárban kirobbant orosz-ukrán háború, a nyomában érkező energia- és egyre fenyegetőbb élelmiszerválság új helyzetet teremtett, amire természetesen reagáltak a kockázatitőke-cégek is: többek között más, válságos időszakokhoz hasonlóan látványosan visszafogták a korai fázisú cégekbe történő forráskihelyezést. Ezek magas kockázatot jelentenek, ami konjunktúra idején inkább bevállalható, mint a jelenlegi bizonytalan geopolitikai helyzetben. Az első negyedév másik meghatározó, a globális problémákra utaló trendje az exitek jelentős visszaesése volt. Az elsődleges részvénykibocsátásra készülő cégek is inkább átgondolták az erre vonatkozó terveiket a tőzsdéken tapasztalható bizonytalanságok miatt, illetve sokan gondoltak úgy, hogy inkább kivárnak meglévő érdekeltségeik értékesítésével. Ez azt eredményezte, hogy míg a tavalyi első negyedévben még 340 milliárd dollár fölött volt a kockázati tőkével is finanszírozott innovatív vállalatok esetében az exitek összértéke, addig az idei első három hónapban ennek az összegnek alig több mint harmadát sikerült elérni, 122 milliárd dollárt.

Rengeteg unikornis

A KPMG „Venture Pulse”-hoz hasonló megállapításokra jutott a CB Insights „State of Venture Q1’22” című jelentése is. Az ő számításaik szerint a kockázati tőkéből megvalósult befektetések összértéke 143,9 milliárd dollár volt az év első három hónapjában, ami 19 százalékkal maradt el az előző negyedéves eredménytől. Számításaik szerint ugyanakkor a tavalyi év január-márciusi időszakát sikerült túlszárnyalni, így minden idők negyedik legjobb három hónapos periódusa volt az első negyedév. A kutatócég által megabefektetésnek tekintett, százmillió dollárt meghaladó forráskihelyezések száma meghaladta a 350-et, és összesen 73,6 milliárd dollár jutott ilyen méretű ügyletek révén az innovatív vállalatokhoz.

A piacon már bizonyított, sikeres startupok – amelyek inkább már scale-upok – a január-márciusi időszakban is számíthattak a befektetők pénzére. Ráadásul a KPMG elemzése szerint meglepően sok, összesen 11 országban volt példa arra, hogy 500 millió dollárt meghaladó forrást kapjon egy ottani székhelyű innovatív vállalkozás.

Az Egyesült Államok, Kína, India, vagy éppen az Egyesült Királyság nem számít meglepőnek egy ilyen felsorolásban, de török, finn, vagy éppen szingapúri startupok ritkábban szoktak szerepelni a nagy tranzakciók listáján. Érdekesség, hogy ismét sikerült látványos eredményt elérnie az észt startup-ökoszisztémának, az új játékosnak nem nevezhető Bolt az év elején egy 628 millió eurós befektetést zárt le, amivel a cég értéke 7,4 milliárd euróra nőtt.

A legnagyobb kockázatitőke-befektetések 2022 első negyedévében

(millió dollár)

Cég	Összeg	Ágazat	Ország
Altos Labs	3000	biotechnológia	Egyesült Államok
Checkout.com	1000	fintech	Egyesült Királyság
Flexport	935	logisztika	Egyesült Államok
Wefox	878	fintech	Németország
BYJU’S	800	edtech	India
JD Property	800	proptech	Kína
Changan New Energy Vehicle Technologies	784	zöld technológia	Kína
Getir	768	e-kereskedelem	Törökország
Ramp	750	fintech	Egyesült Államok
Bolt	710	közlekedés	Észtország

FORRÁS: KPMG VENTURE PULSE Q1 2022

Ez a cikkünk írásakor érvényes árfolyamon 2745 milliárd forintnak felelt meg, összehasonlításként a MOL Nyrt. kapitalizációja a BÉT adatai szerint április 22-én 2543,5 milliárd, az OTP Banké pedig 2993,2 milliárd forint volt.

A Bolt egyébként ezzel a friss forrással bekerült a tíz legtöbb befektetést gyűjtő scale-up közé, igaz, éppenhogy, hiszen a tizedikek ebben a rangsorban. A legnagyobb befektetést az amerikai Altos Labs kapta, a biotechnológiával foglalkozó társaság 3 milliárd dollárhoz jutott, hogy tovább folytathassa fejlesztéseit. A fintech-területen tevékenykedő, londoni központú Checkout.com egymilliárd dollárral gyarapodott az idei első negyedévben, míg a harmadik legtöbb forrást – 935 millió dollárt – a logisztikával foglalkozó Flexport szerezte meg. *(Lásd a táblázatot!)*

A CB Insights elemzéséből pedig az is kiderült, hogy március végére újabb történelmi csúcsra, 1070-re emelkedett az unikornisok, vagyis az egymilliárd dollárnál értékesebb startupok száma. Ez éves szinten 62 százalékos növekedést jelentett.

Védelmi kérdések

A következő időszakra vonatkozóan a KPMG szakértői azzal számolnak, hogy a geopolitikai helyzet alakulása miatt két terület az eddiginél jóval nagyobb figyelmet kaphat a befektetők körében. Az egyik ezek közül a kiberbiztonság – az első negyedév nagy ügyletei közül például a 650 millió dollárt kapó kanadai 1Password is ezzel foglalkozik –, ami a fenyegetések számának növekedésével, illetve az orosz-ukrán háborúval összefüggésben még fontosabbá válik világszerte, így érthető módon a kockázatitőke-cégek is keresik az ígéretes vállalkozásokat ebben a szegmensben.

A másik figyelemre méltó terület a védelmi ipar lehet, amely ugyan inkább állami társaságok és globális nagyvállalatok terepe, de például a drón-technológiák, vagy a rakéták elleni megoldások esetében startupoknak is lehetnek hasznos megoldásaik.

A kibontakozó energiakrízisre, illetve a klímaváltozás elleni harc fontosságára reagálva az alternatív energiaforrásokra és energiatárolásra fókuszáló startupok, valamint az e-autózásban érdekelt innovatív cégek is komolyabb befektetői figyelemre számíthatnak a következő időszakban.

Kalocsai Zoltán

KIBERBIZTONSÁGI KÖRKÉP

Régi biztonsági kockázatok új köntösben

A vállalatok számára új kiberbiztonsági kockázatokat teremtett a megváltozott politikai és gazdasági környezet, a régi, közismert támadások új ruhába öltözve veszélyeztetik a szervezetek működését. Biztonságtudatossági oktatásokkal, az infrastruktúra, a partnerek és az ellátási lánc szereplőinek átvizsgálásával védekezhetünk hatékonyan. A valós IT-biztonságnak persze ára van. Ha a védelmi infrastruktúrát kockázatarányosan, a megbízható IT-szolgáltatókkal közösen alakítjuk ki, minden egyes forintot garantáltan jól költünk el. *Zala Mihállyal,* az EY kiberbizonsági üzletágának vezetőjével beszélgettünk.

– Hogyan változtak a kiberbiztonság trendjei a közelmúlt társadalmi és politikai eseményeit figyelembe véve?

– A járvány jellemezte időszakban minden vállalat számára a távmunka és a vele kapcsolatos biztonsági kihívások kerültek előtérbe. Ekkor a vezetők számára a kiberbiztonsági kockázatok hátrább sorolódtak a fontossági listában és nem meglepő módon az üzletmenet-folytonossági, járvánnyal, katasztrófákkal kapcsolatos aggodalmak váltak hangsúlyossá. Azonban a 2022 elejére jellemző gazdasági problémák és a háború miatt a vállalatok és vezetőik számára újból az kiberkockázatok és az ellátási lánc biztonsága került első helyre. A világ rendkívül polarizálttá vált, a különböző vállalatokat vélt vagy valós politikai hovatartozásuk, cselekedeteik miatt támadnak. A cégek számára ez teljesen új kockázatot jelent, ami miatt nehezen tudják megítélni az esetleges támadások okait. Mindezekre a változásokra a hétköznapi bűnözők is felfigyeltek, és az új helyzetet kihasználva igyekeznek pénzügyi hasznot húzni. Így biztos szép számmal jelentek meg olyan szervezetek, amelyek nem egy legitim alapítvány, hanem saját számlájukra utaltatják manapság akár a menekülteknek kért összegeket is. Ezt már a Covid-járvány esetében

> Még a magas biztonságtudatosságú, a területre kiemelten figyelő cégeknél is lehet hibákra bukkanni

is tapasztaltuk. Az adathalász-támadások akkor a leghatásosabbak, ha az emberek félelmeire, segíteni akarására támaszkodnak. Ezt a bűnözők is nagyon jól tudják. A régi kockázatok most új köntösbe öltöztetve jelennek meg.

– Egy ilyen környezetben milyen támadások kivédésére készüljenek fel a vállalatok?

– Azt gondoljuk, hogy az infrastruktúra elleni támadások jelentősége felértékelődik. Ezt azt jelenti, hogy vállalati viszonylatban nem elég csak egy-egy kritikus üzleti alkalmazást megvizsgálni kiberbiztonsági szempontból, vagy felmérni annak kockázatait. A kevésbé képzett támadók eszköztára is eléggé széles már ahhoz, hogy bármilyen piciny sérülékenységet kihasználva bejussanak a vállalati hálózatba. A támadóknak van idejük alaposan végig nézni minden interneten fellelhető domaint és aldomaint, leltárba veszik az összes, interneten működő szolgáltatást, minden eszközt alaposan megvizsgálnak. Például, ha a kontraktorok számára is van külön fenntartott kommunikációs csatorna, az sem kerüli el figyelmüket. Ha ebben a komplex vállalati infrastruktúrában csak egy sérülékeny elem van, a támadók azonnal lecsapnak, és rajta keresztül eljutnak a kritikus alkalmazásokhoz is.

Az EY-nál nagyon sok vállalati ügyfelünk hálózatát teszteljük és vizsgáljuk. Sajnos, azt kell mondanom, hogy még a magas biztonságtudatú cégek esetében is, akik kiemelt figyelmet fordítanak erre a területre, találunk problémákat és hibákat. Volt olyan ügyfelünk is, akinél pont a nem üzleti rendszereken keresztül tudtunk eljutni a legutolsó HR-es információig, csak egyszerűen végig kellett menni a közismert hibákon.

– Vannak olyan támadástípusok, melyek megújultak, esetleg hatékonyabbá váltak?

– Az ellátási láncokat ért támadások okait nehezebb megítélni. Egyértelműen romboló, gazdaságilag értelmetlen szándékok is megjelentek. A háború miatt voltak és lesznek olyan támadások, melyeknek célja a termelést lelassítani vagy teljesen megakasztani. Míg korábban egyértelműen gazdasági szándék volt a jellemző, egyszerűen a pénzszerzés vagy a versenytársak kiiktatása volt a cél.

Változtak az adathalász támadások is. Sok esetben felderítő tevékenység előzi meg elindításukat. A vállalat életét jobban megismerve sokkal valószínűbb, hogy célba érnek. Célzottan támadják azokat a kulcspozícióban lévő embereket, akik kiemelt jogosultságú felhasználók vagy akiknek hozzáférésük értékesebb lehet a fekete piacon. A gépi fordítók helyett emberi intelligencia fogalmazza meg ezeket a leveleket, így a rossz helyesírás sem fedi fel kilétüket.

– Az IT-biztonságot felhőszolgáltatásként is igénybe lehet venni. Mennyire nyitottak erre a magyar vállalatok?

– Sajnos érettségben még nem tartanak ott a magyar kis- és közepes méretű vállalatok, hogy az IT-biztonságot a felhőből vegyék igénybe. A felhőszolgáltatás itthon biztonság területén még mindig

ZALA MIHÁLY, EY

FORRÁS: ITBUSINESS

tabu téma. Pedig a hardvert, szoftvert és IT-szolgáltatást is sokkal kedvezményesebben lehet a cloudból használni, mint ha saját magunk építenénk ki. Arról nem is beszélve, hogy a rendszerek üzemeltetéséhez szükséges szakembereket nehezen vagy egyáltalán nem találják meg a cégek. Arra is kell gondolni, hogy egy felhőszolgáltató esetében nemcsak előfizetek a biztonságra, hanem egy nemzetközi szakértői csapat tudásához és szakértelméhez is hozzáférek.

– Mit javasol, milyen eszközökre helyezzék a hangsúlyt a szervezetek védekezéskor?

– Azt tapasztaljuk, hogy a biztonságtudatosító oktatásoknak kiemelt szerep jut, esetenként 75-80 százalékkal is növelhető a kollégák biztonságtudatossági szintje. Szerencsére léteznek már olyan oktatási eszközök, melyek segítségével célzottan mérhető a kollégák tudatossági szintje, nyomon követhető, hogy milyen területeken van szükség további oktatásra és milyen területeken kiváló a tudás. Például adathalász támadások esetében eléggé szofisztikált forgatókönyvek segítségével lehet tesztelni a kollégák tudását. A tesztleveleket nem egyszerre, hanem szétszórva, különböző bontásokban küldjük el, egy dashboardon nyomon tudjuk követni, ki mennyit fejlődött az előző teszthez képest.

A második védekezési eszköz az infrastruktúra már említett átvizsgálása. Részletekbe menően érdemes átnézni és kivizsgálni, hogy hol, milyen sérülékenységek vannak, és nemcsak a core rendszereket kell megnézni, hanem az összeset. Ha már az infrastruktúrát vizsgáljuk, akkor érdemes annak terhelhetőségére és áteresztőképességére is időt szánni, így egy kisebb DDoS-támadásnak még ellenáll a rendszer.

Harmadik megvizsgálandó pont az ellátási lánc szereplői és a partnerek egyaránt. Nagyon sok vállalatnál kényelmi és gazdaságossági szempontok miatt a BYOD még mindig divat. Viszont érdemes ezeket a külső eszközöket is egy vállalati biztonsági szabályzat szerint beengedni a céges hálózatba, vagy a szegmentáció elve szerint eleve egy teljesen önállóan működő hálózatba szervezni őket. A járvány miatt elrendelt távmunka egyébként a hálózati szeparáció legnagyobb tesztje volt.

A rossz hírem az, hogy az IT-biztonság megteremtése pénzbe kerül. Azonban, ha a védelmi infrastruktúrát kockázatarányosan, megbízható IT-szolgáltatókkal közösen alakítjuk ki, minden egyes forintot garantáltan jól költünk el. ■

ITBUSINESS Club Liferay

FORRÁS: ITB

Balogh Zsolt
Liferay, ügyvezető

Bakk József
IDC, country manager

Schopp Attila
ITBUSINESS, főszerkesztő

Mester Sándor
ITBUSINESS, moderátor

MÁJUSI ITBUSINESS CLUB

Így tedd élménnyé a digitalizációt!

Magyarországon műszaki szempontból minden adott lenne a felhőtechnológia széleskörű alkalmazásához, sokan mégis ódzkodnak tőle. A vállalatvezetők gondolkodását, hozzáállását könnyebb megváltoztatni, ha látják: lehet egyszerűen, élményszerűn is végrehajtani a digitalizációt.

Az elmúlt két év a szkeptikusok számára is világosan bebizonyította, hogy a digitalizációs fejlesztések elengedhetetlenek, és azokban kulcsszerepet játszik a cloud, a számítási felhő. A felhő nélkül sokkal nehezebb lépést tartani a folyamatos technikai fejlődéssel, naprakészen tartani a teljes szoftverkörnyezetet, belevágni a mind több területen hasznot hozó mesterségesintelligencia- és IoT-fejlesztésekbe, vagy akár gondoskodni az informatikai rendszerek kiberbiztonságáról. Magyarországon ezzel együtt sokan még nem mernek felhőmegoldásokban gondolkodni, számukra a papír alapú megoldásokról való áttérést jelenti a digitális transzformáció.
Pedig számukra is van kész válasz. Az ITBUSINESS Club májusi rendezvényén kiderül, hogy egyszerűen is megoldható a vállalatok számára a digitális, felhő alapú megoldások kialakítása és fejlesztése. *Balogh Zsolt*, a Liferay ügyvezetője bemutatja, miként lehet teljesen testre szabható szoftvereket készíteni, akár kódolás és fejlesztők nélkül a Liferay Experience Cloud és az azon keresztül elérhető digitális élményplatform segítségével, és mit jelent a vállalat számára a „cloud-first” stratégia. Vendégelőadónk, *Bakk József*, az IDC Magyarország country managere pedig érdekes, eddig máshol még nem ismertetett elemzésekkel és adatokkal rukkol elő a felhőhasználattal és -projektekkel kapcsolatban.

Várjuk önt is szeretettel az ITBUSINESS Club májusi rendezvényén, amelyet ezúttal is a Magyar Tudományos Akadémia székházában rendezünk meg.

Időpont: 2022. május 10., 9:00-11:00 óra
Helyszín: Magyar Tudományos Akadémia Klub, Kodály-terem
(Budapest, V. ker., Széchenyi István tér 9.)

Meghívott vendégeinknek a részvétel díjtalan.
A meghívóval nem rendelkezők részvételi díja 50 000 Ft + áfa.

A KIS SEGÍTSÉG IS SEGÍTSÉG

Az adományozásban is előtérbe kerül a digitalizáció

A közelünkben dúló háború felébresztette a magyar lakosság adományozási kedvét. A korábbi összegek sokszorosát küldik az ügyfelek az OTP Bank rendszerein keresztül is, amihez hozzájárul, hogy digitálisan az adományozás is egyszerűbb.

A háború kitörésének napjától, február 24-től, egy bő hónap alatt, március 29-ig a korábbi napi átlag 13-szorosára emelkedett az átutalásos tranzakciók darabszáma, értékük pedig a korábbi 28-szorosára ugrott. A bankkártyás támogatások esetében még látványosabb volt a növekedés: a napi tranzakciók száma a korábbi 38-szorosára, értékük pedig több mint 54-szeresére emelkedett – derült ki az OTP Bank Data Series sorozatából. A pénzintézet hét segélyszervezet (Magyar Máltai Szeretetszolgálat, Magyar Ökumenikus Segélyszervezet, Magyar Vöröskereszt, Baptista Szeretetszolgálat, Református Szeretetszolgálat, Oltalom Karitatív Egyesület, Híd Kárpátaljáért összefogás) számlájára utalt pénzadományok tapasztalatait összesítette.

Fiatalabbak és gazdagabbak

Az adatokból az is kiderült, hogy az ilyen csatornákon adakozók az átlaghoz képest magasabb jövedelemmel rendelkeznek, intenzívebben használják az online banki csatornákat és nagyobb arányban vannak köztük olyanok, akik már a háború kitörése előtt is adományoztak valamely említett szervezetnek. Életkoruk alacsonyabb a teljes ügyfélkör 51 éves átlagánál; a kártyával adományozók esetében ez 42 év, amely összefügg azzal, hogy a széles körű kártyahasználat inkább a fiatalabb korosztályokat jellemzi.
Az adományozás digitális csatornáinak kifejlesztése igényelt fejlesztéseket az egyes rendszerekben – tudtuk meg az OTP Banktól. Korábban a bankfiókok ügyfélterében kihelyezett átlátszó gyűjtődobozokat használtak, és az ezekben összegyűlt összegeket juttatták el a megjelölt civil szervezeteknek.

Adománycsatornák

Az OTP Bank több különféle csatornán is lehetővé teszi az adományozást.

– Weboldal: kiválasztható, hogy mely szervezetnek szeretne adományozni az ügyfél, és rendszeres fix vagy szabadon választott egyösszegű támogatás utalható.
– ATM-ek: a készpénzfelvételi folyamatba beépített adományozásra jelenleg mintegy 800-850 automatánál van lehetőség; a rendszer egy adott alapítványt és 200 forintos adomány lehetőségét ajánlja fel.
– Simple alkalmazás: az „Adományozás” lehetőség a bank weboldalára irányítja az érdeklődőket.
– Internetbank és mobilbank: az azonnali utalás során egyszerűen és díjmentesen adományozhatnak az ügyfelek a kiválasztott szervezetnek.

FORRÁS: OTP BANK

Azonban ezen a téren is előtérbe került a digitalizáció, hogy az ügyfelek a mindennapi pénzügyek intézése közben, kényelmesen tudjanak jótékony célokra adakozni. Ugyanakkor nem csak az adományozás lett könnyebb, hanem az adott civil szervezethez is gyorsabban, egyszerűbben jutnak el a pénzösszegek.

Sok kicsi sokra megy

A bank tapasztalatai szerint nagyban növeli az adományozási kedvet, ha azt egyszerűen lehet végezni. Az is előnye a programnak, hogy kis összegekkel is hozzá lehet járulni egy-egy jó ügy támogatásához. Az adományok összege az ATM esetében 200 forint lehet, az új internet- és mobilbank használatakor pedig 100, 200 vagy 500 forint. Itt az átutalások utolsó lépéseiben kínálja fel a rendszer az adományozás lehetőségét. A weboldalon és a Simple alkalmazáson keresztül más, illetve nagyobb összegek utalására is lehetőség van – érkeztek már több tízezer forintos adományok is.
Szintén növeli az adományozás esélyét, hogy az ügyfelek az OTP Bank által kiválasztott szervezetek projektjeit tudják támogatni. Ennek révén ugyanis biztosak lehetnek abban, hogy adományuk eljut a címzetthez és megfelelően hasznosul. ■

AZ OROSZ-UKRÁN KIBERHÁBORÚ HATÁSAI A GLOBÁLIS IT-TÁRSADALOMRA

Háború az ötödik dimenzióban: kiberpartizánok akcióban

FORRÁS: 123RF.COM

Több mint ötven napja tart az orosz-ukrán fegyveres konfliktus, ami új megvilágításba helyezte azt, amit eddig a kiberhadviselésről gondolunk: többé nem a fizikai hadviselés, hanem az ötödik hadszíntér, ahol a soha nem látott események zajlanak. Eltévedt „kiberrepeszek”, mozgó kiberfront, hacktivizmus és legégetőbb kérdés: mit hoz az orosz-ukrán kiberkonfliktus a globális és a regionális IT-biztonságra és a jövőre nézve?

A kiberhadviselés több évtizedes múltra tekint vissza, hiszen már a 90-es évek végén, a 2000-es évek elején különböző lehallgatásoktól volt hangos az amerikai sajtó, míg az első súlyosabb kibercsörte az amerikai és kínai állam között 2003 környékére tehető. A világ szeme még 2007-ben szegeződött a kibertérre, ahol Oroszország lerohanta az akkor már az e-közigazgatással kacérkodó Észtországot, a célzott és túlterheléses támadásokkal pedig néhány napra leradírozta az észt kormányzatot és az észt bankrendszert a világhálóról. Ez akkor nem torkollott fegyveres konfliktusba, de a köztudatba emelte, hogy nemcsak a fizikális térben robbanhat ki háború. Kilenc évvel később a NATO deklarálta, hogy az információs hadviselés olyan valódi hadviselés, amelynek hadszíntere a kibertér. Hat évvel később 2022-ben pedig kirobbant egy olyan kiberháború, amelyhez foghatót talán még soha nem tapasztaltunk.

Kik vannak célkeresztben?

A kibertér február 24-e előtt sem volt eseménytelen, a háború kirobbanását megelőző és az azóta tartó időszak, azonban felülírta az elképzeléseket.

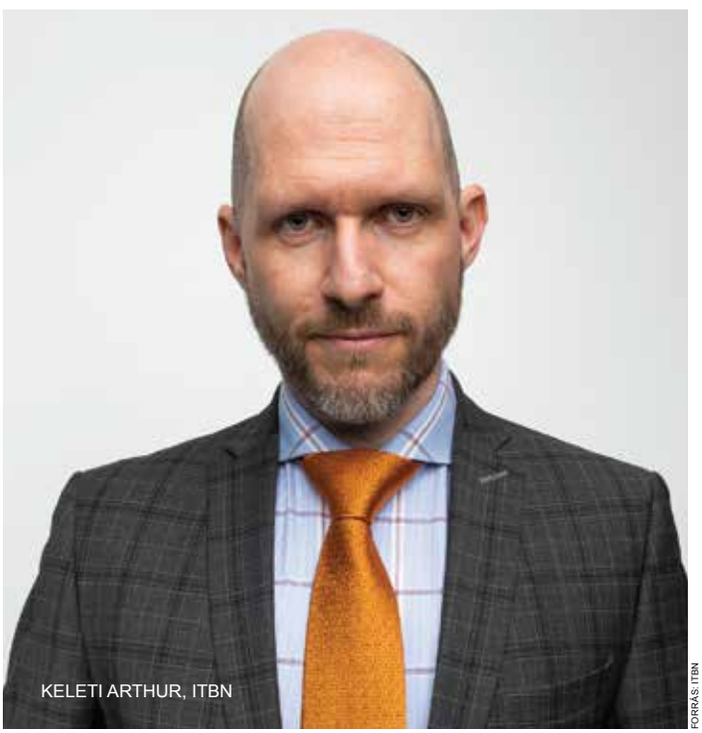
„Trendek szempontjából a kiberháború sebessége és a kiterjedése az, ami szembetűnő. Míg korábban az államokat, kritikus infrastruktúrát, nagyvállalatokat érő támadások kielemzésére és az abból kiolvasható következtetések levonására és integrálására két-három hét vagy adott esetben egy hónap is rendelkezésre állt, most egy-egy ilyen támadás esetén nem, mert már nemcsak havonta egy-kettő fordul elő, hanem napi szinten, óránként érkeznek beszámolók több száz gigabájtnyi adatot vagy több százezer emailt érintő kibertámadásokról”, mondta *Keleti Arthur*, kibertitok-jövőkutató, az Informatikai Biztonság Napja (ITBN) alapítója, az Önkéntes Kibervédelmi Összefogás elnöke.

A támadások célpontjai között szerepelt például az orosz atomenergia-központ, a Kreml honlapja, az orosz posta, egy fehérorosz fegyvergyár, egy orosz gázállomás, a fehérorosz vasúti irányítórendszer vagy az orosz állami tévé. A korábban „tabutémának” számított katonai vagy nukleáris rendszerek sem kivételek, és nem kímélték a titkosszolgálatokat sem. De ugyanez igaz visszafelé is, ukrán vonatkozásban. Ebből a korántsem teljes listából látszik, hogy a célpontok között a kritikus infrastruktúrák – a lakossági ellátásbiztonság stratégiai fontosságú intézményei, úgymint erőművek, kórházak, közműszolgáltatók stb. – előkelő helyet foglalnak el.

„Az is gyakori, hogy kormányzati dolgozók, hivatásos katonák, a különleges egységben szolgálatot teljesítők személyes adatai kerülnek nyilvánosságra. Korábban teljesen elképzelhetetlen volt, hogy ezek az érzékeny adatok nemcsak a hackerek, de a civil lakosság számára is könnyen elérhetővé váljanak. Nemcsak a sebessége gyorsult fel a támadásoknak, hanem a volumene is megnőtt. Csak az elmúlt időszakban több mint 2 terabájt anyag szivárgott ki az orosz-ukrán kormányzati rendszerekből, és a közeljövőben is számíthatunk nyilvánosságra kerülő személyes adatokra, amelyek további sérülékenységekhez vezethetnek. Sajnos, ilyen jellegű, akár teljes szervezetek belső levelezését, érzékeny információit érintő, egyfajta közel 100 százalékos adatszivárgás hatékony kezelésére a legtöbb magyar cég vagy szervezet nem áll készen”, tette hozzá Keleti Arthur.

Targetlista, eltévedt támadások, újrarajzolt védelmi vonalak

Az új keletű támadási formák, és a kevésbé újak is, mintegy „eltévedt golyóként”, a háborúhoz látszólag nem kapcsolódó vállalatokat és a magánfelhasználókat is eltalálhatják. Nem beszélve arról, hogy a szankciókat nem támogató vagy az álláspontjukat nem egyértelműen



KELETI ARTHUR, ITBN

FORRÁS: ITBN


MÁRTON MIKLÓS, VIVETECH

FORRÁS: VIVETECH

kinyilatkoztató országok is felkerülnek a hackerek targetlistájára – ahogy ez Magyarországgal vagy azokkal a vállalatokkal is megtörtént, amelyek nem vonultak ki Oroszországból.

„Előfordulnak »eltévedt« támadások, de ebben a láthatatlan háborúban legfőképpen célzott támadásokról beszélhetünk. Ami jelenleg Oroszország vagy Ukrajna ellen irányul, az főleg hacktivistákhoz, hackercsoportokhoz köthető. A célpontok leginkább kormányzati, hivatali szervek informatikai rendszerei, a hozzájuk kapcsolható belső információk, viszont vannak »civil« célpontok is. Ezek legtöbbször szintén valamilyen formában a háború egyik résztvevőjéhez köthetők; orosz vagy ukrán vállalkozások, esetleg valamelyik félhez politikailag közelebb álló nemzetek kormányzati, hivatali informatikai rendszerei. Orosz oldalról kibertámadás áldozata lett például a Sberbank, míg Ukrajna esetében az UkrTelecom, ezek mellett folyamatos, jellemzően túlterheléses támadások érik a résztvevőkhöz köthető vállalatokat. A civil lakosok nem célpontjai a támadóknak, ezt sok csoport nyilvánosan is lenyilatkozta a közösségi médián keresztül”, mondta *Márton Miklós,* a ViVeTech vezérigazgatója. Hozzátette, hogy „a háború előtt is voltak már támadások, ezek azonban nem feltétlenül jelentek meg koncentrált formában. Amikor egy nagyobb vállalatot súlyos támadás ér, az eseményből felkapott hír lesz, és több emberhez eljut az információ. Fontos azonban leszögezni, hogy nemcsak azok a kibertámadások történnek meg, amelyeket lehoz a sajtó, hanem olyanok is, amelyekről pillanatnyilag az érintett szervezet maga sem tud. Emiatt nagyon nehéz közelítő értéket is mondani arról, hogy valójában mennyi támadás történik a világ számos pontján, akár ebben a pillanatban is.”

Új hullámos hacktivizmus

Bármennyire is azt sulykolják a filmek, valójában nem ül fekete csuklyás, fehér maszkos emberek garmadája, ablaktalan, kék LED-visszfényben derengő gigászi számítógéptermekben, ölükben laptoppal. A valóság ennél sokkal hétköznapibb. „Ebben konfliktusban nemcsak szervezett és profi hackerek vesznek részt ideológiai meggyőződésük függvényében az orosz vagy ukrán oldalon, hanem amatőrök is, akik nem összeszedett hackercsoportokban, hanem egyedül, civilként támadnak, ami a hivatalos jogrend szerint a háborúba való beavatkozást jelenti”, fogalmazta meg Keleti Arthur.

A hackerek ilyen mértékű háborús beavatkozása komoly etikai dilemmákat vet fel a szakemberek körében. „Kritikus infrastruktúrák támadására biztat mindkét fél, amelyeket törvényes módon nem lehet megtámadni. Izgalmas, hogy a legtöbb ukrán szimpatizáns NATO-tagországokban található, így, ha szigorúan nézzük, ezek a szereplők beavatkoznak a háború menetébe. Eddig nagyjából nyolcvan olyan önkéntes hackercsoportot azonosítottak, akik szervezett formában támogatják az erőfeszítéseket, de ezekben a szerveződésekben nemcsak jó fiúk, hanem kiberbűnözők is vannak”, mondta Keleti Arthur.

Nem lehet szemet hunyni a magánzó hacktivisták felett sem. Az ő küldetésük – ukrán szimpatizánsként – bármennyire nemesnek tűnik, valójában veszélyes, hiszen azzal talán nem is számolnak, hogy egy sikeresen bevitt hackertámadásra válaszul megtorló valódi rakéta érkezhet. Kiemelendő még olyan új jelenségek felszínre emelkedése is, mint például a protestware, amelynek írója olyan változtatásokat hajt végre a szoftverben, amely ideológiai megfontolások szerint máshogy működ-

Öt kérdés a megosztott felelősségről

A kiberbiztonság üzleti kockázatot jelent, nemcsak egyszerű IT-probléma a céges igazgatótanácsok 88 százaléka szerint – derül ki a Gartner („Board of Directors Survey 2022”) adataiból. Ez az felismerés azonban nem érhető tetten a felelősségvállalás kultúrájában, a CIO és a CISO továbbra is a kiberbiztonság fő felelőse az esetek 85 százalékában. Az elemzés szerint a CIO-nak a vállalati vezetőkkel közösen kellene megosztani a kiberbiztonsági kockázatokat. Míg a szervezeten belül a CIO-ra és CISO-ra valóban a vállalati biztonság őreként tekintenek, a valóság az, hogy az üzleti vezető naponta hoz olyan döntéseket, amelyek befolyásolják a vállalat kiberbizonságát. Emiatt van szükség a közös felelősségvállalásra, amit a CIO-nak kell szorgalmaznia.

Az alábbi öt kérdés segít felmérni, hogy mennyire felkészült az üzlet az IT-csapattal közösen vállalni ezt a kiberbiztonsági felelősséget, érdemes minél hamarabb végiggondolni ezeket:

– Képes a szervezet kockázati döntéseket hozni a biztonsági szakemberek segítsége nélkül?
– Minden biztonsági kontroll üzleti értékét ki tudja mutatni az IT?
– Mit tükröznek a szervezet biztonsági kontrolljával kapcsolatos mérőszámok: a védelmi szintet (technológiai szempont) vagy a működési funkciókat (üzleti megközelítés)?
– A biztonsági döntések hány százalékát indokolja a szervezet félelmekkel, bizonytalanságokkal az üzleti célokkal összehasonlítva?
– Megvédhető-e a kiberbiztonsági rendszer az ügyfelek, érdekelt felek, szabályozók előtt?

FORRÁS: 123RF.COM

het vagy akár törölhet is, ha bizonyos gépeken, környezetben találja magát. Ugyanígy egyre gyakoribb kiberbiztonsági incidenshez vezető ok a hackerek által ideológiai alapon beszervezett belső munkatárs.
„Fontos figyelembe venni, hogy mivel politikai-társadalmi eredetű a háború, a hacktivisták sokkal intenzívebben járultak hozzá a kibertérben. Számos hackercsoport kiáll amellett, hogy a politikai-társadalmi ellentét szülte háború elszenvedői ártatlan civilek, akiknek védelme érdekében aktívan igyekeznek megállítani egyik-másik fél stratégiai infrastruktúráit az interneten keresztül. Míg a háború fizikai terében részt venni nagyon veszélyes, addig a kibertér személyi biztonság tekintetében kedvező paraméterekkel rendelkezik. Nem szükséges a helyszínre utazni, a világ bármely pontjáról vezethetők kibertámadások internetkapcsolat, internetezésre alkalmas eszköz és a szükséges biztonsági felkészültség és tudás birtokában”, mondta Márton Miklós.

Globális kilátó, és hazai körkép az orosz-ukrán kiberháború IT-biztonsági hatásairól

A háború kitörése után az EU kormányai egyhangúan elkötelezték magukat a védelmi kiadások jelentős növelése mellett. Ez nemcsak történelmi léptékű fordulat – főleg a német hadiipari fejlesztések bejelentése –, hanem azt is jelenti, hogy várhatóan jelentős erőforrásokat csoportosítanak át a kritikus infrastruktúraszolgáltatók kibervédelmére is.
„A háborúhoz köthető kibertámadások várhatóan felnyitják az emberek szemét, és nemcsak magánszemélyek esetén, de a vállalatok vezetésében is megnőhet az érdeklődés a megfelelő védekezés és az online tudatosság iránt. Amikor azt látja egy vállalatvezető a hírekben, hogy hackerek lekapcsolták a belorusz államvasutat, vagy átvették a Kreml belső kameráinak képét, akkor elgondolkodik: ha ezekbe a szuperbiztonságosnak gondolt rendszerekbe így be tudnak hatolni, akkor mit tudnak csinálni az én cégemnél? Szerintem az ukrajnai háború a nagy rádöbbenés élményét hozta el a vállalatok vezetői számára”, mondta Márton Miklós.

> A kiberbiztonság íratlan szabályai teljesen átrendeződtek, feloldódtak, a közeljövőben nem is várható, hogy normális mederbe terelődnek vissza, és ez közvetlenül érinti a magyar cégeket, szervezeteket is

A kibertámadások sokrétűek, ennek elég széles spektrumát mutatják meg a kiberháborúba bekapcsolódó csoportok. A sokrétűség és a médiavisszhang miatt viszonylag mély betekintést nyerhetünk a támadások módszereibe, a kihasznált sérülékenységek, hálózati védelmi hibák és hiányosságok körébe. A megszerzett információk alapján olyan következtetések és tanulságok vonhatók le, amelyekkel a hibák és hiányosságok egy része kiküszöbölhető, és a hasonló támadások megelőzhetők, ezzel direkt és indirekt módon is növelve a biztonsági rendszerek hatékonyságát.
„A Magyarország ellen irányuló, háborús mozgalomhoz köthető támadások száma nem túl magas, így a kiberháborúnak IT-biztonsági szempontból akár pozitív hatásai is lehetnek a fejlődésre. Ami fontos lehet Magyarország, és egész Európa számára, hogy a kritikus infrastruktúrák kiberbiztonságát meg kell erősíteni. Ez a háború megmutatta, milyen sebezhetőek és mekkora károkat tudnak okozni az erőművek, közszolgáltatások, vasutak, kórházak, vagy akár a kiskereskedelmi láncok elleni kibertámadások”, zárta gondolatait Márton Miklós.

Kiss Franciska

ÖTBETŰS MEGOLDÁS AZ INTEGRÁCIÓS KIHÍVÁSOKRA

Jolly Joker az integrációban

FORRÁS: 123RF.COM

Az ügyfelek gyors, hatékony és jó élményt nyújtó kiszolgálását a több rendszerben karbantartott adatok összeszinkronizálása teszi lehetővé, ami a hazai üzleti élet gyakorlatában egyelőre inkább kihívást jelent, mint flottul működő megoldást. Elvégre a meglévő, régi rendszerek és az újonnan érkezők esetében szinte elkerülhetetlen a kompatibilitásból adódó akadálypálya, amire a leleményes „IT-barkácsolás" helyett az integrációs platform mint szolgáltatás, azaz iPaaS nyújthat segédkezet.

Az iPaaS viszonylag új szereplője a hazai és közép-európai „as a service" piacnak. Az elterjedőfélben lévő integrációs technológia tulajdonképpen nem más, mint egy felhőszolgáltatásra épített integrációs rendszer, amely a főleg szoftverintegrációt használó nagyvállalatoknak jelent innovatív, fejlett technológiájú, könnyen bevezethető megoldást.

Buktatók, csapdák, akadályok az integráció labirintusában

Az üzleti hétköznapok vissza-visszatérő eleme a különböző a szoftverek, platformok, technológiák integrációja, ami még a legfelkészültebb szakemberek számára is tartogat kihívásokat és buktatókat. A Deloitte a témához fűződő legfrissebb tanulmá-

nyában arról számolt be, hogy három adatintegrációs projekt közül legalább egynél azon csúszik (el) az élesbe állás, hogy valamelyik rendszerben a többitől eltérően időzítették a szükséges feladatok elvégzését.
Míg az új rendszereknél többnyire kiküszöbölhető a nem kompatibilis technológiák használata, könnyen kezelhetők az adatok kinyerési sebessége és az üzleti elvárások között fennálló különbségek, addig a meglévő, sokszor elavult rendszerek integrációja szinte mindig egyedi megoldásokat kíván. Visszatérő eset az is, amikor egy szervezetnek moduláris, fejlett és modern alapokon fejlesztett informatikai architektúrára kell áttérnie az életben maradáshoz: vagy mert egyre nehézkesebben képesek fenntartani

Az iPaaS segítségével a bankoknak és a pénzügyi intézményeknek már nem kell versenyként tekinteniük a fintech iparágra

az elavult technológiákat, vagy mert a saját IT-csapatuk képtelen időben új komponenseket leszállítani. Szintén gyakran kerülnek a projektek nehéz helyzetbe amiatt, hogy nem egyeztetnek a felek az összes integrációba bevont rendszer üzemeltetőjével a tervezett dátumokról.
„Egy meglévő rendszer újításakor gyakorta találkozunk több integrációs termék párhuzamos használatával, amelyek egységesítése, kiváltása azonnali költségcsökkentést eredményezhet", mondta *Tamás G. Tamás,* a Deloitte Magyarország technológiai tanácsadás üzletágának szenior menedzsere. Ekkor kerül reflektorfénybe az iPaaS, ami a platform as a service (PaaS) és az integráció ötvözésével megteremti annak a feltételeit, hogy mindez buktatók nélkül, zökkenőmentesen történjen.

Előnyök a rugalmasság mentén

„Minden felhőszolgáltatásra igaz, hogy az üzemeltetési költségek csak a valóban felhasznált erőforrások után fizetendőek, nincs szükség felesleges szerverek fenntartására. Az iPaaS technológia másik előnye, hogy a megbízó és a felhő képességei miatt a lehető legrövidebb idő alatt és hatékonyan tud éles környezet szintű integrációt előállítani", fogalmazta meg Tamás G. Tamás.
„Az iPaaS segítségével a szervezetek könnyebben csatlakoztathatnak különböző alkalmazásokat, adatokat, üzleti folyamatokat és szolgáltatásokat függetlenül attól, hogy azokat saját üzemeltetésű környezetben, magánfelhőben vagy nyilvános felhőkörnyezetben tárolják, ezzel gyorsíthatják az üzleti folyamatokat. Néhány konkrétum: csökkentheti az adatok bevitelével töltött időt, és növelheti az alkalmazottak termelékenységét, testre szabhatja az alkalmazásokat az adott ügyféligények szerint, vagy automatizálhatja az informatikai felügyeleti feladatokat, és több felhasználót támogathat alacsonyabb költséggel, mint a hagyományos integrációs eszközök", mondta *Trinh Anh Tuan,* az IVSZ Fintech munkacsoport vezetője.

Mit várhatunk az iPaaS-tól a jövőben?

Mindezek ellenére itthon alacsonyabb a technológia kihasználtsága, mint pár ezer kilométerrel nyugatabbra. „Magyarországon gyakran a csoportos licencek vásárlásával örökölt integrációs technológiákat használták fel a cégek. Például megkötöttek egy nagyobb, adatbázis-szolgáltatásra vonatkozó szerződést, amelynek keretében hozzáfértek a vendor által forgalmazott egyszerűbb integrációs megoldásokhoz. Ez áll a hátterében annak, hogy kevesebben alkalmazzák. Ugyanakkor az iPaaS elterjedésének területi okai mögött több esetben a felhőre

FORRÁS: DELOITTE MAGYARORSZÁG

TAMÁS G TAMÁS,
DELOITTE MAGYARORSZÁG

FORRÁS: IVSZ

TRINH ANH TUAN.
IVSZ, FINTECH MUNKACSOPORT

való nyitottság is összefüggéseket mutat. Idehaza főleg a túl szabályozott nagyvállalatoknak van szüksége integrációs megoldásra, ahol az on-premise szoftvereket lassan váltják csak fel a felhőszolgáltatások", fejtette ki Tamás G. Tamás.
A közeljövőt firtató kérdésekre elárulta, hogy ha itthon is népszerűbbé válnak a felhő alapú CRM-technológiák, akkor az ezekhez leggyorsabban felállítható integrációs technológiák terjedése is élénkül majd. A másik ugrás a felhőszolgáltatásokra való tömeges áttéréskor fog bekövetkezni. „A pénzügyi szektorban már eléggé ismert ez a szolgáltatás. Az iPaaS segítségével a bankoknak és a pénzügyi intézményeknek már nem kell versenyként tekinteniük a fintech

A 360 fokos ügyfélnézet gyakran igényli az eddig több rendszerben karbantartott adatok összeszinkronizálását

iparágra. Az iPaaS segítségével gyorsíthatjuk a bankok és pénzügyi intézmények összekapcsolását a pénzügyi ágazatban zajló legújabb alkalmazásokkal és innovációkkal", tette hozzá Trinh Anh Tuan.
A vállalati rendszerek fejlődésének jelentős szeletét adja a megfelelő adat- és szoftverintegráció, hiszen az egymással kommunikáló és jól működő rendszerek mátrixa teszi azt lehetővé, hogy az adatok szabadon áramoljanak az architektúrában, támogatva az üzleti döntéshozatalt, maximalizálva az ügyfélkiszolgálást, segítve a szervezet összes folyamatát. Az IPaaS előnyei alapján valószínűsíthető, hogy gyorsan népszerűvé és keresetté válik nemcsak a szomszédos országokban, hanem Magyarországon is.

Kiss Franciska

GYORSAN MEGTÉRÜLHET AZ EMBEREKKEL EGYÜTT DOLGOZÓ ROBOTOK BEVETÉSE

Elkerülhetetlen a digitalizáció a gyárakban is

Drámai változásokon ment át a gyártás az elmúlt néhány évben, a Covid-járvány hatására a digitalizáció, az új technológiák bevetése kulcsfontosságúvá vált a termelőcégek számára. Alaposan fel is gyorsultak az ilyen jellegű fejlesztések. Egy mértékadó elemzés szerint a robotok, a 3D nyomtatás, a digitális ikrek, a virtuális- és kiterjesztettvalóság-megoldások fontos szerepet játszanak majd a jövő iparában.

FORRÁS: SIEMENS PLM

Az Ipar 4.0 koncepciót is támogató beruházások olyan, a társadalmi folyamatokból adódó tényezőkre is választ adhatnak, mint a munkaerőhiány, az elöregedő szakértőgárda, illetve a rendelkezésre álló és a szükséges tudás közötti szakadék (a „skill gap”). Ez a három most említett dolog egyébként része azoknak a hatásoknak, amelyek a CB Insights átfogó, „The Future of the Factory: How technology is transforming manufacturing” című elemzésében is szerepelnek a gyártás átalakulását mozgató erők között. A globalizáció eredményeként még kiélezettebbé váló verseny és a kutatás-fejlesztési tevékenység felértékelődése ezzel párhuzamosan szintén megtalálható a kutatócég által meghatározott fő trendek

között. Érdekesség, hogy a kutatás-fejlesztésre legtöbbet költő vállalatok között is igen magas arányban képviseltetik magukat a termelő tevékenységet is végző cégek.

Klímavédelmi elvárások

Egy másik, a modern technológiák, főként az automatizáció és a robotok magasabb szintű alkalmazását kikényszerítő tényező, hogy a globális ellátási láncban keletkezett zavarok miatt egyre több társaság igyekszik a korábban távoli országokba kihelyezett termelést visszavinni az anyaországhoz, vagy a legnagyobb piacokhoz közeli helyszínre. A CB Insights által „reshoring”-nak nevezett jelenség egyik fő gátja a rendelkezésre álló munkaerő mennyisége és költsége, amit a robotok tömeges alkalmazásával lehet enyhíteni. A világon 2020-ban átlagosan 126 robot jutott 10 ezer, a termelésben dolgozó alkalmazottra, de vannak országok, amelyekben jóval magasabb az arányuk. Dél-Korea a listavezető ebben a mutatóban, ahol 10 ezer ipari munkavállalóra 932 robot jutott már 2020-ban is, Szingapúrban 605, Japánban pedig 390 volt ez az érték.
A technológiai fejlesztéseket ösztönző tényezők között szerepel a CB Insights szerint a társadalom részéről érkező elvárás, hogy az ipari cégek is erőfeszítéseket tegyenek a klímavédelem érdekében, és egyre fenntarthatóbban működjenek. Felmérések szerint egyébként folyamatosan nő azoknak a fogyasztóknak az aránya, akik a vásárlási döntések során azt is figyelembe veszik, hogy az adott terméket mennyire fenntartható módon állítják elő, vagy mennyire van lehetőség az újrahasznosítására.

> Megjelent az üzemekben a robotok új generációja, az emberekkel közösen dolgozó, úgynevezett cobot (collaborative robot)

Segítenek az ikrek

Szerencsére már rendelkezésre állnak azok a technológiák, amelyek lehetőségek kínálnak arra, hogy az érintett vállalkozások megfeleljenek az elvárásoknak, illetve hatékonyabbá, versenyképesebbé tegyék a működésüket. A CB Insights elemzésében több technológiai trendet is meghatározott, amelyek a közeljövőben a leginkább meghatározzák majd a gyártás világát. Napjainkban a legfejlettebb ipari társaságok nagy mértékben támaszkodnak a tervező szoftverekre (computer-aided designra, CAD-re), amelyek lehetővé teszik az új termékek – legyen szó akár autókról, műholdakról, háztartási eszközökről, vagy bármi egyébről – 2 vagy 3D-s tervezését és modellezését. Ezen szoftverek piaca az előrejelzések szerint 2028-ig évente átlagosan 10 százalékkal bővül majd, a meghatározó megoldásszállítók pedig a Dassault Systémes – a SolidWorks és a CATIA készítője –, illetve az Autodesk, az AutoCAD fejlesztője.
A gyártás fejlesztési és gyártási fázisainak állandó kihívása, hogy valós időben követhessük a folyamatokat. Itt jönnek képbe a „digitális ikrek”, amelyek egy fizikai tárgy – vagy akár egy egész gyár – virtuális modelljét jelentik. Digitális iker lehet egy konkrét termék virtuális megjelenítése, amely segít a tervezési fázisban, csökkentve a megfelelő kialakításhoz szükséges prototípusok számát. Vagy ez lehet egy gyárban működő felügyeleti rendszer is, hogy a dolgozók mindig tisztában legyenek az összes paraméterrel. Ezen a területen az egyik legizgalmasabb piaci szereplő a NavVis, amely beltéri, térbeli elemzőplatformja segítségével a gyártási terület digitális másolatát készíti el. Az innovatív cég a CB Insights adatai szerint eddig több mint 94 millió dollárnyi befektetéshez jutott hozzá, és olyan nagy cégekkel lépett partnerségre, mint a már említett Autodesk.

A kutatás-fejlesztésre legtöbbet költő cégek

(2020, milliárd dollár)

Amazon	42,7
Alphabet	27,6
Huawei	21,7
Apple	19,5
Samsung	19,4
Microsoft	19,3
Meta	18,5
Volkswagen	17,0
Intel	13,6
Merck	13,6
Roche	13,5
J&J	12,2
Bristol-Myers Squibb	11,1
Pfizer	9,4
Texas Instruments	9,3

FORRÁS: CB INSIGHTS

Új generációs robotok

Az elmúlt évtizedekben számos, emberek által végzett feladatot vettek át a robotok a gyártósorok mellett, az Ipar 4.0 koncepció keretében azonban a robotok alkalmazása és az automatizáció egy egészen új szintje jön el. Az intelligens gyárakban ugyanis a hálózatba kapcsolt berendezések az IoT-technológiát használva kommunikálnak egymással, ami lehetővé teszi a korábbinál sokkal gyorsabb átállást a különböző termékek előállítására, alkalmazkodva ezzel a változó fogyasztói elvárásokhoz is. A CB Insights elemzése szerint a moduláris gyártóberendezések és eszközök segíthetnek a személyre szabott gyártás, az egyedi tömegtermelés elérésében. Ez a koncepció lehetővé teszi, hogy ugyanarról a gyártósorról egymás után különböző modellek kerülhessenek ki, növelve ezzel a termelés rugalmasságát, alkalmazkodóképességét.
Az üzemekben megjelent már a robotok új generációja is, az emberekkel közösen dolgozó, úgynevezett cobot, amelyek könnyen programozható „karjaik” segítségével többféle feladatot is elvégezhetnek. A Universal Robots saját számításai szerint a cég által fejlesztett, könnyen átprogramozható robotkarok alkalmazás átlagosan 195 nap alatt megtérül. A robotok iránti egyre nagyobb igényt mutatja, hogy Észak-Amerikában 2020 harmadik negyedéve és 2021 hasonló időszaka között 32 százalékkal nőtt a megrendelt robotok száma, az Association for Advancing Automation nevű szervezet szerint.
Az új termékek fejlesztésének felgyorsításában, a prototípus elkészítésének megkönnyítésében segíti a termelőcégeket a 3D-s nyomtatás, amelyet az Apple például összekapcsolt a kiterjesztett és virtuális valósággal (AR-rel és VR-rel), hogy még hatékonyabb legyen ez a folyamat. Az AR és VR egyébként a gyártás egyéb területein is jól hasznosítható a CB Insights elemzése szerint, így például a klasszikus betanítást lehet helyettesíteni velük, ami mind a karbantartásnál, mind az új munkatársak betanításánál jól jöhet.

Kalocsai Zoltán

MÁR NEM SCI-FI, VALÓSÁG

Így működnek az okos gyárak Magyarországon

Soha nem látott hatékonyság a raktározás és a gyártás területén, gépi látással támogatott minőségbiztosítás, távolról vezérelt óriásdaruk – az Ipar 4.0 megoldásokra épülő jövő gyára koncepció már nemcsak utópia, hanem valóság. Az alkalmazás kulcsát pedig a felhasználó igényeire szabott, rugalmas és skálázható helyi 5G-hálózatok jelentik, már Magyarországon is.

„Az elmúlt öt évben óriási előrelépésnek lehettünk tanúi, az 5G terjedése sokkal gyorsabb, mint arra a távközlési iparág számított. Mára világszerte 176 kereskedelmi mobilhálózat, 1,5 millió bázisállomás, 500 millió felhasználó, 10 ezernél is több üzleti megoldás és projekt jött létre az ötödik generációs mobiltechnológiával", hangsúlyozta az 5G-technológiában élen járó Huawei Technologies soros elnöke, *Ken Hu.*

Tízszeres sebesség, tízezer üzleti projekt

A végfelhasználói szegmensben az 5G átlagos letöltési sebessége nagyjából tízszer nagyobb a 4G-nél, ami olyan alkalmazások szélesebb körű elterjedését segítette elő, mint a virtuális valóság (VR) és a 360°-os közvetítés. Mindez csak az előnyök egyik fele, hiszen világszerte 10 ezernél is több projekt foglalkozik az 5G üzleti (5GtoB) alkalmazásával. A nagy teljesítményű, vezeték nélküli hálózatok iránti kereslet az intelligens gyártásban folyamatosan növekszik, mivel az 5G kiváló minőségű és rugalmas hálózati képességeket garantál azáltal, hogy integrálja a lánc összes eleméből származó adatokat. Az előrejelzések szerint az 5G okos gyártási piac értéke 2025-re eléri a 232 milliárd dollárt.

A jövő igényeire is gondolni kell

„A Huawei világszerte több mint 100 kutatóközponttal, és partnerekkel, ügyfelekkel közös innovációs laboratóriumokkal is rendelkezik. A vállalat a gyárak vezetőivel és tervezőivel olyan hálózatok kiépítésén dolgozik, amelyek felhasználó-specifikusak, és a jövő-

5G-HÁLÓZATON VEZÉRELT ÓRIÁSDARUK A FÉNYESLITKEI INTERMODÁLIS TERMINÁLON

FORRÁS: MÓRICZ CSABA

ben felmerülő igények szerint is skálázhatók", mondta *Jason Xie,* a Huawei Technologies Magyarország igazgatója. A technológiát már sikeresen tesztelték és alkalmazzák olyan iparágakban, mint a gyártás, a bányászat és a logisztika.
Az intelligens hálózat bárhonnan, bármikor menedzselhető, a kinyert adatok pedig a legkülönfélébb módon vizualizálhatók is, segítve ezzel a döntéshozatalt.
Noha az üzleti 5G-projektek jelentős része jelenleg Kínában koncentrálódik, az ipari csúcstechnológia Magyarországra is megérkezett. A Huawei Technologies Európai Ellátó Központjának pátyi üzemében indult el tavaly hazánk első élő ipari 5G-s hálózata, amelyet továbbiak követtek.

Teljes folyamatok is automatizálhatók

A privát 5G-hálózat kiépítése több lépcsős, egy éves időtartamú beruházást alapozott meg a logisztikai- és gyártóközpontban. A havonta mintegy 60 ezer szállítmányt kezelő pátyi üzemben egy saját maghálózat és egy felhőhöz hasonló, helyi edge-computing rendszer dolgozik össze. Az adatátvitel ennek és az 5G-nek köszönhetően nagyon gyors, a késleltetési idő gyakorlatilag nulla. Önvezető targoncák dolgoznak a logisztikai részlegen, amelyek az 5G-hálózaton keresztül kapcsolódnak a szerverhez. A rájuk szerelt kamerák képét továbbítják egy központi számítógéphez, ami automatikusan kiszámolja és megadja az útjukat, így teljesen automatizált az egész folyamat a beérkezéstől az összeszerelési pontra szállításig.
Szintén az 5G-hálózatra kapcsolódnak a gyártás folyamatosságát biztosító mobil munkaállomások, így nem az anyagot mozgatják a gyárban, hanem a munkaállomás megy helybe elvégezni a feladatot. A mesterséges intelligenciának köszönhetően vizuális képfeldolgozóval felszerelt munkaállomások is segítik a minőségbiztosítást, nagy felbontású kamerákkal készítenek képet az elkészült termékről, hogy kiszűrjék a hibás darabokat. Az üzemben kiterjesztett valóságot (Augmented Reality-t, AR-t) is használnak karbantartásra, oktatásra, magas érzékenységű műveletekre és távoli műszaki segítségnyújtásra. Az AR-szemüveg kamerája továbbítja a képet a mérnököknek, akik tanácsait a szemüveg viselője a beépített kijelzőn követheti nyomon, jelentősen gyorsítva ezzel a folyamatot.

Hatékonyabb folyamatok, kevesebb hiba

„A Pátyon megvalósult fejlesztés kiemelkedő, ténylegesen is működő példája az 5G üzleti felhasználásának az Ipar 4.0 modellben", hangsúlyozza Jason Xie.

A technológiai fejlesztések bevezetése óta jelentősen csökkent a raktári és termelési átfutási idő, a teljesítmény 30 százalékkal, egyes folyamatoknál pedig 40 százalékkal növekedett. Felére csökkent a hibarizikó több terméksoron, javult a munkahelyi ergonómia, és kiemelkedő a munka- és adatbiztonság.

5G-vel vezérelt óriásdaruk

Szintén a Huawei vezeték nélküli 5G megoldásait használják a fényeslitkei East-West Gate (EWG) intermodális vasúti terminálon, amely kontinens legnagyobb kapacitású ilyen létesítménye. A terminálon Európában elsőként telepítettek távolról, 5G-n keresztül vezérelt óriásdarukat. A négy darut egy központból irányítják, amely biztonságosabb és jobb munkafeltételeket biztosít a személyzetnek. Minden darura húsz nagyfelbontású kamerát helyeztek el, amelyek képét az 5G segítségével valós időben látják az operátorok, és késleltetés nélkül tudnak reagálni, éppen úgy, mintha a daruk tetején, egy fülkében ülnének.

5G-HÁLÓZATRA KAPCSOLÓDNAK A HUAWEI PÁTYI LOGISZTIKAI ÉS GYÁRTÓKÖZPONTJÁNAK ÖNVEZETŐ TARGONCÁI

FORRÁS: HUAWEI

Szintén az 5G-hálózaton keresztül, valós időben követik nyomon az összes vasúti kamion, félpótkocsi és konténer, valamint a vasúti szerelvényeken érkező rakomány útját a terminálra való belépéstől a kilépésig. A rendszer nemcsak gyorsítja a be- és kiléptetést, az áruátrakást, hanem a terminálirányítást és a biztonságot is szolgálja.
Az 5G segítségével gyorsabban tudják átrakodni a konténereket, mint a hagyományos terminálok. A hatékonyság növelését és a biztonságot szolgálja a nyomonkövetési rendszer is. Ezzel nem csak a terminál működését támogatják, hanem az ügyfeleink valós időben kaphatnak információt arról, hogyan halad a konténerük átrakása.

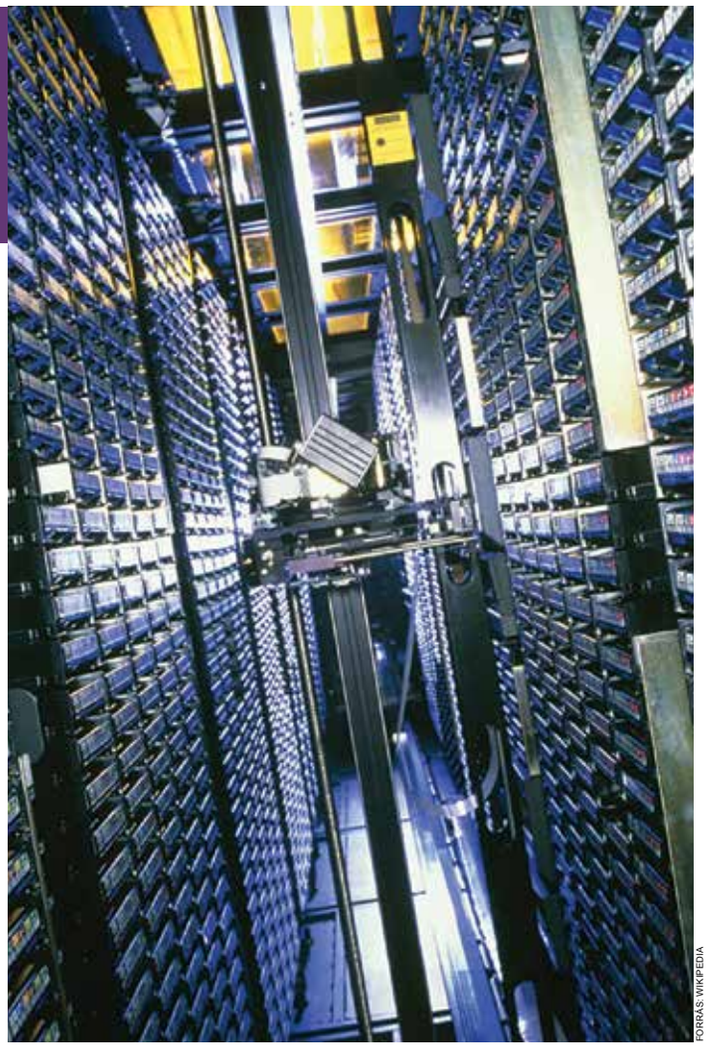
Digitális ikertestvér

Világújdonságként, egy magyar startup közreműködésével felépült az EWG digitális ikertestvére (Digital Twin) is, amely az 5G segítségével valós időben, 3D-ben követi a logisztikai központ folyamatait és működését. A vonatok, kamionok, daruk és szállítójárművek mozgásának és útjának egyszerű ellenőrizhetősége segíti a hatékonyság növelését, a folyamatok optimalizálását és tervezését, mindezt az Ipar 4.0 elvei alapján. Ez a rendszer az operátorok betanítását, képzését is lehetővé teszi, valószerű szimulációval, nem zavarva a terminál működését. ■

A KLASSZIKUS MEGOLDÁSOKRÓL EGYRE TÖBBEN ÁLLNAK ÁT A FELHŐS MÓDSZERRE

Mentő körülmények

A korábban általánosnak mondható szalagos módszerről főleg a kis- és közepes vállalkozások közül egyre többen váltanak át a felhős megoldásra a biztonsági mentések esetében, az átállást a piacon elérhető SaaS-alkalmazások is segítik. Míg az üzleti szektorban széleskörűen elterjedt a biztonsági másolatok készítése, a magánfelhasználók közel harmada még sosem élt ezzel a lehetőséggel.



FORRÁS: WIKIPEDIA

Az emberek 30 százaléka még sosem készített biztonsági mentést adatairól – többek között ezt az információt osztották meg a március 31-i World Backup Day szervezői a nyilvánossággal, hogy felhívják a figyelmet ennek a műveletnek a fontosságára. Ez a magas arány annak fényében még inkább megdöbbentő, hogy világszerte percenként mintegy 113 telefont veszítenek vagy lopnak el, és havonta átlagosan 10-ből 1 számítógép fertőződik meg vírusokkal. Ha pedig nem készült biztonsági mentés, akkor fontos és pótolhatatlan adatok, feljegyzések, emlékek, fotók és videók veszhetnek el örökre csak azért, mert nem szántunk korábban egy kis időt erre a feladatra.
Az egyéni felhasználók esetében egyszerűbb a helyzet, hiszen kevesebb fontos adattal rendelkeznek, mint a cégek, és ezeket általában jól strukturált módon, automatizáltan mentik a készülékeik. Ráadásul egyszerűen használható biztonsági mentési megoldásokat kínálnak számukra mind az okostelefonok, tabletek és számítógépek gyártói, mind a legnagyobb online szolgáltatásokat biztosító cégek.
A vállalatok esetében már bonyolultabb a helyzet, hiszen a cégek sokkal több adatot hoznak létre, tárolnak és használnak. Ráadásul napjaink gyorsan digitalizálódó világában az adatok elengedhetetlenek a szervezetek mindennapi működéséhez, és nem csupán eszmei veszteséget jelent az elvesztésük. Tovább nehezíti a feladatot, hogy az adatok szétszórtan helyezkednek el a vállalati infrastruktúrában, például az alkalmazottak számítógépein, a céges szervereken és a felhőben, ezeken belül is különféle alkalmazásokban és adatbázisokban – írja elemzésében a Micro Focus.

Gyors fejlődés

A felhőbe történő mentés a következő időszakban viszonylag gyorsan fejlődik majd az előrejelzések szerint. A Global Industry Analysts elemzése szerint míg 2020-ban még csak kétmilliárd dolláros volt ez a szegmens, addig 2027-re már 8,4 milliárd dolláros üzletet jelent majd a biztonsági mentések felhőben tárolása. Ez azt jelenti, hogy évente átlagosan 22,9 százalékos bővülés várható a piacon. A nagyvállalatok körében évente átlagosan közel 20 százalékkal bővül majd az erre a célra szánt összeg, így 2027-re már 4,3 milliárd dollárt fordítanak felhős mentésre.

Átmeneti időszak

„A nagyvállalatoknál már nem számít újdonságnak, hogy rendelkeznek részletes tervvel katasztrófahelyzetekre, illetve az üzletmenet helyreállítására és ezt auditálják és tesztelik is, aminek természetesen része az is, hogy biztonsági mentést készítenek a fontos adatállományokról. Ezt eddig is komolyan vették és ezután is így tesznek majd. Változás inkább abban látszik, hogy míg korábban erre a célra elsősorban szalagos mentési megoldást használtak, addig most már egyre gyakrabban próbálják adatközpontban, vagy felhőben megoldani a mentést. Jelenleg átmeneti időszakot élünk, amikor már érződik az új trend, de még akadnak vállalkozások, amelyek vagy a jogszabályi környezet, vagy egyéb okok miatt nem tudják meglépni ezt a váltást”, számolt be a helyzetről *Erdősi Gilbert,* a papíralapú és digitális dokumentumkezeléssel foglalkozó Iron Mountain digitális portfólió menedzsere.
A szakember szerint egyébként egyre gyorsabb lesz majd az átállás az adatközpontban tárolt biztonsági mentésekre, amit a szolgáltatók fejlesztései is támogatnak. Az Iron Mountain például 2017 óta több mint

kétmilliárd dollárt fektetett be az adatközponti üzletága fejlesztésébe, összesen 19 helyszínen van ilyen létesítményük, közülük három Európában található.

Speciális igények

„A biztonsági mentések kapcsán a szalagos megoldás előnye, hogy mivel nem egy adatközpontban lévő szerveren tárolják az információkat, hanem offline adathordozókon, így nem áll fenn annak veszélye, hogy egy hackertámadásban illetéktelenek férhetnek hozzá az adatokhoz. A szalagos mentés azonban egyszeri beruházást és folyamatos erőfeszítést is igényel a cégektől. Egyrészt rendelkezni kell azokkal az eszközökkel, amelyekkel a vállalati informatikai rendszerekből az adatbázisokat ki tudják menteni a szalagos adathordozókra. Odafigyelést igényel az is, hogy ez rendszeresen

Jelenleg átmeneti időszakot élünk, amikor már érződik az új trend

megtörténjen és az adott időpontban rendelkezésre álljanak a szükséges eszközök. Mivel a katasztrófahelyzetekre vonatkozó akciótervekben fontos szerepet játszik a földrajzi redundancia, a kazetták tárolását külső helyszínen kell megoldani. Ehhez pedig meg kell tervezni a szállítást, előre kell gondolkozni az adott helyszín fizikai tárolási kapacitása kapcsán. Vagyis összességében ez egy lényegében naponta jelentkező logisztikai feladatot jelent a vállalkozások számára. Mi is nyújtunk ilyen szolgáltatást, speciális helyiségben tároljuk a szalagos adathordozókat, ahol állandó a hőmérséklet és a páratartalom, tűz esetén pedig gázzal oltunk, hogy az oltóanyag ne tegye tönkre a szalagokat. A kazetták mozgatását pedig speciális járművel végezzük, amely szintén képes biztosítani az állandó hőmérsékletet”, mondta el Erdősi Gilbert.

FORRÁS: IRON MOUNTAIN

ERDŐSI GILBERT, IRON MOUNTAIN

Az adatközpontba történő biztonsági mentés nagy előnye, hogy nem igényel eszközberuházásokat, illetve jól felügyelhetően automatizálható a biztonsági mentési folyamat kialakítása. Emellett ebben az esetben jól skálázható a szolgáltatás, vagyis annyit kell fizetniük a vállalkozásoknak, amennyi tárhelyet aktuálisan használnak, nem kell előre nagyobb tárolási kapacitással felkészülniük. Az Iron Mountain digitális portfólió menedzsere szerint napjainkra a 250 főt, vagy annál kevesebbet foglalkoztató vállalkozások túlnyomó többsége már szinte teljesen átállt a felhős, adatközponti biztonsági mentésre. A váltást segíti az ő esetükben, hogy rendelkezésre állnak olyan SaaS-megoldások, amelyek keretében a biztonsági mentést szolgáltatásként tudják igénybe venni.

Kalocsai Zoltán

UGYANAZOK AZ ALAPELVEK

Nem ördöngösség a felhőbiztonság

Sok minden miatt tartanak a felhőhasználattól a vállalati vezetők, és az aggodalmak listáján előkelő helyet foglalnak el a biztonsággal kapcsolatos kételyek. Pedig a felhő nem kevésbé biztonságos, mint a saját infrastruktúra – amennyiben betartunk néhány alapelvet.

Akár a felhőben, akár saját adatközpontjában működteti rendszereit és tárolja adatait a vállalat, mindkét helyen nagyjából ugyanazokkal a veszélyforrásokkal találkozhat, ugyanazoknak a kockázatoknak van kitéve. Ennek megfelelően a védekezés módszerei is többé-kevésbé hasonlóak. „Ám a különbségek mégis vannak akkorák, hogy érdemes legyen beszélni róluk”, mondja *Nagy Zoltán,* a Magyar Telekom csoport biztonsági igazgatója.

A több nem feltétlenül jobb

Az alapelv az, hogy a felhőben mindazok a veszélyek fellelhetőek, amelyek az on-premise környezetet fenyegetik. A felhasználók ki vannak téve a phishing-támadásoknak, érkeznek a zsarolóvírusok, kihasználhatják a hackerek a nulladik napi sérülékenységeket, és érhetik túlterheléses támadások az infrastruktúrát. Ugyanakkor az adatközponti infrastruktúrában használt biztonsági megoldásoknak is megtalálhatók a felhős megfelelői.
A felhőbiztonság megteremtésében legalább olyan fontos a megfontolt tervezés és a stratégiai gondolkodás, mint a felhőbe átvinni kívánt szolgáltatások és adatok körét határozza meg a vállalat, hangsúlyozza az igazgató. A felhőbe vezető útnak, vagyis a „cloud journey”-nek része kell legyen az is, amikor a védekezés célját, eszközeit és módszereit határozza meg a vezetés.

NAGY ZOLTÁN, A MAGYAR TELEKOM CSOPORT BIZTONSÁGI IGAZGATÓJA

FORRÁS: T-SYSTEMS

„Nagyon könnyű menet közben elcsábulni. Bármit könnyedén össze lehet kattintgatni, megveheti magának a cég a szerveroldali védelmet, a végpont-oldali védelmet, mindent, ami szem-szájnak ingere. Viszont csak részben igaz, hogy a több rendszer egyben nagyobb védelmet is jelent. Bizonyos komponensek akár akadályozhatják is egymás működését, és gondolni kell arra is, hogy a rendszerekből származó logokat elemezni, értelmezni is kell, mint ahogy az incidensekre adott válaszokat is előre meg kell tervezni, majd szükség esetén végre kell hajtani. Végtelen mennyiségű pénzt el lehet költeni, pedig igazából a kockázattal arányos védelemre lenne szükség", hívja fel a figyelmet a különbségre Nagy Zoltán.

Ellenőrzött hozzáférés

Az egyik nagy különbség a felhőinfrastruktúra és a saját adatközpont védelme között az elérési csatorna biztosítása, mind IT-biztonsági, mind üzletmenet-folytonossági szempontból. „Amikor a dolgozók az irodában ülnek, az adatközpont a székházban van, a másodlagos helyszínnel pedig dupla optikai szál köti össze, az állandó kapcsolat garantáltnak tekinthető. Amikor a munkatársak távolról jelentkeznek be, és külföldi szolgáltatókkal kell állandó kapcsolatot létesíteni, ez már mindenképpen extra feladatot jelent", mondja Nagy Zoltán.

Ugyancsak fokozott figyelmet kell fordítani a felhasználók jogosultságainak kezelésére. Hagyományos irodai környezetben is lényeges, hogy milyen erős azonosítás után érik el a rendszereket a dolgozók, de a felhő esetében ez kulcsfontosságúnak számít. Az egyszerű felhasználónév-jelszó páros ma már nem számít elégséges védelemnek – túl sok olyan támadási forma van már, amely ezt ki tudja aknázni. Kellő biztonságot a kétfaktoros autentikáció tud adni, a dolgozói jogosultságok részletes és naprakész kezelésével.

Legalább ilyen fontos a dolgozói eszközök védelme. Valóban rendkívül kényelmes, hogy a laptopról vagy akár a mobilról bárhonnan, bármikor el lehet érni a munkához szükséges rendszereket, funkciókat, adatokat. A laptopot vagy a mobilt azonban el is lehet veszíteni vagy el lehet lopni, márpedig, ha a rajta tárolt adatok nem eléggé védettek, vagy rajta keresztül kontroll nélkül hozzá lehet férni a felhőszolgáltatásokhoz, máris kész a baj.

Feladatok és felelősségek

Hacsak a vállalat nem maga intéz mindent, a felhős rendszerek működtetésében három szereplő vesz részt: maga az ügyfél; az infrastruktúrát, a platformot vagy az alkalmazást kínáló felhőszolgáltató; és kettejük között az a partner, amelyik mutatja az irányt a felhőbe vezető úton.

A feladatok és felelősségi körök tisztázása a három fél között rendkívül lényeges, különösen a biztonság kapcsán, emlékeztet Nagy Zoltán.

A felhőszolgáltató elsődleges kötelessége, hogy stabil, megbízható, állandó és biztonságos környezetet biztosítson. Az ügyfélnek fel kell ismernie, hogy folyamatosan fenyegetik a veszélyek, még akkor is, ha közepes magyar cégről van szó: mindenki adatai érdekesek és értékesek a kiberbűnözők számára. Ezért az ügyfél dolga, hogy meghatározza a védendő adatok körét, azok értékét az üzlet számára.

A T-Systemshez hasonló partnerek pedig abban tudnak segíteni, hogy megteremtsék az összhangot az ügyfél igényei és a szolgáltató kínálta lehetőségek között. A rendszerek, az igények és a kockázatok felmérése után tanácsot tudnak adni a védekezés optimális módjait illetően, és az üzemeltetés során is figyelhetik az eseményeket és időben reagálhatnak a támadásokra. Természetesen ez némi költséggel jár, de az esetek túlnyomó többségében megéri, hiszen a tanácsadónak kifizetett díj még mindig alacsonyabb, mint amibe a feleslegesen megrendelt szolgáltatok kerülnének.

A hibrid felhő sok tekintetben biztonságosabb és üzembiztosabb tud lenni, mint akár a saját adatközpont, akár a tisztán felhős környezet

Előny a hibrid felhőnél

A felhő, és különösen a hibrid felhő sok tekintetben biztonságosabb és üzembiztosabb tud lenni, mint akár a saját adatközpont, akár a tisztán felhős környezet, teszi hozzá Nagy Zoltán. A szolgáltatók minden erőfeszítése dacára előfordulhat, hogy egyes felhőkörnyezetek vagy -szolgáltatások időlegesen lehalnak. Ilyenkor hiába biztosított az elérés, ha maga a szolgáltatás nem működik. A fordítottját – vagyis amikor a szolgáltatás működik, csak az elérés akadozik – már könnyebb kivédeni. Nincs szükség nemzetközi vonalakra, ha a szolgáltatás hazai felhőközpontokból is elérhető, ahonnan ugyanazokat a funkciókat megkapja az ügyfél (gyorsabban és üzembiztosabban), mint a globális központokból. „Különösen hasznos, ha a felhős infrastruktúrát biztosító cég mögött egy távközlési szolgáltató is áll, mint ahogy ez a T-Systems esetében működik", említ egy további szempontot Nagy Zoltán. Nemcsak a felhőközpontok elérése biztosabb így, de az internetes kapcsolatokat megbénító szolgáltatásmegtagadási (DDoS-) támadások kivédése is könnyebben megy.

A biztonságot növeli a felhőszolgáltatók méretéből fakadó előnye is. Egy Amazon vagy Google biztonsági kitettsége ugyan sokszorosa egy magyar vállalatának, ám a védelemre fordítható erőforrások és szakértelem dolgában is messze felülmúlják a többi céget. Egy nulladik napi támadás ugyanúgy megtalálhat felhőszolgáltatót, mint a saját infrastruktúrát üzemeltető magyar vállalkozást, ám az előbbi hamarabb észreveszi és reagál, illetve az érintett szoftver fejlesztőjétől is valószínűleg hamarabb kap segítséget.

Üzemeltetni is egyszerűbb

Összességében, ha a vállalat a biztonságtudatosság kellően magas fokán állt, azaz a saját infrastruktúrájában is odafigyelt a hozzáférések és jogosultságok kezelésére, tudják, hogy milyen adatokat és milyen veszélyek ellen kell védeni, a felhővel nem vesz plusz kockázatokat a nyakába. Éppen ellenkezőleg, az üzemeltetés szempontjából még könnyebb is lesz a dolga, teszi még hozzá Nagy Zoltán. „A felhőben a szolgáltató számos feladatot magára vállal, egyszerűbb, automatizált lesz a szoftverek frissítése, a hibajavítások menedzselése. A drága élőmunka kiváltásával nemcsak a biztonsági szint lesz magasabb, hanem attól sem kell félni, hogy az üzemeltetési szakemberek egyik napról a másikra odébbállnak", mondja. ■

„ÚJRATERVEZÉS…"

Hogyan kövessük a gyors változásokat az IT-költségvetéssel?

FORRÁS: DEUSCHE TELEKOM

A Covid, majd a mostani időkre is hatással lévő chiphiány és legújabban a háborús helyzet miatt gyökeresen megváltoznak az üzleti élet körülményei, aminek következtében az IT-szervezeteknek is folyamatosan reagálniuk kell a változásokra. Az IT-menedzsment legérzékenyebb pontja az IT-költségvetés, amelyet rendkívüli időkben rendkívüli gyakorisággal és olykor rendkívüli mértékben szükséges felülírni.

Recover, Redesign, Restart – a Covid globális szinten mindenre jelentős hatást gyakorolt, mindezek közül talán a legjelentősebb az a pénzügyi átalakulás, amelyen az IT-költségvetés ment keresztül. Az alaposan megtervezett büdzséket az elmúlt időszakban a digitális átalakulás, és az informatikai ökoszisztéma modernizációja, a távmunkára való átállás, a digitális ellátási lánc menedzsmentje, az üzletfolytonosságot távolról fenntartó eszközök, szoftverek és megoldások beszerzése, integrálása, kialakítása mind-mind átírta. Így a mai napig tartó technológiai gyorsulás és digitális transzformáció mellett az IT elmúlt két évét az átalakuló prioritások a költségvetésen hagyott lenyomata jellemezte.

Költség az egekben

Rendkívüli időkben rendkívüli gyakorisággal és olykor rendkívüli mértékben szükséges felülírni mindazt, amit a vállalat előzetesen eltervezett, ami jelen esetben a globális szinten is rekord magasra nőtt felhőmigráció képében öltött testet.
A Hewlett Packard Enterprise 2020 augusztusában készített tanulmánya szerint a Covid-19 markáns „mellékhatása" a felhős megoldások igénybevételének növekedése volt. A Synergy Research Group kutatása szerint 2021-ben összesen 178 milliárd dollárt költöttek felhőszolgáltatásokra a cégek, ami 37 százalékos növekedés a 2020-ban elköltött 130 milliárd dollárhoz képest, és kétszerese annak, amit a vállalatok ehhez mérten az adatközpontjaikra költenek.
A cloud és az általa elérhető, IaaS-, PaaS-, SaaS-szolgáltatások növekedése mögött értelemszerűen a lezárásokra válaszul megerősödött távmunka állt. Azonban, ami két éve még kényszermegoldásnak tűnt, mára az új generációs munkavégzés formájaként megszilárdult, ezért kétségtelen, hogy az IT-kiadások jelentős része a cloudra és a távoli, hibrid munkavégzés folyamatát támogató eszközökre, szoftverekre, megoldásokra és a kiberbiztonságra összpontosul a jövőben is.
A Deloitte Global azt jósolja, hogy felhős szolgáltatást kínáló cégek bevételnövekedése a 2021-től 2025-ig tartó időszakban is 30 százalék fölött lesz, mivel a vállalkozások a felhőre töltik át/fel adataikat, hogy spóroljanak, agilisabbá váljanak, és ösztönözzék az innovációt. Ezért a piacot várhatóan minden eddiginél erősebbé teszi a pandémia.

A költségvetés-készítés gyakorlata is reziliensebbé vált

A meglóduló IT-költségvetés markáns része a felhő és a kollaboráció, illetve kiberbiztonsági megoldások beszerzésének, integrálásának és – adott esetben- üzemeltetésének számlájára írható, ugyanakkor egyéb, a következő időszakra át nem tolható költségek is felmerülnek, amire különböző cégek, különböző módon reagálnak itthon is.

Az előző évek tanulságait mindig felhasználjuk a következő év költségvetésének tervezésekor

HAZSLINSZKY ÁKOS, BUDAI EGÉSZSÉGKÖZPONT

FORRÁS: ITBUSINESS

Hazslinszky Ákos, a Budai Egészségközpont informatikai igazgatója arra a kérdésre, hogy hogyan változott az utóbbi időkben az IT-költségvetés-készítés és -frissítés gyakorlata, válaszát az előző évek tanulságaival kezdte. „Az előző évek tanulságait mindig felhasználjuk a következő év költségvetés-tervezésekor. Például ilyen a hibrid munkavégzés tartós támogatása vagy a szezonális változások egyre bonyolultabb modellje. Fel kellett készülnünk arra is, hogy szükség esetén rövid időn belül a költségvetés átrendezésével le tudjunk követni akár jelentős változásokat is. Ehhez az igények és a prioritások pontos ismerete elengedhetetlen."
Az IT-költségvetéskészítés és -követés gyakorlata a Ceva-Phylaxia esetében is erősen megváltozott „a globális chiphiány okozta ellátásilánc-problémák miatt, mivel a szállítási idők jelentősen megnőttek. Eddig a következő évre terveztük a költségvetést a további

évek igényeinek figyelembevételével. Mivel sajnos az informatikai eszközök szállítása akár egy éves határidővel történik, a költségekkel kettő évre előre kell tervezni. Sajnos, az árak is dinamikusan változnak, ezért fel kell készülnünk arra is, hogy év közben kell módosítanunk a költségvetést", válaszolta meg kérdésünket *Dinnyér Krisztián,* a Ceva-Phylaxia platform IT-managere.

Az IT-költségvetés prioritásai és az újratervezés gyakorisága

Az elmúlt két évben nem volt egyszerű a pénzügyért felelős vállalati vezetők élete. Először a pandémia, majd a fokozódó félvezető és chiphiány, majd a globális hiánygazdaság, most pedig a háború kényszeríti ki a folytonos gazdasági újratervezést.

„Hivatalosan negyedévente vizsgáljuk felül a költségvetés alakulását, de folyamatos a belső költségkontroll. Minden új igénylésnél mérlegeljük, hogy az

FORRÁS: 123RF.COM

DINNYÉR KRISZTIÁN, CEVA-PHYLAXIA

FORRÁS: CEVA-PHYLAXIA

mennyire időszerű és megalapozott, valamint belefér-e a tervezett költségkeretbe. Ha nem a tervezett ütemben változik egy-egy költségnem, vagy ha jelentős, nem tervezett, de indokolt költség merül fel, akkor elsősorban belső költség átstrukturálást végzünk", avatott be a céges költségvetés újratervezésének gyakoriságába Hazslinszky Ákos.

Ami a vállalati prioritásokat illeti, hozzátette: „vannak tisztán IT-érintettségű tervezett költségek, ezek jellemzően a kiszolgáló erőforrásokhoz vagy azok üzemeltetéséhez kapcsolódnak. Ezen kívül a korábban megkezdett digitalizációs projektek folytatásaként további jelentős fejlesztések költségeivel is számolni kell. Végezetül az idén induló új kórházépület építéséhez kapcsolódó rövid- és hosszútávú IT-feladatok költségét is prioritásként kezeljük."

Dinnyér Krisztián az IT-költségvetés újratervezése kapcsán a havi szintű átvizsgálást tartja szükségesnek. „A megnövekedett szállítási idők és a dinamikusan változó árak miatt több beszállító már nem tud árgaranciát biztosítani a megrendelésekre, ezért havi szinten követjük a költségvetés alakulását. Drasztikus növekedés esetén újra kell terveznünk a költségeket", mondta.

A legfontosabb prioritás az üzleti folytonosság fenntartása és az eszközök életciklusának követése

5 érdekesség a felhőről

– A nyilvános felhőszolgáltatás piaca 2023-ra várhatóan eléri a 623,3 milliárd dollárt világszerte.
– Az összes IT-költségvetés 30 százaléka a számítási felhőre irányul.
– Az amerikai vállalkozások 66 százaléka már rendelkezik központi felhőcsapattal vagy felhőalapú kiválósági központtal.
– Egy átlagos szervezet egyidejűleg 4-5 különböző felhőplatformot használ.
– 2025-re a felhőalapú adatközpontokban tárolt adatok száma meghaladja a 100 zettabájtot.

FORRÁS: WEBTRIBUNAL.NET

„A legfontosabb prioritás az üzleti folytonosság fenntartása és az eszközök életciklusának követése. E mellett a cég dinamikus növekedésben van, ami létszámbővüléssel is együtt jár. Fontos, hogy ezt a pozitív változást IT-szempontból is le tudjuk követni. Természetesen a költségek alakulása is nagyon fontos”, egészítette ki Dinnyér Krisztián.
Persze az sem mindegy, hogy az IT-költségvetést elkészítő csapatban kik vannak az IT-szervezeten kívüli társosztályoktól, hiszen csak akkor lehet mindenki számára optimális a végeredmény, ha minden társosztály kooperál a folyamatban.
„A 2022-es költségvetést a Gazdasági Osztállyal együtt készítettük. A nagy, teljes vállalatot átfogó, IT-érintettségű projektek miatt, azonban szükségessé vált, a társosztályok bevonása is a költségvetés elkészítésébe. Várhatóan az idei évben, a következő IT-költségvetés elkészítésében a Gazdasági Osztály mellett a legnagyobb belső megrendelő társosztályok is aktívan részt fognak venni, elsősorban a közös fejlesztési feladatok meghatározása, koordinálása és azok várható költségeinek megtervezése miatt”, mondta Hazslinszky Ákos.
Dinnyér Krisztián pedig arról számolt be, hogy az IT-költségvetés elkészítésében az Informatikai Osztály dolgozóin kívül részt vesznek a Beszerzési Osztály kollégái, de segítséget kapnak a Pénzügyi Igazgatóságtól is.

A hagyományos reziliencia már nem elég

A Covid még 2022-ben is világszerte hatással van az üzleti folyamatokra és a befektetésekre is. Az erősen globalizálódott üzleti környezet összekapcsolt jellege miatt nagyobb a kockázat, a kitettség, így a cégek pénzügyi és piaci stabilitásához már nem elegendő, ha a megszokott krízisforgatókönyvtől várják a megoldást.
A válságállósághoz elengedhetetlen a reziliens gondolkodás, amelynek a stratégiában is manifesztálódnia kell. Talán soha nem volt olyan fontos megtalálni az egyensúlyt az IT-költségek és a többi terület ráfordításai között. Az viszont nyilvánvaló, hogy a gyorsan digitalizálódó információs társadalomban az IT-költés biztos befektetés a jövőbe.

Kiss Franciska

Minden korábbinál könnyebb dolga lett a HR-nek a Telekomnál

FORRÁS: MAGYAR TELEKOM

A Magyar Telekom karrieroldalának megújítása nemcsak a munkavállalói jelentkezéseket gyorsította fel, de a HR működését és a jelöltek kényelmét is új szintre emelte. Ennek eléréséért a legnagyobb hazai telekommunikációs cég a ShiwaForce csapatának szakértelmét hívta segítségül.

Az adminisztratív útvesztők helyett a valódi feladatra és az emberekre koncentrálhatnak az új Karrier portál és jelöltkezelő rendszer (applicant tracking system, ATS) bevezetését követően.
A Telekom Magyarországon több mint 5000 embert foglalkoztat és évente átlagosan 350-380 főt vesz fel 600-650 meghirdetett pozícióra. A karrieroldalon átlagosan 50-60 elérhető állás közül válogathatnak az érdeklődők.
„Amit karrieroldalnak nevezünk, az korábban is megvolt, de mellette futott még egy ebből következő, konkrét állásokat tartalmazó »job portálunk«, illetve az ATS. Tehát három különböző rendszert használtunk, ami felhasználói és adminisztrátori szempontból is nagyon körülményes volt”, mondja *Dorogházi Enikő,* a Telekom szenior HR-menedzsere.

A három felületet kettőre kellett redukálni: a karrieroldalon belépőket egy új, komfortosabb ATS-re irányítva. A Magyar Telekom az agilis IT-megoldásokban utazó ShiwaForce-ot bízta meg az összetett feladattal.
Az új ATS a Prescreen megoldása lett, a ShiwaForce a beszállító segítségével épített ki testreszabott interfészt és felhasználói rendszert, mindezt a Telekom igényeinek megfelelően. A projekt 2020 novemberében indult, és fél évvel később, júniusban a Telekom már át is vehette az új rendszert.
A ShiwaForce működési módszerei lehetővé tették, hogy az ügyfélvisszajelzéseket folyamatosan építsék be a karrieroldalba és az ATS-be.
Kíváncsi vagy, mik voltak az akadályok, és hogy végül hogyan valósult meg a projekt? Olvasd le a QR-kódot! ■

VAN MUNKAERŐ, CSAK FEL IS KELL VENNI

Hogyan vegyél fel egy év alatt 60 embert?

Létező probléma a munkaerő-hiány a magyar informatikai piacon, de ha valaki tényleg akarja, fordít rá energiát és erőforrást, és mindezt még kidolgozott folyamatokkal is megtámogatja, akkor képes lesz új munkaerőt találni vállalkozásába.

EGERSZEGI KRISZTIÁN, MINICRM

FORRÁS: MINICRM

„A probléma, mint oly sok esetben, a múltban és a fejekben gyökerezik”, állítja határozottan *Egerszegi Krisztián,* a MiniCRM cégvezetője. Számtalan hazai kkv-t olyanok alapítottak, akik a saját szakmájukhoz jól értenek, de a cégvezetés adminisztratív ügyeivel, és különösen a toborzással nem szívesen foglalkoznak. Így viszont nem bővül a csapat, megreked a vállalkozás, a szervezet pedig nem lesz képes kiszolgálni a cég növekedését.

Megoldódnának a problémák, ha a munkaerő toborzásával és megtartásával kapcsolatos feladatokat jól definiált folyamatokba rendszerezve végeznék. Egerszegi Krisztiánék nem meglepő módon a MiniCRM HR-modulját használják erre a célra. A hatékonyság kulcsa, hogy a dolgozó teljes életciklusát egyetlen rendszerben és folyamatként kezelik. „A folyamat minden egyes lépéséhez, a státusz minden egyes változásához hozzárendeltük a feladatokat, amelyek egy jó részét a rendszer automatikusan végzi el”, mondja erről a cégvezető.

Lépésről lépésre

Hogyan néz ki ez a gyakorlatban? Az előszűrőn kiesett jelentkezőknek automatikusan megy az udvarias elutasító levél – sokat javít a cég imázsán, hogy egyáltalán válaszra méltatja az elutasított jelölteket. A többieknek a rendszer szintén automatikusan kiküldi az előre elkészített tesztfeladatot, a szükséges információkkal, például a határidővel.

A tesztet sikeresen kitöltőket először a HR-esek interjúztatják (előre megírt kérdéssor segít, hogy semmiről ne feledkezzenek el), majd a következő lépcsőfokon a szakmai interjú jön. Az utolsó akadály az úgynevezett „team fit” interjú, amikor leendő munkatársaival ismerkedik meg a jelölt. Ha ezt is sikerrel vette a jelölt, az ajánlatok automatikusan generálódnak a MiniCRM-ből, mint ahogy a belépésnél szükséges dokumentumokat sem kell manuálisan megírni és kitölteni. Ráadásul a belépéssel és az onboardinggal kapcsolatos különféle feladatokat is a rendszer osztja ki az illetékes kollégáknak, így egyetlen részlet sem marad ki.

Mérhető, így javítható

A folyamat ráadásul mérhető is. Ez a HR-nek is érdeke, hívja fel a figyelmet Egerszegi Krisztián, mert így kiderülhet, hogy tényleg túl sok a munkája, és több erőforrásra lenne szüksége.

Ugyanakkor a mérés biztosítja azt is, hogy a folyamatok az elvárt (és előírt) ütemben haladjanak. Ilyen elvárás például, hogy a minősített jelentkezőknek három napon belül jelezzenek vissza – 100 jelentkező esetében ez nem is annyira triviális. Egy másik KPI szerint 21 napon belül ajánlatot kell adni az arra érdemes jelentkezőnek. Ennyi idő alatt lezajlanak a különféle interjúk, pedig lehet, hogy hat ember is dolgozott azon, hogy idáig eljusson a folyamat.

„Jelenleg 17 nap alatt van ez a mérőszámunk. Ha egy másik cég ennyi idő alatt a telefonos interjúig sem jut el, akkor nagy hátrányban van a munkaerőpiacon. Mi is a rendszerünknek és a folyamatainknak köszönhetően tudtunk az elmúlt 1 évben két országban összesen 60 embert felvenni”, teszi hozzá az ügyvezető igazgató. ■

Megtartani is könnyebb

A rendszerezett folyamatok, az előre gondolkodás a dolgozók megtartásában is segít. A MiniCRM-nél az új belépőkkel kitöltetnek egy kérdőívet (kedvenc zenéi, ételei, hobbijai). Amikor közeleg az egy éves évfordulója, a HR-es kolléga automatikusan kap egy feladatot a rendszerből, hogy a megadott információk alapján készüljön valami meglepetéssel. A hároméves évfordulónál pedig valami komolyabb ajándékkal kedveskedünk. „Ez igazából nem kerül semmibe, de a dolgozó érzi, hogy figyelünk rá, fontos nekünk”, mondja Egerszegi Krisztián.

A FEHÉR CÍMKE ELŐNYEI

Megéri egyedileg fejleszteni, vagy válasszunk inkább dobozos szoftvereket?

SZÉLL SZILÁRD, GRAPE SOLUTIONS

FORRÁS: ITBUSINESS

Sokszor nem egyértelmű a vállalkozások számára sem, hogy üzleti folyamataik ellátásához piackész megoldást válasszanak, vagy szoftvertervezők és -fejlesztők segítségével nulláról kezdjék el a szoftver kialakítását. A dobozos szoftverek kérdéskörét jártuk körbe *Széll Szilárddal*, a Grape Solutions vezérigazgatójával.

Az utóbbi évek gyors infrastruktúrafejlődése, a digitalizáció mind hozzájárult ahhoz, hogy a vállalatok azonnal kézbe vehető SaaS-szoftvereket keresnek, amelyeket majd saját márkajelzésük alatt tudnak felhasználóik számára elérhetővé tenni. A dobozos szolgáltatások jobb áron biztosítanak kiváló minőségű termékeket, szemben az egyedi szoftverfejlesztéssel, ahol a fejlesztés költsége mellett a fejlesztési idő is kockázat a vállalkozások számára. A „white label" termékek eladásra, használatra készek, részletekbe menően tesztelt és ellenőrzött megoldások, így nagyobb biztonságot jelentenek a vállalatok számára.

Öt év múlva szinte csak felhős szoftverek lesznek

„Nemzetközi viszonylatban azt látjuk, hogy a vevők keresik azokat a megoldásokat, amelyek kulcsrakész szolgáltatással, akár azonnal elérhetőek a vállalat számára, így jelentős pénzt és időt spórolhatnak meg a tervezéstől a bevezetésig tartó folyamatban. Ez a zöld, fenntartható megoldásokra hatványozottan igaz. A hazai szoftverfejlesztési piacon azt tapasztaljuk, hogy partnereink inkább az ún. »hibrid« megoldásokat keresik, tehát igénylik a vállalat sajátosságaira jellemző funkciók beépítését is. Természetesen vannak esetek, amikor a vevői igény annyira speciális, hogy azt csak egyedi szoftverfejlesztéssel lehet megfelelően kielégíteni, ebben szintén segítséget tudunk számukra nyújtani, hiszen az elmúlt 15 évben megannyi partnerünk problémájára sikerült közösen megoldást találnunk", magyarázza Széll Szilárd, a Grape Solutions vezérigazgatója.

A Grand View Research felmérései szerint a szoftverfejlesztési piac 733 milliárd dollárra bővülhet 2028-ra, leginkább a rohamosan fejlődő banki, pénzügyi, telekommunikációs, egészségügyi és gyógyszeripari szektorok miatt. A kutatás arra is rávilágít, hogy bár a cloud és on-premise üzemeltetés jelenleg fej-fej mellett halad, 2028-ra a felhő szolgáltatás lesz egyeduralkodó globális viszonylatban. Ez a szoftverfejlesztő vállalatok számára is irányt mutat, merre érdemes a jövő dobozos termékeit fejleszteni.

„Nincs egyszerű helyzetben sem egy innovatív startup, sem pedig egy innovációra nyitott nagyvállalat, amikor új, vagy továbbfejlesztett terméket kíván bevezetni a piacon. Mindkét szereplő a felhasználó problémája mentén közelíti meg a kérdést: »Vajon mire van szüksége?«, ezen a ponton csatlakozik be a piackutatás fontossága. Időt és pénzt sem sajnálva dolgozunk azon, hogy jobban megértsük partnereink és felhasználóik igényeit, legyen szó akár elektromos jármű töltéséről, akár általános projektmenedzsmentről. Kutatásaink mentén jön létre az a funkciólista, amelynek integrálásával egyedibbé tehetik partnereink még a dobozos megoldásokat is", fejtette ki Széll Szilárd.

Tapasztalat és támogatás is van a dobozban

A white label megoldások esetében olyan termékekről van szó, amelyek más partnerek, fejlesztői teamek által már kipróbált, tesztelt szoftverek, tehát kisebb kockázatot jelentenek új tulajdonosaik számára. Ráadásul nem egyszeri beruházásként, CAPEX-ből kell előteremteni a termék finanszírozását, hanem rendszeres licencdíj ellenében, OPEX-ből is megoldható.

„A szoftverek bevezetése után sem elhanyagolható a support tevékenység, legyen szó akár folyamatos szolgáltatásnyújtásról, vagy későbbi funkciók beépítéséről", tette hozzá Széll Szilárd.

A Grape Solutions számos iparág részére nyújt kulcsrakész szoftvert, például az elektromosjármű-töltő szolgáltatók, az energiaközösségek, a marketing kommunikációs csapatok vagy az okos eszközeiket IoT-felületen menedzselni kívánó vállalkozások számára. ■

A HACKER NEM VÁLOGAT: MINDENKI CÉLKERESZTBEN VAN

Kockázatelemzés kockázatos időkben

A kiberbiztonságiak alapvető törekvése, hogy a várható fenyegetettségek kezelésére készítsék fel az általuk felügyelt informatikai rendszereket. Minden efféle védelem megtervezése a várható kockázatok felmérésével és elemzésével kezdődik.

A nemkívánatos események bekövetkezési valószínűségeinek feltárására hivatott a kockázatelemzés, a kockázatértékelés. Nemcsak a vállalati stratégiaalkotásban játszik szerepet, de a hatékony információbiztonsági rendszer kiépítésének alapja is a részletes kockázatelemzés. Ennek több módszere is van, érdemes körültekintően választani közülük.
„Információbiztonsági rendszerünk működtetésében az ISO 27001 irányelveit követjük, alapvetően az ott definiált kockázatelemzési módszertant követjük amellett, hogy az ISO 27001 minősítéssel még nem rendelkezünk. A kockázatelemzések első inputját különböző belső auditok, valamint hatósági kötelezettségből, például kritikus nemzeti infrastruktúraelemekből adódó vizsgálatok és adatszolgáltatások adják”, fogalmazta meg *dr. Zsuffa András,* a DIGI CISO-ja.
Fritsch Róbert, a Fővárosi Vízművek informatikai igazgatója arról beszélt, hogy az elemzéseket rendszeres időközönként végzik egy saját maguk által fejlesztett folyamat alapján. „A folyamatnál nagyban támaszkodunk a korábbi évek tapasztalataira és megpróbáljuk az értékelések után finomítani az eljárásokat, esetleg új, korábban még ki nem próbált módszerekkel, technikákkal jobbá tenni a saját folyamatunkat”, mondta el.
Ugyanerre a kérdésre *Hagen István,* a Bonafarm CISO-ja azt mondta, hogy a kockázatelemzés minden ágazatban, szektorban más és más. „A létfontosságú rendszerelemeknél törvényi előírás és előre definiált, igen bonyolult módszertan alapján kell elvégezni, de akad olyan terület is, ahol elegendő egy leegyszerűsített, saját módszertan használata. Ami mindegyik elemzésnél azonos, az az, hogy a felsorolt kockázatokat pontozni, majd ez alapján priorizálni kell, végül az így kapott eredmény alapján kell elkészíteni egy kockázatarányos intézkedési tervet”, fejtette ki.

FORRÁS: 123RF.COM

A kockázatelemzés eredményei hozzájárulnak a megfelelő vállalati stratégia megalkotásához

Kéz a kézben jár a kockázatelemzés és a hatékony kiberbiztonság

A kockázatelemzés elsősorban a gyenge pontok, fenyegetésében felismerésében nyújt segítséget. De vajon miként születik meg a fenyegetettségek toplistája, vagyis azoknak a fenyegetettségeknek a sorrendje, amelyekkel a leginkább számolni kell az elemzés által lefedett időtávban?
„Az elsődleges inputot ehhez a toplistához nem az információbiztonsági auditok eredménye adja, hanem az internetről, különböző Infosec szervezetek, például CISA, ENISA, BID stb. és szakmai NGO-k által publikált sérülékenységi és kockázati listák top elemei. Szerencsére az auditok megállapításai és ezen listák tartalma között elég nagy a távolság, azonban az igazi veszélyt az utóbbiak jelentik, felkészülni azok megelőzésére kell. A kockázatelemzéshez külső tanácsadókkal dolgozunk, illetve online eszközöket is igénybe veszünk”, mondta dr. Zsuffa András.
Természetesen az Informatikában a globális fenyegetettséget mindig figyelemmel kell kísérni. „Nálunk ezt a feladatot az informatikán belül az IT-üzemeltetéssel karöltve a biztonsági osztály információbiztonsági feladatokkal megbízott kollégájának bevonásával rangsoroljuk. A toplista

FORRÁS: ITBUSINESS

FRITSCH RÓBERT, FŐVÁROSI VÍZMŰVEK

FORRÁS: ITBUSINESS

HAGEN ISTVÁN, BONAFARM

felállításánál a globális fenyegetettséget mindig rávetítjük a saját infrastruktúránkra, így kapunk reális képet a tényleges kockázatról", mondta Fritsch Róbert.

„Az eredmény a hatásvizsgálatból esik ki. Ezt mindenképpen úgy végezzük, hogy minden egyes kockázatnál megvizsgáljuk a kockázat bekövetkezésének valószínűségét, majd annak hatását. Azok a kockázatok, amelyek magas bekövetkezési valószínűséggel, magas üzleti hatással bírnak, azok képezik a lista elemeit. A hatásvizsgálatban IT-biztonsági és informatikai szakértők és üzleti döntéshozók is részt vesznek. A menedzsment validációja után áll elő a végleges toplista", részletezte Hagen István.

A kockázatelemzés felülvizsgálatának gyakorisága

Akárcsak az informatikai költségvetést, úgy a kockázatelemzésben foglaltak érvényességét is fontos rendszeres időközönként felülvizsgálni. Dr. Zsuffa András szerint „a felülvizsgálat periodicitását az egyes kockázatelemzések típusa határozza meg. A belső Infosec auditokat/kockázatelemzéseket folyamatosan, szakterületenként végezzük, mintegy 18 hónap alatt érünk körbe az egész cégen, és utána újrakezdjük, finomított és több részterületen mélyebb vizsgálatokkal. A külső és belső sérülékenységvizsgálatokat szintén folyamatosan végezzük, bizonyos rendszerek esetében akár heti gyakorisággal, az eredményeket inputként használjuk fel a kockázatelemzésekhez.".

Hozzátette, hogy ebben a folyamatban, a felülvizsgálatokat a CISO vezeti külső szakértői támogatással. A kockázatelemzések tartalmától függően elsősorban szakmai szervezeti egységek vesznek részt ezeken, de például az információbiztonsági szabályzat betartását minden szervezeti egységben, a vezetőkkel együttműködve ellenőrizik.

A Fővárosi Vízműveknél évente kétszer vizsgálják felül a vállalati kockázatelemzést, amely tartalmazza az információbiztonsági területet is. „Ezen túl az információbiztonsági törvény részletes kockázatelemzést ír elő társaságunk részére, amelyet ezen intervallumokon belül az informatika és a biztonsági osztály együttesen értékel, és meghatározza a további tennivalókat. Fontos szempont, hogy jelentősen csökkentsük az vállalat elleni támadások kockázatát. Nagymértékben támaszkodunk a belső szaktudásra és tapasztalatra, de az elemzéseknél nagy hangsúlyt kapnak az automatizált külső vagy belső vizsgálatok eredményei is. Ezen kívül irányított vizsgálatokat is szoktunk készíteni. Ezeknél a vizsgálatoknál a cél határozza meg az igényelt szaktudást és ezen keresztül a partnert", foglalta össze Fritsch Róbert. Hagen István szerint a kockázatelemzés szükségességét az alábbiak határozzák meg: iteratív feladat, üzleti folyamatban történő változás, új infrastruktúra bevezetése, audit vagy sérülékenységvizsgálat során feltárt nem megfelelőségek, nem várt események, külső hatások (például háború a szomszéd országban). Egyes területeken törvényi kötelezettség, amely a belső szabályzat szintjén is előírja a kockázatelemzés rendszeres elvégzésének szükségességét.

Önmagában a kockázatelemzés nem oldja meg az IT-biztonsági problémákat

A kockázatelemzés noha nem oldja meg magában az IT-security problematikáját, a megfelelő kiberbiztonsági rendszer alapját adja, így kétségtelen, hogy mindenki számára hangsúlyos.

Kiss Franciska

ERŐSÖDIK A HACKERAKTIVITÁS A KIBERTÉRBEN

Baljós árnyak

„Különleges katonai művelet”, hogy maradjunk a hivatalos megközelítésnél. Sokan, sok mindent és sok helyen elmondtak már erről a századunkat mindenképpen meghatározó eseményről. Ne szépítsük, ahol repkednek a golyók, bizony háború van. Azonban a nem elhanyagolandó fizikai veszély mellett mindenkinek számolnia kell a virtuális térben, az interneten egyre szaporodó támadásokkal. A kirakatban természetesen a nemzetállamok állnak. *(Schneck Zsolt, a Shield Informatics ügyvezetője írása.)*

A fizikai konfliktust megelőzően hackertámadás érte az ukrán parlament, és a külügyminisztérium oldalát, valamint kabinet és egy sor kulcsfontosságú infrastruktúrát üzemeltető magáncég rendszerét, amelyeknek az ország működtetésében kiemelt a szerepe. Persze a válaszcsapás sem késett, a Kreml és az orosz kormányzati portálok sem úszták meg az Anonymous támadásait. Ez a háború felértékeli a kiberbiztonságot, és természetesen a kiberbiztonsággal foglalkozó cégeket, megoldásszállítókat is. Egy hatékony kibertámadás gazdasági hatása felérhet a fegyverekkel okozott károkkal.

Ez a konfliktus nem beszivárgott, hanem egyenesen belecsapódott a mindennapjainkba, téma a villamoson, a kávézókban és persze a céges megbeszéléseken. Mindenhol. A multi és nagyvállalatok humán és anyagi erőforrások bevonásával és egyre komolyabb biztonsági protokollok bevezetésével sokat tesznek azért, hogy a saját rendszereik biztonságát megerősítsék. A kkv azonban más kávéház.

FORRÁS: ITBUSINESS

SCHNECK ZSOLT, SHIELD INFORMATICS

A veszélyes tolvaj nem csap zajt

A nagyon látványos dolgok többnyire – kivéve, ha mondjuk egy hírportált vagy webshopot érintenek – kevesebb veszélyt rejtenek magukban, mint gondolnánk. Ha leáll a weboldal, elég gyorsan kiderül, a felkészült IT-csapat hamar orvosolja, az élet megy tovább. Azok az incidensek jelentenek igazán nagy gondot, amelyek láthatatlanul történnek, a támadók hosszú időt töltenek a rendszerben, gyakran csak megfigyelve annak jellegzetességeit, keresve a hibákat, feltérképezik a felhasználókat és azok szokásait.

Ezért a fenyegetés az esetek jelentős részében nem közvetlenül a nagy céghez érkezik. Sokkal egyszerűbb a támadók dolga, ha egy kisebb beszállító vagy más üzleti partner informatikai eszközeit törik fel, esetleg felhasználóit hackelik meg. Ahol nem áll rendelkezésre a megfelelő határ- és végpontvédelem, nincs elég erőforrás a hálózatok monitorozására, ott egyszerűbb kártékony kódokat elhelyezni. Egy jókor és jó helyen elindított adathalász-kampány többet ér, mint a vállalat webszerverének leállítása, a lényeg az adat és az információ.

Mi legyen a kkv dolga?

A multicégeknek érdekük, hogy a beszállítóik rendszereiről képet kapjanak, azaz minősítsék őket az informatikai rendszerük alapján is. A CIO-k előbb vagy utóbb ki fogják dolgozni azokat a megfelelőségi protokollokat, amelyeket a beszállítóknak teljesíteni kell, az együttműködéshez. A kisvállalati üzemeltetőknek és cégtulajdonosoknak pedig már most, jó előre érdemes gondolkodni a megoldásokon, megcsináltatni a belső és külső auditokat, azaz meg kell győződni a rendszereik valós állapotáról. Ezután tudnak döntéseket hozni, hogy melyek az elengedhetetlen beruházások, milyen intézkedési terveket kell elkészíteni, és hogyan kell adott esetben újragondolni a rendszereiket.

Itt az idő, hogy minden felelős vezető elgondolkodjon a vírus- és határvédelmi rendszerek korszerűsítésén, a levelezőrendszerek megfelelő védelmén, és úgy általában azon, hogy az IT-üzemeltetés és az IT-biztonság nem a szükséges rossz. Emberek, ezzel dolgoztok, ezzel kerestek pénzt! És sajnos a kritikus rendszerek támadása már mindennapos. A kiberháború már itt van, és hasonlít a fegyverekkel vívottra. Sokkal jobban az életünk része, mint az gondolnánk. *(X)*

LÁTHATÓVÁ TETT HIBRID KÖRNYEZETEK

Információk egy helyen

A hibrid munka lett az új norma, fontossá is vált a szervezet sikerének elérésében. A digitális, hibrid munkahelyen együtt dolgoznak felhő alapú, SaaS és öröklött technológiák, az alkalmazottak bárhol, bármikor, bármilyen eszközön képesek együttműködni, és kapcsolatba lépni az ügyfelekkel. De ez csak úgy megy, ha az IT a teljes informatikai környezetet látja.

FORRÁS: NTT MAGYARORSZÁG

ATTILA VAN DAM, RIVERBED | ATERNITY

„A mai nagyvállalati igények kielégítése érdekében az üzleti területek és az ügyfelek egyaránt elvárják az informatikai szervezettől, hogy korszerű és biztonságos megoldásokkal lássa el őket", mondja *Attila van Dam*, a Riverbed | Aternity Észak-Európáért felelős regionális vezetője.

A digitális átállás felgyorsítása gyakorlatilag megköveteli a nyilvános és privát felhőinfrastruktúrák használatát. A kihívás abban rejlik, hogy miként integrálhatók az öröklött környezetek az új felhőinfrastruktúrákkal, és miként lehet meggyőződni ennek a digitális átalakításnak a hatékonyságáról. Ha valaki modern, hibrid felhőkörnyezetek létrehozásán fáradozik, akkor meg kell birkóznia a saját adatközpontban, a felhőben és az edge-en működő erőforrások komplexitásával. Ehhez olyan megoldásokat kell bevezetni, amelyek teljes körű láthatóságot és kontrollt biztosítanak, lehetővé téve ezáltal a munkatársaknak, hogy robusztus, megbízható, biztonságos környezetben dolgozzanak.

Teljes láthatóság

A mai hálózatok összetettsége és az egyre gyakoribb és agresszívabb kibertámadások soha nem látott kihívások elé állítják az informatikai szervezeteket. Az informatikusoknak képesnek kell lenniük a biztonság és a teljesítmény szempontjából egyaránt teljeskörűen ellenőrizni a modern, hibrid környezeteket. Ehhez viszont arra van szükség,

Az egyre több digitális eszköz és szenzor, valamint az összetettebb hálózatok egyre több adatforrást is jelentenek – ezek hatékony kezeléséhez új, hatékony eszközök szükségesek

hogy ne csupán mintákat vegyenek az adatokból, hanem azokat a maguk teljességében tudják vizsgálni, legyen szó hálózatokról, alkalmazásokról és végfelhasználókról. Ezt teszik lehetővé a Riverbed megoldásai.

Ma már rengeteg adat keletkezik minden vállalatnál, hiszen az egyre több digitális eszköz és szenzor, valamint az összetettebb hálózatok több adatforrást is jelentenek. Ugyanakkor számos szervezet küszködik azzal, hogy a különféle monitorozó eszközökből származó adataik egymástól elkülönült silókba kerülnek, emiatt nehéz ezeket konszolidálni, és azonnali cselekvésre, döntésre felhasználni.

„A döntéshozókat elárasztják az adatok és a riasztások, amelyekből továbbra is hiányzik az üzleti intelligencia és a gyakorlati használhatóság, pedig ez még fontosabb lenne a hibrid hálózatok, a felhő és a földrajzilag szétszórt munkaerő esetében. Ám ha a felhasználóktól, az alkalmazásokból és a hálózatból származó összes, eddig silókban tárolt adatkat a felhőbe gyűjtjük, olyan, gyakorlatban is felhasználható információt nyerhetünk ki belőlük, amelyekkel optimalizálhatjuk a teljesítményt, maximalizálhatjuk a termelékenységet, csökkenthetjük a kockázatokat és javíthatjuk az ügyfélélményt. Így válhat az IT a vállalati hatékonyságnövelés motorjává", mondja Attila van Dam.

Érték az üzletnek

Ha az adatokat egységes nézetben látjuk, akkor nincs kérdés azzal kapcsolatban, hogy melyik adatforrásunknak szabad hinnünk és melyiknek nem. Ebből kiindulva lehet olyan információkat kínálni, amelyek révén az IT végrehajtóból a technológiai fejlődés mozgatórugója lesz. Azáltal, hogy soha nem látott teljesítményt, fokozott termelékenységet és hatékonyságot, valamint zökkenőmentes üzletmenet-folytonosságot biztosít, az üzlet egésze számára kínál értéket.

„Mi készen állunk arra, hogy segítsünk ügyfeleinknek és a piacnak felkészülni erre az új hibrid korszakra, amelyben minden a digitális élményről és teljesítményről szól", teszi még hozzá Attila van Dam. „Vessen egy pillantást a *Riberbed | Aternity Hybrid Work Global Survey 2021* tanulmányra, és fedezze fel, hogyan tudja létrehozni saját, nagy teljesítményre képes hibrid munkakörnyezetét, vagy vegye fel velünk a kapcsolatot", javasolja végül. ■

AKTÍV ÉS JÖVŐBELI INFORMATIKAI VEZETŐK FIGYELMÉBE

Hat jel, hogy gyengébb a CIO, mint gondolná

Amikor vegyes eredményeket produkál az IT-csapat, a tehetséges emberek elmennek a cégtől, és a CIO pedig mindent megígér, csakhogy jó színben tűnjön fel a nagyfőnök előtt, itt az idő megvizsgálni a középszerű teljesítmény okait, és átgondolni vezető megközelítést.

FORRÁS: 123RF.COM

Az IT-vezetők gyakran foglalkoznak alkalmazottaik hatékonyságának növelésével, de arra kevesebb idő jut, hogy egy lépéssel távolabbról megvizsgálják, mennyire jól menedzselik a csapatot. A CIO-t gyakran a saját vélt sikerének népszerűsítése foglalja le, és eközben nem veszi észre, hogy rossz alapokra építkezett. A vezetés elméletével foglalkozó szakemberek és a CIO-k szerint is vannak figyelmeztető jelek arra, hogy a vezetőnek át kell gondolnia vezetési stílusát és megközelítését. A cio.com és az amerikai Forbes cikkeinek segítségével hat, változtatásért kiáltó jelet mutatunk be.

1. A tehetségek elhagyják a céget

A gyenge vezető egyik legbiztosabb jele, ha a bizonyítottan értékes munkatársak sorra hagyják el a szervezetet. Az embereket a cég brandje vonzza be, de a rossz vezető miatt távoznak – mint az közismert. A tehetségek megtartása sok esetben nem is pénz, hanem odafigyelés és empátia kérdése.
Ha a kollégák azt érzik, vezetőjük nem törődik velük, nem hallgatja meg őket, akkor hogyan várhatjuk el tőlük, hogy törődjenek a vezetővel és a szervezet céljaival? Sok probléma megoldható, ha a CIO kellően odafigyel, és ténylegesen meghallgatja a kulcsembereket. Inspirálja, támogatja és motiválja őket, hogy a lehető legjobb formájukban dolgozzanak – vagyis igazi empatikus vezetőként viselkedik.

2. Nem ismeri be tévedéseit

Ne higgyünk édesanyánk dicséretének, nem vagyunk tökéletesek. Ha tévedünk, fel kell vállalni, el kell ismerni az egész csapat előtt, és a következtetéseket levonva tanulni belőle. Az alázatnak az is a jele,

> Azokra a projektekre kell összpontosítani, amelyek előnyt élveznek, mert valóban a szervezet stratégiai céljait szolgálják

hogy tiszteljük a többieket, és elfogadjuk hibáinkat. Ezért néhanapján érdemes egy jót kacagni saját magunkon. Egy erős vezető mindezt képes felvállalni.
Ugyancsak tévedés, hogy kellő vezetői alázat nélkül, diktátorként erős kézzel kell vezetni a csapatot. Bármennyire hihetetlen, másnak is lehet korszakalkotó ötlete vagy hatékonyságnövelő javaslata. A jó vezető felismeri ezeket a jó ötleteket, és szakmai alázattal, „forrásmegjelöléssel" építi be a tervekbe, stratégiákba. Ezzel is bátorítjuk a kollégákat, hogy mutassák be új ötleteiket, hiszen a vezető elérhető, megszólítható, partner az újdonságokban.

3. Az eredmények eléggé vegyesek

A gyenge vezetőnek gyakran túlzottak az elvárásai a projektek céljával és határidejével kapcsolatban. Ezek a vezetők egyszerűen nem veszik figyelembe, hogy a csapat ideje is véges, és hogy az új projekteket a meglévő feladatok mellé vállalták be. Az összeszedett CIO a csapat tagjaival közösen méri fel, hogy mi valósítható meg az elképzelésből, és hogy mennyi az a szimultán feladatmennyiség, amennyi nem okoz kiégést. Ha mindezt rosszul méri fel, akkor a tehetséges emberek egyszerűen elhagyják a szervezetet, miközben az eredmények is elmaradnak.
A rendelkezésünkre álló erőforrásokat és a csapat teherbírását figyelembe véve azokra a projektekre kell összpontosítani, amelyek tényleg előnyt élveznek, tényleg a szervezet céljait szolgálják. Hallgassunk a csapat visszajelzéseire, és ha megszorulnánk, vásároljunk külső erőforrásokat, ezzel is segítve munkatársainkat.

+1: nem értékeljük eléggé a női csapattagokat

Belátjuk, a hardcore IT-területen alulreprezentáltak a nők, nincs sok női programozó vagy IT-biztonsági szakértő. Ha már van egy lány a csapatban, akkor ne csak azért legyen ott, hogy teljesítsük a nemi kvótát, kipipálhassuk ezt a négyzetet. Értékeljük őket tehetségük szerint, biztosítsunk fejlődési alkalmakat nekik, becsüljük meg kellőképpen munkájukat. Biztos, hogy kiváló tehetségekről van szó, akik rengeteg előítéletet és sztereotípiát leküzdve állják a sarat a(z egyelőre) férfias területen.

4. Mindent megígér a vezető

Vannak CIO-k, akik a csillagos eget is megígérik a vállalatnak, csak hogy jó színben tüntessék fel saját magukat a felső vezetés előtt. Azonban, ahogy az előző pontban is elmondtuk, a csapat teherbírásának függvényében kell az ígéreteinket is megfogalmazni. A túl sok vállalás túlórához, megfeszített munkatempóhoz, sokkal több hibához és végső soron kiégéshez, katasztrófához vezet. Lehet sprintekben dolgozni, de hosszú távon ezt senki sem bírja. A túlhajszolt, kiégett kollégák pedig az első adandó alkalommal elhagyják a céget.

5. Saját vállát veregeti

Aggasztó jele a vezetői gyengeségnek, ha az adott vezető folyamatosan arról beszél, hogy ő milyen erős és jó főnök. A valóban jó főnök általában megpihen, egy lépést hátralép, úgy figyeli meg saját vezetői stílusát, néha megkérdőjelezi képességeit, és aktívan keresi a visszajelzéseket környezetétől. Ugyanakkor a jó vezető törődik a tehetségekkel, szakmai szempontból kielégítő feladatokat biztosít számukra, teret enged kreativitásuknak, támogatja önálló döntéshozatalukat.
A gyenge vezetőnél minden saját személye körül forog, az erős főnök viszont a csapatával törődik. Például nem lopja el a csapat ötleteit, csak hogy jól mutasson a cég előtt. Elég magabiztos és bátor ahhoz, hogy a kreatív munkatársakat, csapatokat megdicsérje, rendszeresen elismerje hozzájárulásukat és tehetségüket, inspirálja őket a közös cél érdekében. Ha a vezetőnek csak a saját személye a fontos, nem képes fejlődési lehetőségeket teremteni csapattársai számára, esetleg vezetői képzést biztosítani a tehetségeknek.

6. Nincs munka-magánélet egyensúly

A gyenge vezető túlórával kompenzál, ő az első reggel az irodában, és este is ő kapcsolja le a villanyt távozáskor. Munkán kívül senki sem ismeri ezt a munkamániás vezetőt, csak a szakmai robotarcát mutatja állandóan. Az egy dolog, hogy elkötelezettek vagyunk a munka mellett, de ha túl sokat dolgozunk, akkor ugyanezt várjuk el a többiektől is – ami a kiégés tökéletes receptje. Ami pedig a személyes életünket illeti, az erős vezető ahhoz elég erős, hogy szerettei körében, sérülékenyen is megmutassa magát kollégái előtt – ezzel is erősítve a csapatot összetartó társadalmi kötelékeket.

Vass Enikő

LELKIISMERET-FURDALÁS NÉLKÜL

Szabadidős tevékenység munkaidőben? Miért ne?

FORRÁS: 123RF.COM

A tehetséges munkavállalók megtartásának egyik alulértékelt eszköze, amikor a munkáltató ténylegesen támogatja, hogy a kolléga munkaidőben a hobbiját végezhesse. Így a kollégák valóban lelkiismeret-furdalás nélkül szabadíthatnak fel olyan kreatív energiákat, amelyek a vállalat hasznára válnak. A nem szokványos juttatások itthon a nemzetközi cégekre vagy a kreatív iparágakra jellemzőek, de ott sem szabad túlzásokba esni.

Sokat foglalkoznak a vállalatok azzal, hogy milyen eszközökkel, hogyan tartsák meg a tehetséges alkalmazottakat: vonzó irodákat rendeznek be, jobban odafigyelnek a kollégák egészségére, netán egész családjára, igyekeznek a kisebb gyermekeket közelebb hozni a szülőkhöz, például saját bölcsőde üzemeltetésével.
A „Juttatások – Magyarország 2020" című tanulmány szerint itthon a szervezetek 69 százaléka élt a juttatások lehetőségével a javadalmazási politikájában. A megkérdezett cégek 9 százaléka mondta azt, hogy a juttatások csak bizonyos dolgozói csoportoknak érhető el, 57 százalékuk az összes dolgozó számára egységesen biztosít juttatást, 34 százalékuknál pedig minden dolgozó részesül juttatásban, de dolgozói csoportonként

A kisebb cégek a tapasztalatok szerint inkább a klasszikus juttatásoknál maradnak annak ellenére, hogy már felismerték a cafeteria-rendszer megtartó és jutalmazó erejét

eltérő mértékben. A juttatást nem kínáló szervezetek felénél költségcsökkentés miatt szüntették meg az egyébként korábban létező juttatásokat, másik felénél meg egyáltalán nem is volt hasonló.
Az egyik mellőzött és talán kevésbé használt ilyen juttatás a kollégák hobbijának támogatása. Egy tanulmány szerint a vállalat azzal tudja támogatni az alkalmazottak munkán kívüli hobbiját, ha közösen időt találnak erre. A kutatók szerint, ha az alkalmazottaknak sokkal nagyobb beleszólásuk van saját munkaidejük meghatározásába, akkor a hobbira is jut idő. Magyarul, ha a cégnél az az elvárás, hogy a kollégák a hobbis tevékenységek köré szervezzék munkaidejüket, akkor jut is idő rá. Hiszen sok esetben a szabadidős tevékenység azt jelenti, hogy bizonyos időben, rendszeresen távol kell lenniük a cégtől. A munkáltatónak lehetőséget kell adnia a kollégának, hogy lelkiismeret-furdalás nélkül ott tudja hagyni a munkát, és a hobbijára összpontosítson. Mindezt úgy, hogy a teljesítményértékeléseket se befolyásolja.
Egy elkötelezett apuka minden vágya az volt, hogy a lánya iskolás focicsapatát edzhesse. Ez azt jelentette, hogy minden szerdán és pénteken 4-kor az iskolában kell lennie, miközben a munkaidő gyakran 6-7 óráig is elhúzódik. A megoldás: a tervezett szabadidő. Az apuka szerdán és pénteken 9 helyett már 7-kor kezdte a munkát, de cserébe fél 4-kor már letehette a billentyűzetet, hogy fociedző lehessen.

A kreatív szabadság is feltölti az energiákat

A tervezett szabadidő ennél hosszabb is lehet, amelyet már „sabbaticalnak" neveznek. Ez azt jelenti, hogy például fél évig a kolléga utazhat, hogy kikapcsolódjon, miközben a munkaadó megtartja állását, esetenként még fizetve is őt. *(Magyarul leginkább tanulmányi, alkotói szabadság néven ismeretes – a szerk.)* Az Adobe például a náluk legalább öt éve dolgozóknak a szokásos szabadság felett négy hét fizetett szabadságot ad az álomvakációra vagy a régóta dédelgetett könyv megírására. A Google-nál egy ösztöndíjprogram keretén belül a kollégák maximum hat hónapot dolgozhatnak az általuk kiválasztott alapítványnál vagy projekteken.
A fenti kutatás azt is feltárta, hogy ha egy cég támogatja is a szokatlan időbeosztást, a kollégák tartanak a lehetőség kihasználásától: a hobbi okozta szokatlan időbeosztás miatt úgy tűnhet, hogy kevésbé elkötelezettek munkájuk iránt. Azonban nincs semmilyen bizonyíték arra, hogy a munkaidőből kiszakított hobbiidő csökkentené a munkahelyi teljesítményt. Sőt, a kutatások szerint egy fő tevékenység mellett végzett hobbi vagy esetleg mellékes munka növeli a fő tevékenység hatékonyságát és eredményeit.
A hobbival kapcsolatos hasonló félreértések tisztázásában a vezetőknek jut komoly szerep. A saját hobbi és annak hatásainak bemutatásával a vezető arra biztatja beosztottait, hogy ők is nyugodtan szakítsanak minderre időt. A vezetőknek tenniük kell azért, hogy a kollégák egymás kedvteléseit megismerjék: időt és helyet kell biztosítaniuk a hobbis tevékenységek megosztására, ez lehet egy pénteki megbeszélés vagy egy virtuális találkozó is. Az embereket jobban is érdekli a velük egy szinten lévő kollégák szabadidős elfoglaltsága, mint a vezetőjüké. Amikor a kollégák megosztják egymás között hobbijaikat, közelebb kerülnek egymáshoz, pozitív kapcsolatok alakulnak ki – amelyeket végső soron a cég eredményeinek javítására használnak majd fel, szinte akaratlanul.

A kreatív vállalatok élnek vele

„A nem szokványos juttatások a nemzetközi cégeknél jellemzőbbek, ott is leginkább a kirívóan munkaerőhiánnyal sújtott területeken, mint az informatika, de jelen van az innovatívabb, kreatív startupok esetében" is, mondja *Pákozdi Dorottya,* a Vision Recruitment csoportvezetője, sze-

FORRÁS: VISION RECRUITMENT

PÁKOZDI DOROTTYA, VISION RECRUITMENT

FORRÁS: 123RF.COM

nior HR-tanácsadó. A szabadidős tevékenységek munkaidőben történő támogatása leginkább azoknak a vállalatoknak az életébe építhető be, amelyek törzsidővel vagy rugalmas beosztással dolgoznak. A kisebb cégek a tapasztalatok szerint inkább a klasszikus juttatásoknál maradnak annak ellenére, hogy már felismerték a cafeteria-rendszer megtartó és jutalmazó erejét. A juttatások mind a munkaerő bevonzása, mind megtartása szempontjából fontosak, hiszen a jelöltek számára is meghatározó, hogy az alapbéren felül még milyen plusz bevétellel számolhatnak.
Az a vállalat, amelyik tehetséges embereket szeretne magához vonzani, előnyös, ha hangsúlyt fektet az ilyen jellegű extra juttatásokra. „Tapasztalataink szerint azonban a jelölteket egyre inkább a minél magasabb alapbér vonzza elsősorban, egy-egy ajánlat elfogadása esetében ez a döntő szempont", hangsúlyozta Pákozdi Dorottya, aki nem hisz az extremitásokban. A szervezeteknek ügyelniük kell arra, hogy egészséges egyensúlyt alakítsanak ki. „Figyeljünk arra, hogy az extra juttatások ne vigyék el a fókuszt, és a kollégák továbbra is tudjanak a valós feladatokra összpontosítani. Egyes projektalapú munkát végző informatikai cégeknél például lehet érdekes egy Xbox- vagy PlayStation-sarok, ahol a munka befejeztével vagy két projekt között kiengedhetik a fejlesztők a gőzt. Más helyeken viszont zavaró is lehet mindez, a tényleges munka és produktivitás kárára mehet", figyelmeztetett.

Kreatív juttatások

Pákozdi Dorottya segítségével több kategóriába soroltuk a nem szokványos juttatások körét. A teljesség igénye nélkül az alábbi kategóriákat lehet megkülönböztetni.

– Egészség, hobbi: a járvány miatt is kerültek még inkább a középpontba. Az egészség megőrzésével kapcsolatos élet- és egészségbiztosításról, menedzseri egészségszűrés csomagokról van itt elsősorban szó. Ide tartozhat a munkavállaló hobbijának támogatása, a sport-kártyák biztosítása, a céges jóga vagy zumba szervezése, netán sporteseményen, kulturális eseményen való részvétel támogatása.

– Családi élet, magánélet: vállalati bölcsőde, óvoda biztosítása, a céghez közel lévő, esetenként magánóvodába járás támogatása. Családi vagy pénzügyi problémák esetére tanácsadás, konzultáció biztosítása, adott számú alkalomra.

– Tanulás, szakmai fejlődés támogatása: egyes vállalatok a tanuláshoz szükséges időt biztosítják a munkaidő kárára, más helyen nyelvi kurzusokat tesznek elérhetővé vagy a szakmai tanfolyamok költségét állja a cég. A drágább, exkluzívabb kurzusok esetén megszokott a tanulmányi szerződés, ahol az oktatási költségek fejében a cég elvárásokat támaszt és megállapodást kötnek a munkahelyváltás feltételeiről. Ide tartozik a konferenciákon való részvétel támogatása is.

– Utazási költségek: a gyakran előforduló üzemanyag-támogatáson és BKVbérleteken túl taxicsekk is adható azon alkalmazottak részére, akiknek a műszakjuk a késői órákban ér véget. Az autóbérléssel, kölcsönzéssel foglalkozó cégeknél a kollégák kedvezményesen használhatják ezeket szolgáltatásokat.
– Irodai juttatások: itt sokszor csak a képzelet szab határt (szélsőséges példa: ingyenes Túró Rudi automata). A kávé vagy tea biztosítása szinte alapvetőnek számít már, de szervezhetők közös céges reggelik, vacsorák. Főként startup-cégeknél gyakori az állatbarát iroda kialakítása, játszósarok megépítése, bizonyos ételek korlátlan fogyasztása, vagy akár az irodai masszázs.
– A szabadságokhoz kapcsolódó juttatások: ide tartozik a jelenléti bónusz, amely az indokolatlan táppénzes távolmaradást hivatott csökkenteni. Létezik teljesítményhez vagy eseményhez (születésnaphoz, gyermekszületéshez, egyéb családi eseményekhez) kapcsolódó extra szabadnap.
– Home office biztosítása: a járvány harmadik évében egyre kevésbé számít extra juttatásnak, hiszen vannak területek, ahol állandósulni látszik a hibrid munkavégzés, átlagosan heti 2-3 nap irodai munkával. De vannak iparágak, ahol nem életszerű a rendszeres otthoni munkavégzés. A távmunka esetében juttatásnak számít a kényelmes otthoni munkakörülmények megteremtésének vagy a rezsiköltségeknek a támogatására is.
– Ajándékok: bizonyos esetekben a legjobban teljesítő kollégát jutalmazhatja a cég valamilyen kikapcsolódást nyújtó programmal (szabadidő, wellness, gasztronómia, üdülés).

A tehetségek fejlődésébe kell fektetni

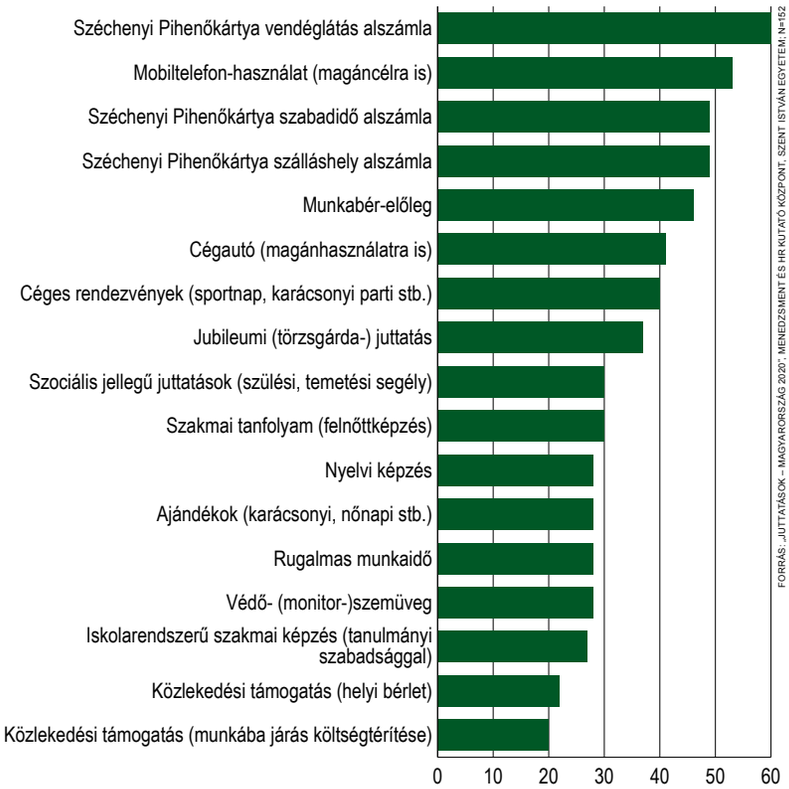
„Az ösztönzés kulcsa a lojalitás kialakítása”, mondja *Zubor Anikó*, a NEXON szenior HR-generalistája. „Alapvető eszközeiben nem változott a módszertan, a tapasztalataink szerint, inkább a lehetséges eszkö-

FORRÁS: NEXON

ZUBOR ANIKÓ, NEXON

A leggyakoribb fix juttatási formák 2020-ban

(válaszolók százalékában)



FORRÁS: „JUTTATÁSOK – MAGYARORSZÁG 2020”, MENEDZSMENT ÉS HR KUTATÓ KÖZPONT, SZENT ISTVÁN EGYETEM; N=152

zök prioritási sorrendje alakult át. Több kutatás is megerősíti, hogy bár az elérhető jövedelem továbbra is fontos, de hátrébb sorolódott a fontossági listán”, teszi hozzá.
A digitalizáció korában a hibrid munkavégzés, valamint a munka-magánélet egyensúlyának támogatása az alapvető munkavállalói igények közé került. A munkavállalók biztonságérzetének megteremtése a távmunka erején is túlmutat. A világban zajló külpolitikai, egészségügyi és gazdasági események hatásai a munkáltatóknál is megjelentek. Az erre történő reakció, a reziliencia mértéke minden munkavállaló számára nagy jelentőségű. „Azt tapasztaljuk, hogy rendszeres kommunikációval és folyamatos tájékoztatással tovább tudjuk erősíteni tehetséges kollégáink lojalitását. Törekszünk arra, hogy a vállalati célkitűzések és a tervezett jövőbeli lépések ismertetésével megteremtsük azt a légkört, melyben tudnak és akarnak hosszú távra tervezni”, mondta el a HR-generalista.
Egy szakmai mondás szerint egy munkavállaló céget választ, de vezetőt hagy el. A tehetségek megtartása tekintetében tehát a márka és a cégkultúra mellett a vezetőikkel való együttműködés minősége is döntő tényező, hiszen a munkavállalók felé a vezető képviseli azt, amit a vállalat nyújt. A jól teljesítő, fejlődni vágyó kollégák számára kiemelt jelentőségű, hogy vezetőjükkel közvetlen, állandó kapcsolatuk legyen. „A vezető jelenléte, figyelme elengedhetetlen, hogy a bevonást, felhatalmazást és a fejlődés lehetőségét érezze a munkatárs. Nemcsak az új munkaerő növekedésére kell tehát odafigyelni, hanem a meglévő tehetségek fejlődésébe is be kell fektetni”, fejezte be Zubor Anikó.

Vass Enikő

ELENGEDHETETLENEK A CSAPATÉPÍTŐ PROGRAMOK A KÖZÖSSÉG ÉLETÉBEN

Egyedül nem megy

FORRÁS: 123RF.COM

A csapatépítő programok jó alkalmat jelenthetnek arra, hogy a nem IT-fókuszú cégeknél dolgozó, a közösségbe esetleg nehezebben beilleszkedő informatikusokat is integrálják a csapatokba. Az ITBUSINESS-nek nyilatkozó szakértők szerint mindig akadnak visszahúzódó emberek, főleg a nagyobb létszámú csoportokban, őket sok türelemmel és apró, de biztos lépések során keresztül lehet bevonni a közös aktivitásokba.

Sokat változott az elmúlt években az informatikusokról élő kép a közvéleményben, hiszen a sötét kuckókban gubbasztó, maguknak való, folyamatosan a billentyűzetet nyomkodó, inkább támogató szerepet betöltő emberek a legkeresettebb munkavállalókká váltak, a tudásuk lényegében minden cégnél nélkülözhetetlen. A feladataik azonban sok esetben lehetővé teszik, hogy akár otthonról, vagy a többi munkatárstól elkülönülve végezzék azokat, így a közösségbe illeszkedésük is nehezebb lehet, ha nem kifejezetten IT-fókuszú vállalkozásról van szó. Pedig az, hogy csapatban is képesek legyenek dolgozni az alkalmazottak, összeadódjanak a problémamegoldó

képességek és az egyes részlegeknél meglévő tudás, az adott cég versenyképessége szempontjából is fontos lehet. A csapatépítő tréningek jó alkalmat jelenthetnek az ilyen kihívások leküzdésére, és a tapasztalatok azt mutatják, hogy még az ilyen programokat alapból elutasító, a többiekkel nehezebben szót értő, nehezebben megnyíló embereket is be lehet vonni a közös erőfeszítésekbe.

Mindenki szeret játszani

„Mindannyiunkban ott van a gyerek felnőtt korunkban is, így az emberek többsége szerencsére nyitott a játékos programokra. Az általunk kínált szolgáltatások játékos formában építik a közösséget, így könnyen bevonódnak a résztvevők. Viszont főleg a nagyobb létszámú rendezvényeken gyakran előfordul, hogy visszahúzódó, a közösségbe nehezen beilleszkedő emberekkel találkozunk. Az a tapasztalatunk, hogy az ilyen típusú emberek gátlásosabbak, azonban ezeket a gátlásokat a játékok során általában sikerül levetkőzni, ezért az esemény végén felszabadultabban távoznak tőlünk, mint ahogyan érkeztek. Ha őket külön szólítanánk meg, azt gondolom, felhívnánk a gyengeségükre a figyelmet, ezért a közösség ugyanolyan tagjaként kezeljük őket, és szinte kivétel nélkül sikerül bevonnunk őket a programokba”, számolt be a tapasztalatokról *Mátyás Péter,* a Trap Factory ügyvezető igazgatója.

„Azt tapasztaljuk, hogy a kötelező csapatépítések mindig megosztják a társaságot: vannak, akik nyitottabbak, vannak, akik kevésbé. Ez nagyban függ a személyiségtől, helyzettől, néha magától a programtól, helyszíntől vagy akár a napszaktól is. Ami viszont tagadhatatlan, hogy az ilyen jellegű csapatépítő programok elengedhetetlenek egy közösség életében, ezért fontos, hogy mindenki részt vegyen bennük a saját komfortzónájának megfelelően. A saját szabadulószobás programjainkon eddig mindig azt láttuk, hogy előbb-utóbb minden résztvevő csatlakozik. Persze az emberek sokfélék, és mindig van minimum egy-két személy,

> A játék hangulata magával ragadja a résztvevőket, és a végére mindenki bevonódik

aki nehezebben oldódik fel. Ez nem kell, hogy problémát jelentsen, különbözőek vagyunk, és a csapatépítésnek az is része, hogy ezt megtanuljuk kezelni és elfogadni. Úgy gondoljuk, hogy ezekben a helyzetekben a türelem és az apró, de biztos lépések megtétele működik a legjobban. Ha valakin látjuk, hogy nehezebben oldódik, akkor a játék bevezetésénél több figyelmet szentelünk neki, és éreztetjük vele, hogy ez egy biztonságos közeg. A szabadulószoba alapvetően olyan helyzetet teremt, amely bevonzza az eredetileg kevésbé érdeklődő játékosokat is, és mindenki talál magának olyan feladatot, amelyben örömét leli. A játék hangulata magával ragadja a bent lévőket, és a végére mindenki csinál valamit. Nagyon ritka, hogy valaki teljesen passzív marad a szabadulószobában. Ilyenkor általában összetettebb háttérproblémák is vannak, például konfliktus a személyek közötti,

FORRÁS: KELEMEN BALÁZS

MÁTYÁS PÉTER,
TRAP FACTORY

FORRÁS: HUMANFIELD

VALUSKA SÁRA,
FORTÉLY-SÁTOR ALAPÍTVÁNY

amelyekre legalább így fény derül, és elkezdhetnek a megoldáson dolgozni”, meséli *Valuska Sára* pedagógus, a csapatépítő programokat is rendszeresen szervező Fortély-sátor Alapítvány oktatási szakértője.

Közös célok

Azt, hogy milyen csapatépítő eseményt érdemes szervezni, nagy mértékben a program célja határozza meg, hiszen teljesen más jellegű aktivitásra van szükség, ha a szórakozás és az együtt töltött minőségi idő a cél, és megint másra, ha van egy konkrét fókusz, egy cél, amelyet az adott csapattal el szeretnének érni. „Főleg az utóbbi esetben érdemes behívni valakit, aki vezeti és moderálja az eseményt. A szabadulószobákban az a jó, hogy tematizálhatók és felépíthetők az adott közösség igényei szerint. Így alkalmasak szimplán szórakozásra, de ha van egy fókusza a programnak, azzal is tudunk dolgozni. Például előfordult már, hogy egy játékost elszeparáltunk a többiektől, és ezért extrán oda kellett figyelniük arra, hogy pontosan és jól kommunikáljanak, hogy sikeresen teljesítsék a feladatokat”, tette hozzá Valuska Sára.

Mátyás Péter szerint egy közös sporttevékenységnek is megvan a csapatot összekovácsoló jellege, de a Trap Factory-nél jobban hisznek azokban az aktivitásokban, ahol közösen kell gondolkodni közös célok elérése érdekében. „Egy szabadulószoba például semmi máshoz nem hasonlítható élményt biztosít a csapatoknak, ahol a kijutás érdekében, emelt adrenalinszint mellett kell minél inkább egymásra figyelni, együtt gondolkodni a résztvevőknek. Szépen nyomon követhető ebben a játékban, hogy melyik játékos milyen kvalitásával tud kitűnni és előre vinni a csapatát. Mégis, ha az egyéni képességekről beszélünk, akkor ügyességi és virtuálisvalóság-játékaink azok, amelyeknél leginkább számszerűsíthető és mérhető az adott egyén képessége”, mutatott rá Mátyás Péter. Úgy látja, hogy a közösségépítő programok során a legnagyobb kihívást talán a flow megtartása jelenti nemcsak a játékok, de a teljes esemény ideje alatt. Valuska Sára tapasztalatai szerint néha nehéz megtalálni a megfelelő programot, amely tényleg azt a funkciót tölti be, amely az adott közösség számára a legjobb, emellett pedig gyakran nehéz megfelelni a résztvevők túlságosan széles körű elvárásainak.

Kalocsai Zoltán

CHATBOTOK A CSAPATBAN, HR-HATÉKONYSÁG A MAXIMUMON

A hónap dolgozója: digitális kolléga a fedélzeten

FORRÁS: 123RF.COM

Nem kér enni, nem kér inni, motivációján a századik banális kérdés sem ejt csorbát, a nap huszonnégy órájában dolgozik, előszűri az adatokat és még az interjúszervezésben is segít, cserébe nem mesél fárasztó vicceket, és sosem morcos – kell ennél több? A chatbotok HR-beli alkalmazási területeire és a gyakorlati működésükre voltunk kíváncsiak, és arra is, hogy vajon öt év múlva hús-vér toborzó vagy gép válaszol-e majd a feltett kérdésekre.

A chatbotok létezését a felhasználói szokások változása tette indokolttá azzal, hogy egyre többen használnak rendszeresen valamilyen chat platformot, és nem csak hogy használják, de annyira az élet részévé vált, hogy a legtöbb esetben itt vagyunk elérhetőek.

A „Hónap dolgozója” címért is versenybe szállhatna

„A chatbotok egyre nagyobb szeletet tudnak vállalni a toborzás folyamatából. Jellemzően azokat a repetitív és adminisztrációs feladatokat veszik le a toborzókról, melyek nem igényelnek humán kapacitást, jellemzően nem kedvelt részei a napi »harcnak«. Továbbá az eszköz alkalmas arra is, hogy megfelelő algoritmusokkal a háttérben akár pszichometriai elemzéseket is kezeljen” – fogalmazta meg *Hujber Tibor,* a ChatBoss Team CEO-ja.

A toborzási területen a pályázók továbbra is preferálják a személyes kommunikációt írásban is, telefonon még inkább, ha ez rendelkezésre áll

Ha a toborzás oldaláról közelítjük meg a kérdést, a klasszikus előszűrési részfeladatokra kiválóan alkalmas egy chabot. Nemcsak abban segít, hogy a jelölt megtalálja a megfelelő állást, hanem a jelentkezésben is. Míg a másik oldalról a HR-szakembert például az interjúszervezésben támogatja azáltal, hogy az adott pozícióra jelentkezéskor az azzal kapcsolatos kérdésekre adott válaszokat képes pontozni, és annak megfelelő shortlistet készíteni a jelentkezőkből. A high-tech cégekre szabottnak tűnő megoldás valójában a teljes piaci paletta toborzás-kiválasztás folyamatát tudja támogatni a fehér- és kékgalléros területet egyaránt.

„A mesterséges intelligencia alapú chatbot-megoldástól elvárt, hogy gyorsabb legyen az előszűrés és a jelöltlista kialakítása, valamint takarítsa meg az első interjú szervezésére és a gyakori kérdések megválaszolására fordított időt. Olyan pozíciók esetében működhet, amelyre nagy létszámú jelentkező érkezik.

Miben segít a chatbot?

– Tájékoztatja a jelölteket az elérhető álláslehetőségekről lokáció szerint.
– Érdeklődés esetén adatkezelési nyilatkozatot tud elfogadtatni.
– Elvégzi az alapvető logikai teszteket a toborzók helyett.
– Begyűjti a jelölt preferenciáit, illetve a tanulmánnyal és szakmai háttérrel kapcsolatos adatokat.
– Interjú-időpontot egyeztet.
– Választ tud adni a leggyakrabban előforduló kérdésekre.
– Mindezt a vállalat rendszerébe (ATS-be, adatbázisba stb.) rögzíti
– Gyorsan, 2-3 perc alatt lezajlik a jelentkezés.
– Bármikor indítható, például a villamosról két megálló között végig lehet vinni egy jelentkezést.
– Bármikor érkezik a kérdés, azonnal érkezik rá válasz.

FORRÁS: HUMANFIELD

VIDUS ANETT, HUMANFIELD

Sajnos a hazai munkaerőpiacra egyre inkább jellemző, hogy releváns jelöltek egyáltalán nem jelentkeznek álláshirdetésekre, igaz ez alacsonyabb szintű pozíciókra is. Az IT-szakemberek piacán szinte senki sem jelentkezik már az állásokra, hiszen a jelöltek tucatjával kapják a megkereséseket a cégektől és a fejvadászoktól”, mondta el *Vidus Anett,* a HumanField szenior részlegvezetője.

A gyakorlat prói és kontrái

Ami a chatbot gyakorlati használatát illeti, leggyakrabban a vállalat web- vagy Facebook-oldalán találkozhatunk a botokkal, illetve a Viber platformon működik még kiválóan. „A chatbotok vagy proaktívan megszólítják a jelöltet és végigviszik az előszűrés feladatát, vagy hirdetésekbe ágyazott linkekkel irányítja át a jelöltet a megfelelő chat folyamatba, ahol gyorsan, könnyen, akár menürendszeres struktúrában is eljuthat a jelentkezésig, illetve CV feltöltéséig”, összegezte Hujber Tibor.

Az előnye egyértelműen a hatékonyság és produktivitás növelése a toborzásban, illetve a vállalat eredményességében. Elsősorban olyan szervezeteknél hasznos, ahol fontos, hogy időben, megfelelő mennyiségű és minőségű jelölt kerüljön a rendszerbe. Minél nagyobb a vállalat létszáma, annál intenzívebben járul hozzá egy chatbot a toborzás sikerességéhez. Egy jól strukturált, toborzási szakemberek által elkészített eszköz mindenképp hozzáad a folyamatokhoz: rövidül a toborzási idő, csökkennek a költségek, kiváltható külső szolgáltató bevonása, csökken az adminisztrációra fordított idő, a jogi (GDPR-) kockázatok megszüntethetők, a vállalati brand javul a jelöltélmény javulásával, és végül, de nem utolsó

sorban a toborzásban dolgozó kollégák lojalitása növekszik, hiszen olyan feladatokra kell csak koncentrálniuk, amelyekhez ténylegesen szükségesek a képességeik.
„Jellemzően azok a vállalatok választják a chatbotot, ahol a létszám magasabb, mint 200 fő, vagy tömeges toborzás van, illetve, azok, akik szeretnék hatékonyabban, gyorsabban kiszolgálni HR-oldalról a termelést. Főként a toborzó és gyártó cégek sorolhatók ide. Fizikai munkások és diákok toborzásban hozza legygyorsabban az eredményeket, könnyen és gyorsan elérhető például a Facebookon, és amiatt is, mivel ma a pályázók általában gyorsan akarnak jelentkezni, nem szívesen töltenek 4-8 percnél hosszabb időt ezzel a tevékenységgel”, mondta el *Dömötör Péter,* a ChatBoss Team CTO-ja.
Ami a hátrányokat illeti, a technológiai, fejlesztői hiányosságok merülnek fel: ha nem készítjük fel megfelelően a chatbotunkat, vagy nem a megfelelő technológiát használjuk, akkor buta robotnak fog tűnni, és a jelöltek nem fogják kedvelni. „Az egyetlen negatív tapasztalat, hogy a szellemi pozíciók toborzásában egyelőre csak nagyon kis részét tudja kiváltani a feladatoknak, mert itt a folyamatok lényegesen nagyobb arányban igényelnek személyes egyeztetéseket, interjúkat. Ezen túl érzékelhető egy előítélet a chatbotokkal kapcsolatban, mert rengeteg, nem jól felépített, valós segítséget nem nyújtó eszköz érhető el az interneten. Gyakran ez a benchmark, és ez nehezíti a nyitottságot. Hazánkban még edukálni kell a piacot, de szépen haladunk előre”, tette hozzá Hujber Tibor.

Chatbot a csapatban – sajátos elvárások és a tágabb piac

„Fontos megemlíteni, hogy a toborzási területen a pályázók továbbra is preferálják a személyes kommunikációt írásban is, telefonon még inkább, ha ez rendelkezésre áll. A toborzási élmény része a cégek employer brandingjének, egy rosszul menedzselt kiválasztási folyamat árthat a cég hírnevének. A folyamatot egy fejvadászcég sokkal hatékonyabban tudja koordinálni, mint egy chatbot. Belső kommunikációs célokra azonban kiváló megoldás, könnyen lehet tájékoztatni

A visszajelzések alapján több, mint 90 százalék a pozitív visszajelzés, ezt mutatja a hagyományos előszűrésnél nagyobb konverziós ráta

nagy létszámot. Egyszerűbbé válhat a szabadsággal, bérszámfejtéssel kapcsolatos kérdések megválaszolása, gyorsabbá válik a folyamat”, fogalmazta meg véleményét Vidus Anett. „Nemzetközi szinten elterjedtebb a chatbotok használata, mint itthon. A hazai cégek vállalati kommunikációs csatornája továbbra is az emailes formára fókuszál, pedig ezen a funkció sokat segíthet”, tette hozzá.

Kiss Franciska

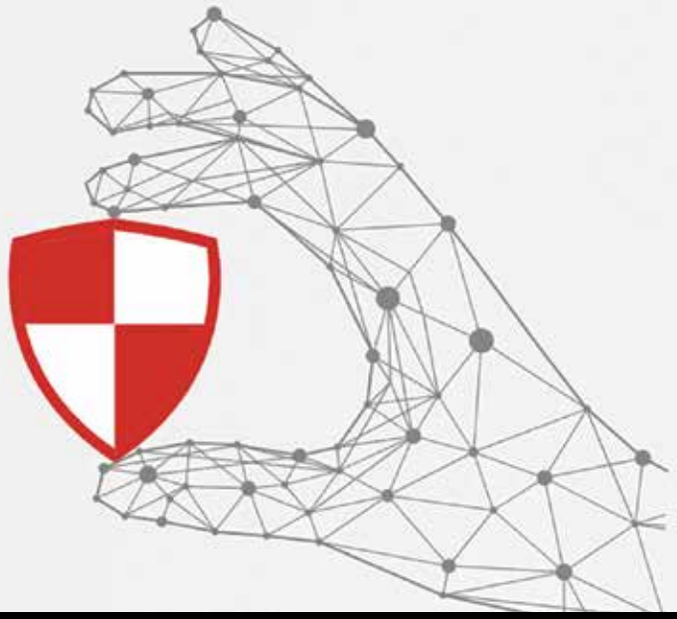
Kollaborációs megoldások az agilitás és a hibrid felsőoktatás szolgálatában

A hibrid munkavégzés harmadik evolúciós szintje már nemcsak az üzleti életben, hanem a felsőoktatásban, illetve a kollaborációs megoldások agilis módszertant kiszolgáló eszköztárában is innovációt indukál. A vizualitásra nagy mértékben építő agilis módszerek (mint a scrum vagy a kanban) digitális transzformációja új kihívásként jelent meg a kollaborációs folyamatokban – ezek támogatásáról és a konkrét fejlesztésekről beszélgettünk *Leveli Andrással,* az LSK Hungária üzlet- és termékfejlesztési igazgatójával.


LEVELI ANDRÁS, LSK HUNGÁRIA

FORRÁS: ITBUSINESS

„A pandémiás időszak irányította fejlesztések után visszatértünk a gyökerekhez és az interaktív kijelzőink kollaborációs szoftvercsomagjának továbbfejlesztése kerül ismét a fókuszba”, mondta Leveli András. Az újonnan érkező intuitív, gesztusvezérlési csomag alapjaiban fogja megváltoztatni a felhasználói élményt, és várhatóan olyan jelentőségű lesz, mint a kétujjas (multitouch-) nagyítás-kicsinyítés bevezetése volt. Emellett pedig hamarosan elérhető lesz a közvetlen post-it beszúrás is a fehértábla-szoftverben, amellyel teljessé válik az agilis módszertanok analóg eszköztárának (a filctollnak, a post-itnek és a fehértáblának) teljesen digitális megfelelője. Ezáltal az agilis munkafolyamatok az online térbe költözhetnek, vagyis teljesen kompatibilissé válnak a hibrid munkavégzés harmadik evolúciós szintjének elvárásaival.
Folytatjuk a 21. századi hibrid felsőoktatási megoldások fejlesztését is, amelyek első mérföldköve az érintőképernyős teremvezérlő rendszerünkhöz kifejlesztett mini TV stúdió lesz, ahol az előadó egyetlen kattintással kiválaszthatja majd, hogy melyik konferencia- vagy streamingkamera, valamint melyik tartalom kép kerüljön bele az online közvetítésbe, ráadásul milyen elrendezésben. ■



Kristálygömb 2022

A lezárásokkal teli időszak után idén végre élőben is megtartjuk a PROtACTION konferenciánkat. Ez az az esemény, amelyen megpróbáljuk felvillantani a kiberbiztonsági szakma forró trendjeit, új eszközöket, megoldásokat mutatunk be, új technológiákat hozunk, akár teljesen új gyártókkal, amelyek mostanában jelennek meg a magyar piacon. A mellékletünkben szereplő írások sokszínűsége jelzi, ahogy eddig, idénre is óriásit fejlődött a szakma. Egyre több megoldás kap direkt jelenlétet a régiónkban, és a CLICO, már több mint harminc éve, mindig a legfrissebb, legígéretesebb kínálattal van jelen, 2016 óta a magyar piacon is.

CSINOS TAMÁS, CLICO

FORRÁS: CLICO MAGYARORSZÁG

Idén bővült a portfóliónk az **Illumio** termékekkel. Olyan megoldást fejlesztenek, amely a mikroszegmentáció – zero trust megvalósítást az eddigi hálózatos megközelítés helyett végponti hangsúllyal próbálja sikerre vinni. Ez talán közelebb áll a hazai gyakorlatokhoz, mint más megközelítések, és a gyártó gyors sikerei Európában azt mutatják, hogy működik az üzenet és a technológia.
Szintén újdonság kínálatunkban az **Infinera,** amely az optikai transzport hálózatok egyik vezető megoldásszállítója. A rengeteg szabadalom és szabvány, amely az Infinera műhelyeiből kerül be más gyártók megoldásaiba, azt bizonyítja, hogy ezen az egyébként kicsit belassult piacon van, aki friss lendülettel képes megújulni, és a technológiai fölénye segítségével pozíciókat szerezni.
A legfrissebb (lapzártakor pár órás!) igazolásunk a **Netskope,** amely a SASE/SSE-piac vezetője az elemzők felmérései alapján. Ugyan ezekről a technológiákról évek óta beszélünk ilyen-olyan megnevezésekkel, de csak mostanában kezd megszilárdulni a kapcsolódó terminológia és ügyfél-elvárás-készlet.
Nem harmatosan friss (már egy egész éve foglalkozunk vele!), mégis a legtöbb ügyfélnek még újdonság a kereskedelmi forgalomban igénybe vehető kiberhírszerzési források megjelenése is. A CTI, azaz Cyber Threat Intelligence a biztonsági előrejelző vagy éppen post mortem csapatok alapeszköze lesz a közeljövőben, sokkal pontosabb, részletesebb, akár a felső, nem szakmai vezetés számára is értékes riportokkal, információkkal. Nemcsak a várható és folyamatosan változó támadási részletekkel, de iparági, sőt, geopolitikai kontextusba helyezéssel is pontosíthatjuk védelmi beruházásainkat és stratégiánkat, hiszen még a legpontosabb kockázatbecsléseket is lehet tovább finomítani.
Akinek sikerül időt szakítani **2022 május 4-én,** hogy vendégünk legyen a **PROtACTION** konferencián, az a helyszínen még színesebb, még bőségesebb infókat kaphat a trendekről. Ha mégsem, akkor sincs semmi veszve, olvassák a cikkeket, és örömmel állunk rendelkezésükre bármelyik elérhetőségünkön.

Jó tanulást, jó szórakozást, a CLICO Magyarország csapata nevében!

Csinos Tamás
country manager

A strukturálatlan adatok veszélye

Az adatok a vállalkozásunk éltető elemei. Vannak köztük olyanok is, egyre növekvő mennyiségben, amelyek érzékeny információt tartalmaznak, így azokat védenünk kell(ene). Rendszerint úgy gondoljuk, hogy a kritikus adataink strukturált formátumban biztonságban vannak, de meglehetősen egyszerű folyamat az értékes adatok kinyerése, például ERP-ből és más rendszerekből, majd ezekből megosztható fájlok létrehozása.

NÉMETH MÓNIKA, SZENIOR RENDSZERMÉRNÖK

FORRÁS: CLICO MAGYARORSZÁG

A felhasználók adatokat nyernek ki az alkalmazásokból, és új tartalmakat hoznak létre belőlük, amelyeket különféle fájlmegosztókon, felhőalapú tárolórendszerekben tárolnak, ezek pedig gyakran kívül esnek az informatikai osztály hatáskörén. Sajnos, ezeknek a sok esetben kritikus adatoknak a nagy része manapság strukturálatlan adatként – dokumentumok, táblázatok, prezentációk, jelentések, jellemzően egyedi fájlok formájában – van jelen. Külön kihívást jelent annak a megértése, hogy ezek az adatok hol vannak pontosan, ki férhet hozzájuk és egyáltalán mennyi ilyen jellegű adatunk van. Ha nem foglalkozunk a strukturálatlan adatokhoz kapcsolódó hozzáférési problémákkal, jelentős biztonsági és megfelelőségi kockázatoknak tehetjük ki a vállalatunkat, mivel a szabályzások (mint például a GDPR) ezek védelmét is megkövetelik. Ráadásul a támadók is egyre gyakrabban veszik célba a strukturálatlan adatokat, hiszen ezeket sokszor könnyű ellopni, legtöbbször nincsenek titkosítva, és értékes információkkal teli kincsesbányára lelnek bennük. Tucatnyi példát sorolhatnánk fel különböző adatvédelmi incidensekre, amelyek email-archívumok, jogi szerződések, orvosi dokumentumok, üzleti titkok, forráskódok és más, rendkívül érzékeny anyagok ellopásával jártak – mindezeket fájlokban, strukturálatlan adatként tárolták.

Miért nem védjük a strukturálatlan adatainkat?

Ennek számos oka lehet. Az egyik legvalószínűbb, hogy nem tudjuk, milyen és mennyi érzékeny adatunk van a különböző fájlokban tárolva, és amúgy is a büdzsénk csak a kritikus alkalmazások és adatbázisok védelmére elegendő. Gyakran azt sem tudjuk eldönteni, hogy az adott fájl védelme kihez tartozik, ki a gazdája, kinek kellene kategorizálni az adatokat, kiszűrni a redundáns vagy elavult információkat.

A biztonsági csapat elsődleges feladata a belső és külső fenyegetések észlelése és megelőzése, amelyre számos eszközt használnak is, mint például tűzfalak, SIEM- és DLP-eszközök, titkosítás. Noha egyes DLP-megoldások a strukturálatlan adatok kezelését célozzák, nem biztosítanak identitáskezelési képességeket. Hiányzik belőlük az a tudás, hogy átlássák és ellenőrizzék, hogy ki férhet egyáltalán hozzá az adatokhoz, és melyek az érzékeny adataink. Identitáskezelés nélkül pedig arra sem leszünk képesek, hogy az adatokhoz való hozzáférést felhasználónként vagy felhasználó csoportonként engedélyezni tudjuk, vagy vissza tudjuk vonni, ha éppen úgy szükséges.

Van erre a problémára valamilyen megoldás?

Mire van egyáltalán szükségünk? Azt már tudjuk, hogy egy olyan eszközre, amely képes átfogó képet nyújtani arról, hogy a strukturált és a strukturálatlan adataink közül ki mihez fér hozzá, valamint


FORRÁS: CPOMAGAZINE.COM

képes következetes hozzáférés-szabályozási és hozzáférés-ellenőrzési folyamatok biztosítására.

A **SailPoint IdentityIQ File Access Manager** (FAM) megoldása identitás- és hozzáférés-kezelést biztosít a fájlokhoz. Megmutatja, hol helyezkednek el az érzékeny adatok, ki fér hozzájuk, segít a megfelelő adattulajdonosok kiválasztásában, valamint azt is láthatóvá teszi, hogy aki eléri ezeket az adatokat, az hogyan használja azokat.

Az IdentityIQ FAM segítségével gyorsan megtalálhatjuk és katalogizálhatjuk az érzékeny adatainkat. Kereshetünk attribútumok (például kulcsszószabályok) vagy viselkedés (például fájlhasználat) alapján. Így azonosítani tudjuk, hogy a különböző lehetséges „helyszíneken” belül pontosan hol vannak értékesnek számító adatok. Képes gyorsan kiértékelni, hogy ezekhez az adatokhoz mely entitások férnek hozzá, és hogyan szerezték ezt a hozzáférést. Részletes elemzést nyújt a hozzáférési modellekről, és kiemeli a kihasználatlan és az eltúlzott jogosultságokat, amelyek kockázatot jelenthetnek a szervezet számára. Figyeli a felhasználók fájlokkal kapcsolatos tevékenységeit, biztosítja, hogy azok összhangban legyenek a vállalati szabályzásokkal, és riasztást küld az adattulajdonosoknak, amikor a házirend megsértését érzékeli. Rugalmas házirend motorja segít egy átfogó szabályzás létrehozásában, amely segítségével proaktívan felügyelhetjük a hozzáféréseket. Emellett minden egyes megfigyelt tevékenységhez hozzárendeli a tevékenység teljes biztonsági kontextusát, ami döntő fontosságú lehet a jogos hozzáférések és a hozzáférési jogsértések megkülönböztetésében.

Az adattulajdonosok feladatai

Az üzleti felhasználók a szervezeti adatok tulajdonosai, mivel ők hozzák létre és használják ezeket az adatokat. Az IdentityIQ FAM közvetlenül az ő segítségüket kéri a hozzáférés szabályzásához. Egy innovatív belső vállalati „crowdsourcing” technológiát alkalmazva teszi lehetővé az adattulajdonosok megválasztását. A hagyományos megközelítéssel ellentétben, amikor a legaktívabb felhasználót választjuk meg adattulajdonosnak, az IdentityIQ FAM meghatározza az adat szempontjából érintett tényleges felhasználói csoportot, majd a csoporttagok szavazatai alapján választja meg az adattulajdonost. Így válik ismertté, hogy valójában ki az adat gazdája.

Biztosítja, hogy a felhasználók csak a munkájuk elvégzéséhez szükséges adatokhoz férhessenek hozzá, mindezt úgy, hogy a hozzáférési kérelmeket egy önkiszolgáló felületen keresztül kezelhetjük. Ezenkívül a FAM automatizált hozzáférése felülvizsgálja a folyamatban lévő kérések érvényesítését is.

Mindezeket figyelembe véve a SailPoint IdentityIQ File Access Manager egy olyan megoldást nyújt a cégek számára, amely mellett nyugodtan hátra dőlhetünk, és biztosak lehetünk abban, hogy a különböző fájlokban előforduló érzékeny adataink is biztonságban vannak, és csak azok férhetnek hozzájuk, akiknek valóban szükségük van rá.

SailPoint

Miért van szükség IT-biztonságra az egészségügyben?

Az elmúlt években egyre többet halljuk, hogy az ipari és a „hagyományos” vállalati eszközök egyre inkább keverednek egymással a céges környezetekben, közösen kell őket kezelni. Mi is több alkalommal írtunk már erről az ITBUSINESS hasábjain, és ezt a trendet igazolja az is, hogy egyre több gyártó végez felvásárlásokat vagy invesztál komolyabb fejlesztésekbe a témában.

A trend pedig hasonló az egészségügy vonatkozásában is. Ezen a területen is azt látjuk, hogy folyamatosan fejlődnek az eszközök, és egyre nagyobb hangsúlyt kapnak azok az analitikai és diagnosztikai megoldások, amelyek a különféle egészségügyi eszközök esetében is megkövetelik a hálózati kapcsolatokat. Ezek kitettsége legalább annyira fontos szempont, és sok veszélyt hordoz magában, mint például egy ipari hálózat esetében. Gondoljunk csak bele, milyen problémákat okozhat egy nem megbízhatóan működő infúziós pumpa, amikor hirtelen túl kevés vagy túl sok gyógyszert adagol a betegnek, vagy mennyire kritikus lehet, ha egy képalkotó diagnosztikai rendszert feltörnek, és összekeverednek vagy megsemmisülnek a betegek leletei, esetleg „csak” pár napra kiesik a rendszer.
Ezeknek az IT-szakmában „medical IoT”-nak nevezett eszközöknek újfajta védelemre van szükségük, amely felépítésében ugyan az ipari biztonsághoz hasonló, ám az egészségügyre szabott biztonsági megoldásokat tartalmaz. A legtöbb fejlett eszköz esetében igazából műszernek „álcázott” számítógépről beszélünk, vagyis a borítás alatt valószínűleg egy hagyományos számítógép állítja elő a fejlett MRI- vagy CT-gép által látott információhalmazból az adott leletet. Viszont van egy fontos különbség: a hagyományos sérülékenységek és biztonsági kihívások mellett például az egészségügyi visszahívásokkal és problémákkal is foglalkozni kell, mivel az erről szóló hírek és bejelentések nem mindig jutnak el a megfelelő helyekre.
Ilyen esetekben óriási segítség lehet egy egészségügyi rendszerekre specializálódott IT-biztonsági megoldás, amely képes riasztani és egy közös felületen kezelni a különböző kitettségeket. Külön hasznos dolog, ha ez a megoldás akár beavatkozni is tud és a hálózat, illetve a biztonsági rendszerek között hidat képezve képes a megfelelő szabálymódosítások elvégzésére, illetve probléma esetén akár a kompromittálódott végpont elszigetelésére.

FORRÁS: FEPASOE.COM

Ezek a képességek a **Forescout** esetében egy integrált rendszerben találhatók meg, amely egyszerre képes IT-, IoT-, ipari és egészségügyi rendszerek kezelésére is. A platform fejlesztésekor korábban még egy modern NAC- (network access control) megoldást álmodtak meg, amely a hálózati hozzáférések kezelését és az eszköz viziblitásának biztosítását is megoldja, viszont ahogy a technológia fejlődött és a különböző IT-rendszerek egyre inkább összefonódtak, szükségessé vált, hogy új képességeket integráljanak a platformba. Így maga a megoldás továbbra is képes a korábbi funkciók ellátására, a különböző specifikusabb igények kiszolgálásra pedig a gyártó az adott iparágak kiemelkedő és vezető megoldásainak megvásárlásával, illetve integrálásával válaszolt, ezzel garantálva, hogy az így kialakított platform az élvonalba tartozzon. A Forescout megoldása képes akár teljesen passzív működésre is, de ha szükséges és a környezet megengedi, akkor a legkülönbfélébb integrációknak köszönhetően be is tud avatkozni.

<) FORESCOUT

SASE, SD-WAN és a többiek

Van úgy, hogy előbb születik meg egy technológia, illetve kezdik el az emberek használni az adott megoldást, mint hogy neve lenne. Sok esetben csak a használatakor adnak az adott technológiának valamilyen pár betűs elnevezést a különféle elemzőcégek.

Legalább ilyen gyakran fordulnak elő olyan esetek is, amikor egy elemzőcég hamarabb kezd el evangelizálni egy nagy koncepciót, mint ahogy az valós, elérhető és kézzelfogható megoldás lenne a piacon az adott szegmensben. A SASE- (secure access service edge) megoldások ez utóbbi tábort erősítik. Ugyan már hosszabb ideje halljuk, hogy ez a jövő, viszont eleinte nem láthattunk olyan megoldást, amely ténylegesen lefedte volna a koncepció összes területét.

Szerencsére most már kezdenek megjelenni azok a megoldások, amelyek egy ilyen komplex feladatot is képesek kiszolgálni. Ez a SASE esetében leginkább részleteiben jelent meg a különböző gyártók portfóliójában. A **Palo Alto Networks** esetében például viszonylag hamar megjelentek a különféle szolgáltatások felhős megfelelői, illetve ezeknek jó része már a SASE-koncepciónak való „megfelelési kényszer” előtt is létezett. Ez nem is meglepő, hiszen egy vezető IT-biztonsági gyártó esetén nagyon fontos, hogy kövesse a trendeket, illetve sok esetben diktálja is azokat, mint ahogy például az XDR esetében meg is tette.

A SASE-koncepció viszont egy kicsit más terület, mivel itt már nemcsak az IT-biztonság problémáit kell megoldani, hanem például hálózatoptimalizálásról, routingról, illetve QoS-ről is szó van. Ezért amikor a Palo Alto Networks előállt a megoldásával, nem csak a saját fejlesztéseire alapozott.

A bevált recept alapján a SASE-koncepciójuk hálózatbiztonsági funkcióit a jól ismert, új generációs tűzfalak felhős kivitelével és a már korábban is jelentős felhős kapacitásokkal bíró biztonsági funkciókkal szolgáltatják. Ez már önmagában is komoly és biztonságos gerincet nyújt a legkülönfélébb felhasználási esetekben. Viszont mivel a SASE nem csak IT-biztonsági megoldás, a gyártó által végrehajtott sok akvizíció közé bekerült például egy Cloudgenix nevű, új generációs SD-WAN technológiával foglakozó cég is. Fontos, hogy ebben az esetben az „új generáció” nem csak töltelékszó. Ugyanúgy, ahogy a tűzfalak esetében a Palo Alto Networks egyik fő vonzereje a fejlett alkalmazásfelismerés, ez a képesség az SD-WAN/SASE-megoldásuk esetében is megmaradt – például ebben az esetben alkalmazások szerint tudunk útvonalakat optimalizálni. A megoldásukat, hogy illeszkedjen a Palo Alto Networks portfólió elnevezéseihez, **„Prisma SD-WAN”** névre keresztelték és ezen a néven folytatják a további fejlesztését.

Ezzel a felvásárlással, illetve a megoldás integrálásával a SASE különféle területeit nagyon hatékonyan képesek lefedni. Ha valaki ezt az utat választja, és megfelelő hálózati kapcsolatokkal rendelkezik, akkor az irodák kiszolgálásához akár elég lehet csupán sima IPSEC-képes végpontokra támaszkodni, illetve a mozgó felhasználók esetében a jól ismert GlobalProtect kliensre. Ha első lépésként csak bizonyos funkciókat szeretnénk használni, a FWaaS- (szolgáltatásként elérhető tűzfalak) és felhős lehetőségekkel szemben konzervatívabb módon is megoldhatjuk a rendszer felépítését. Ilyenkor a megfelelő licencekkel ellátott tűzfalakkal, illetve az egyre inkább megkerülhetetlen felhős rendszerek védelmére kialakított megoldások megvásárlásával is megvédhetjük cégünket.

Alapvetően a SASE, illetve a SD-WAN törekvések esetén nagyon fontos, hogy érdemes akár évekre előre gondolkozni, és ha nem is választjuk egyből a felhős megoldásokat, célszerű olyan eszközöket beszerezni a különböző telephelyi funkciók ellátására, amelyek később képesek integrálódni egy közös nagy platformba, és elősegítik, hogy bárhol is legyen egy felhasználó vagy eszköz, ugyanazt a vizibilitást, felhasználói élményt és biztonságot kapja, mintha a céges határokon belül tartózkodna. Az ilyen, sok cég életében még csak elérendő célként felmerülő igények esetén a Palo Alto Networks megoldásai kiváló alapot képesek adni, amelynek köszönhetően hatékonyan védhetjük meg cégünket. ■

ALMÁSI ZSOLT SZENIOR RENDSZERMÉRNÖK, TANÚSÍTOTT PALO ALTO NETWORKS OKTATÓ

FORRÁS: CLICO MAGYARORSZÁG

Bolyongás a Tufin piacterén

FORRÁS: THE_FUTURE_OF_COMMERCE.COM

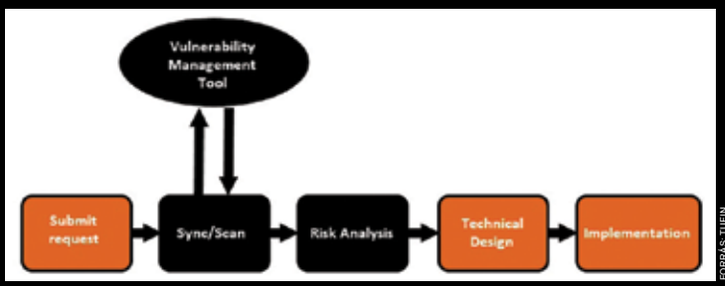
A Tufin Orchestration Suite (TOS) egy három modulból – a SecureTrackből, a SecureChange-ből és a SecureAppból – felépülő, átfogó, szabályrendszer-kezelő megoldás. Ez a három modul biztosítja, hogy a szabályrendszerünk „tiszta” legyen akár vegyes gyártói eszközökből felépített hálózat esetében is, ne legyenek felesleges policy-k, csak olyanok, amelyekre tényleg szükség van. Mindezt úgy, hogy az üzemeltetés közben elvégzett módosítások dokumentálva legyenek és csak olyan módosítások lépjenek életbe, amelyeket már jóváhagytak.

A **SecureTrack** segítségével betekintést nyerhetünk a tűzfalainkon, hálózati eszközeinken lévő szabályrendszerekbe, konfigurációkba, és nyomon követhetjük az ezekben bekövetkező változásokat, valamint kézhez kapjuk az eszközeinket és a köztük lévő kapcsolatokat ábrázoló topológia térképet is. A **SecureChange** modul a házirendek módosításában nyújt nagy segítséget. Tulajdonképpen egy ticketing rendszer, amellyel megterveztethetjük, hogy egy új igény felmerülésekor mely tűzfalakon milyen módosítást kell ahhoz végrehajtani, hogy a kívánt kapcsolat létrejöhessen. De abban is nagy segítséget nyújt, ha a meglévő szabályrendszert szeretnénk felülvizsgálni vagy karbantartani. A **SecureApp** modul pedig az alkalmazásaink működéséhez szükséges kapcsolatok rendelkezésre állását támogatja. Nyomon követi, hogy az alkalmazás elemei és felhasználói, illetve adminisztrátorai közötti kommunikáció átjut-e a köztes tűzfalakon és hálózati eszközökön.

A piactér

– SecureTrack Reporting Essentials (STRE) Ezzel a kiegészítővel könnyen értelmezhető riportokat generálhatunk a SecureTrack által összegyűjtött adatokból. Persze, ez nem azt jelenti, hogy a SecureTrack enélkül nem tud riportokat készíteni. Maga az alapmegoldás is számos riportsablont tartalmaz, így például, ha egy monitorozott eszköz konfigurációjában változás történik, akkor arról nemcsak a dashboardon keresztül értesülhetünk, hanem az új revízió érkezésével párhuzamosan generálódhat egy riport is, amelyet akár ki is küld a rendszer a beállított személyeknek. De készíthetünk riportot a lejárt vagy valamennyi időn belül lejáró szabályainkról is. Aztán készülhet riport a legtöbbet használt vagy legkevésbé használt szabályainkról/objektumainkról.
A SecureTrack Reporting Essentials pedig olyan új riportsablonokat tartalmaz, amelyek magában a SecureTrackben nincsenek benne. Például a segítségével készíthetünk „Shadowed Rules" riportot is, amely összegyűjti azokat a szabályokat, amelyek nem kezelnek forgalmat, ugyanis a sorban valahol előttük már van olyan másik szabály, amelyre illeszkedik a forgalom.
– Vulnerability Mitigation App (VMA) Kulcsrakész integrációt biztosít a Tufin SecureTrack és a széles körben elterjedt sérülékenység-menedzsment alkalmazások – Rapid7 Nexpose, Rapid7 InsightVM, Tenable vagy Qualys – között. A sérülékenység-vizsgáló alkalmazástól kapott sebezhetőségi adatokat a SecureTrack össze tudja vetni a szabályrendszert leíró információkkal, így gyakorlatilag láthatóvá válik, hogy a hálózatunkban fellelhető sérülékeny eszközök elérését melyik tűzfalszabályok teszik lehetővé. Itt már csak annyi a feladatunk (ha a folyamat nem automatizált), hogy a SecureChange segítségével kezdeményezzük az érintett szabályok kiiktatását vagy módosítását. Legalábbis arra az időre, amíg magát a sérülékenységet nem küszöböljük ki.
– **Vulnerability-based Change Automation (VCA)** Ez a Marketplace alkalmazás a SecureChange modult integrálja third party sérülékenység-vizsgáló eszközökkel. A sérülékenység-menedzsmenttől kapott információk felhasználásával az új tűzfal-szabályok létrehozása előtt értesülhetünk arról, ha a szabály olyan forrás vagy cél entitást tartalmaz, amely sebezhető. A SecureChange integráció pedig biztosítja, hogy a SecureChange folyamatokban lévő biztonsági ellenőrzésekkel automatizálni tudjuk a tűzfal-szabályok megnyitása közben elvégzendő kockázat jóváhagyási folyamatot. Ezenkívül a VCA segítségével az érintett SecureChange „Access Request" típusú ticketekhez HTML-jelentéseket hozhatunk létre, amelyek részletes leírást adnak a ticketben szereplő eszközök észlelt sebezhetőségeiről.
– Security Policy Builder (SPB) Az alkalmazás, amely a vállalati access hálózat szegmentációs keretrendszerének kiépítésében és telepítésében segít. A SecureTrackben eddig is rendelkezésünkre álltak a Unified Security Policy (USP) mátrixok, amelyeket arra tudunk felhasználni, hogy „megmondjuk" a SecureTracknek, milyen forgalmakat szeretnénk engedélyezni a hálózatunk egyes logikai egységei (zónái) között. A mátrixokban – több mátrixot is használhatunk – definiálni tudjuk, hogy egy-egy zónapár között melyek azok a forgalmak (például ssh, telnet, icmp stb.), amelyek engedélyezettnek vagy

A TUFIN VULNERABILITY MITIGATION APP (VMA) MŰKÖDÉSE



A TUFIN VULNERABILITY-BASED CHANGE AUTOMATION APP (VCA) MŰKÖDÉSE

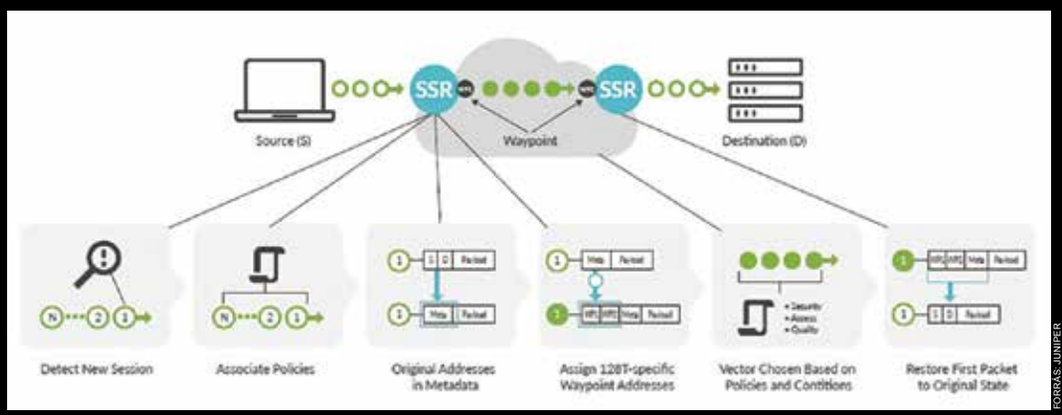
tiltottnak számítanak. A SecureTrack ezeknek az ismereteknek a birtokában folyamatosan vizsgálni tudja a szabályrendszerünket, hogy a meglévő szabályaink eleget tesznek-e ezeknek az elvárásoknak. Vagy esetleg vannak-e olyan rule-ok, amelyek nem kívánt forgalmat is lehetővé tesznek a két zóna között. Ilyen mátrixokat természetesen eddig is tudtunk használni, csak az előállításuk volt nehezebb, ugyanis nekünk kellett „kitalálni", hogyan is kellene a hálózatunknak működnie, hogy az megfeleljen a saját belső elvárásainknak, illetve azoknak a követelményeknek, amelyeket a ránk vonatkozó előírások támasztanak velünk szemben. Majd ezt az információt a SecureTrackkel is meg kellett osztanunk, a régebbi verziókban csv-fájl segítségével, az új verzióban pedig már grafikus módon. Ezekkel szemben az SPB segítségével már arra is van lehetőségünk, hogy az alkalmazás elemezze a kiválasztott zónára vonatkozó szabályainkat, és automatikusan létrehozza az USP mátrixot. A mátrixok rendszeres felülvizsgálatára is szükség van – ebben szintén segítséget nyújt az SPB –, mivel változhatnak az elvárásaink és a ránk vonatkozó szabályzások is, melyeket a szabályrendszerben is követnünk kell, így, ha a mátrix up-to-date, akkor könnyen megtaláljuk, mely szabályokon kell még csiszolnunk, hogy a teljes szabályrendszer is tökéletes legyen.
Listánk messze nem teljes, mondhatni, csak a jéghegy csúcsa. Reméljük, hogy ebből a néhány kiragadott és bemutatott kiegészítőből is kitűnik, hogy egy amúgy jól működő alkalmazáshoz mennyi plusz funkciót lehet adni, amelyek segítenek még emberközelibbé tenni egy alapból is könnyen használható megoldást.

. tufin

Session Smart Router, a hálózat teljesítményének és hatékonyságának lelke

A **Juniper Networks** által nyújtott **Session Smart Router** (SSR-) technológia egy régóta fennálló problémára nyújt újabb megoldást, mégpedig arra, hogy komplex hálózatokban hogyan irányítsuk, titkosítsuk a csomagokat, javítsuk a válaszidőt és biztosítsunk nagyobb sávszélességet.

Az SDN kiterjesztése az SD-WAN, amely egy automatizált és programozható megközelítés a hálózati kapcsolatok kezelésére, használatával a szervezetek egy „okos” hybrid WAN-t tudnak kialakítani, ezzel is csökkentve a hálózat üzemeltetésének költségeit. Egy nagyvállalati IP VPN-ből, szélessávú internetből és vezeték nélküli szolgáltatásokból álló SD-WAN használatával az alkalmazások költséghatékonyan kezelhetővé válnak, különösképp a felhőben. A forgalom automatikusan és dinamikusan kerül továbbításra a legmegfelelőbb és leghatékonyabb WAN-útvonalon a hálózat állapota, az alkalmazások biztonsága és a szolgáltatásminőség (QoS) követelményei, valamint a hálózati költségek figyelembevétele alapján.
Az SD-WAN koncepció esetén ügyféloldali végberendezéseken (CPE-ken) futó SD-WAN szoftver figyeli az összes nyilvános és privátvonal szolgáltatás állapotát, és határozza meg az egyes alkalmazástípusok forgalmának irányítását. Például alapértelmezetten Voice-over-IP (VoIP) forgalom esetén MPLS VPN-szolgáltatás használata



FORRÁS: JUNIPER

AZ ELSŐ CSOMAG SESSION ALAPÚ FELDOLGOZÁSA

definiált, azonban az MPLS-kapcsolat túlterhelődése esetén az SD-WAN átirányíthatja a forgalmat egy széles sávú internetre vagy 4G LTE vezeték nélküli kapcsolatra. Ezáltal SD-WAN használatával az automatikus terheléselosztás is megvalósítható a hálózati torlódások, a legjobb teljesítmény és a legolcsóbb útválasztás érdekében.
Az SD-WAN mint koncepció sok gyártó kínálatában szerepel, a mai megoldások többsége hagyományos tunneles megközelítésen alapszik. Ezért azt kell felismerni, hogy miközben egy IPSEC-tunnel fejlécekkel bővített csomagokat mozgat, rengeteg értékes sávszélességet emészt fel, ezzel is csökkentve az alkalmazások teljesítményét. Arról nem beszélve, hogy a tunnel használata miatt olyan fontos telemetria-adatok, mint a késleltetés vagy a csomagvesztés mindössze tunnel szinten lesznek láthatók.
A **Juniper** válasza egy mesterséges intelligencián alapuló, munkamenet központú megközelítés Úgy kell elképzelni a gyakorlatban, hogy például videóhívás esetén minden egyes videóhívás késleltetését, csomagvesztését külön-külön is látjuk. Arról nem beszélve, hogy amennyiben az elvárt SLA-szintet az adott kapcsolat nem tudja garantálni, úgy a sessiont azonnal átirányítják egy alkalmasabb linkre. Mindezt megfejelve, a mesterséges intelligencia lehetővé teszi anomáliák észlelését is, ezzel is segítve a hálózat üzemeltetőit a kiemelkedő ügyfélélmény biztosításában. Ráadásul a Juniper megoldása nem használ tunneleket sem, így a rendelkezésre álló sávszélesség gyakorlatilag teljes egészében felhasználható a „normál csomagok” továbbítására. Csupán az egyes sessionök első csomagjaiba kerül be némi metaadat, amelyeket a két végpont közötti útvonal létrehozására használunk fel, majd a többi, ugyanehhez a forgalomhoz tartozó csomagot a már kitaposott ösvényen küldjük el.
Mi a helyzet a titkosítással? A megoldás úgynevezett adaptív titkosítást használ, amely alapján a már eleve titkosított csomagokat – ha azok megfelelnek egy bizonyos titkosítási szintnek – felesleges még egyszer „becsomagolni”, így kiküszöbölhetjük a kettős titkosításból adódó többletterhelést.
A mai hálózatoknak képeseknek kell lenniük arra, hogy az üzlet számára szükséges alkalmazásokat és szolgáltatásokat akkor és ott nyújtsák, amikor és ahol azokra szükség van. Ennek teljesítéséhez olyan alkalmazások, routerek és szolgáltatások szükségesek, amelyek „értenek a munkamenetek nyelvén”, amire a legtöbb hálózat képtelen. Mint kiderült, ez a nyelvi hiányosság az alapvető oka számos, jelenleg nem megfelelően működő dolognak a hálózatkezelésben. A Juniper Session Smart Routing megoldása pedig éppen ezt kezeli. ■

Juniper NETWORKS

Miért válasszunk XDR-gyártótól adatkezelő platformot?

Ha követjük a különböző piaci trendeket, egyre inkább az látszik, hogy minden IT-biztonsági gyártó arra törekszik, hogy legyen egy robusztus és több lábon álló XDR-megoldása. A különböző platformok sokszor igencsak eltérő „történelmi” gyökerekkel rendelkeznek, ezért a megoldásoknak is eltérőek az erős pontjaik. A Gartner és más elemző cégek miatt egyre nagyobb a nyomás ezeken a gyártókon, hogy a fejlesztések során a hiányzó vagy kívánt funkciókról is gondoskodjanak, vagy felvásárlások, esetleg integrációk útján illesszék be a platform képességei közé.

Ahogy a nevük is mutatja, az XDR- (eXtended Detection and Response) megoldásoknak kiterjedt és több irányból támogatott megoldásként kell létezniük. A legtöbb esetben a végpontvédelmi irányból indultak, a korábban EPP- és EDR-megoldásoknak hívott termékekből alakultak ki, és mára különböző extra képességeket kaptak a végpontvédelem mellé.

A legsűrűbben említett XDR-funkció a hálózati forgalomelemzés (NDR), de legalább ennyire fontos, hogy a különböző forrásokból megszerzett információkat rendezetten és kezelhető formában tároljuk, képesek legyünk hatékonyan keresni bennük, és ne jelentsen problémát az se, ha az adatok mennyisége akár hirtelen és drasztikusan növekszik. Ezért fontos, hogy a választott megoldásnak legyen egy robusztus adatkezelő háttere, amely óriási mennyiségű naplóbejegyzést képes feldolgozni.

FORRÁS: 123RF.COM

A **SentinelOne** platformja is rendelkezik ilyen pillérrel, amelyet az XDR-megoldás használ, legtöbbször elrejtve a szemünk elől. Ellentétben a többi piacon lévő megoldással, ezt a „sima” felhasználók számára is elérhetővé tették **DataSet** néven. Ez gyakorlatilag egy cloud-natív felhős adatplatformot takar.

A DataSet leginkább a „data lake” termékekhez hasonlítható a logkezelő megoldások közül. Képes akár napi több terabájt adatot is fogadni, mindezt a lehető leghatékonyabb módon kezelve, és ezzel egyszerre sikerült gyors, skálázható és költséghatékony megoldást alkotni. A korábban létező SIEM-megoldásokkal szemben itt nem jelent problémát az se, ha a legkülönbözőbb adatforrásokból folyamatosan nagy mennyiségű adat árad a tárhelyünkbe, ilyenkor is megtartja a gyorsaságát és feldolgozóképességét. Az egyedi architektúrának köszönhetően az adatok folyamatosan elérhetők, nem kell a különböző tárhelyszintek között mozgatni azokat, így nincs felesleges várakozási idő, ezért a legkülönfélébb felhasználási módok esetén is hatékonyan tud működni, legyen az akár adatvizualizálás, akár egyedi, kifinomult keresések. Szintén az egyedi architektúrához tartozik, hogy az adattárolás és az ezeken végzett analitikai műveletek skálázása egymástól teljesen függetlenül történik az igényeinknek megfelelően.

A legtöbb cég életében általában elég érzékeny pontnak számít a különféle naplók tárolása, ezért fontos megemlíteni, hogy az ide beküldött naplók és bejegyzések végig titkosítva haladnak a hálózaton, illetve a tárolásuk is magas fokú titkosítással történik. A biztonsági előnyök közé tartozik továbbá, hogy az általunk gyűjtött adat végig a miénk, tehát az irányítás a mi kezünkben marad.

A biztonsági előnyökön kívül legalább ennyire fontos az is, hogy a hagyományos SIEM és sima loggyűjtő megoldásokkal szemben a DataSet használata és üzemeltetése közben nem szükséges sok üzemeltetői energiát ráfordítanunk, mivel akár teljesen SaaS-felépítésben is elérhető.

Az a tény, hogy egy vezető XDR-gyártó a saját megoldása mögött is ezt a rendszert használja, már önmagában is elég meggyőző, viszont a különböző lehetőségeket közelebbről megvizsgálva még inkább egyértelművé válik, hogy ha nagy mennyiségű naplóbejegyzést kell tárolnunk, illetve feldolgoznunk a legkülönfélébb módokon, akkor a DataSet lehet a jelenleg elérhető egyik legjobb megoldás az ügyfelek számára. ■

SentinelOne™

Nagyvállalati Out-of-Band megoldások az Opengear kínálatában

Az IT-szegmensben egyre inkább teret nyer a virtualizáció, a felhős alkalmazások, az IoT-eszközök használata, a hálózat soha nem látott mértékben válik bonyolulttá és kezelhetetlenné. Értelemszerűen ezen fejlesztések szükségességét senki sem kérdőjelezi meg, de ezzel párhuzamosan nagyobb valószínűséggel fordulhatnak elő kimaradások is.

Napjaink trendjei, a távmunka, a virtualizáció, elősegítik az agilis üzleti működést, de növelik a szervezet kitettségét az esetleges meghibásodásokkal, támadásokkal szemben. Egyre többször hallani olyan, nem várt eseményekről, amelyek valamilyen negatív, rosszindulatú külső hatás miatt következnek be és okoznak – jobb esetben „csak” – kellemetlen perceket az üzemeltetőknek. Elég pusztán egy ütemezett firmware-frissítésre gondolnunk, amely nem az előre definiált forgatókönyv szerint zajlott le, és elvesztettük a kapcsolatot az eszközzel.

Miért történnek leállások?

A szervezetek az informatikai érettségüknek megfelelően egyre több és összetettebb réteggel bővítik a hálózataikat, ami gyakran számtalan sebezhetőséget eredményez. Napjainkban sok olyan tényezővel találkozunk, amelyek hálózat- vagy rendszerkimaradást okozhatnak – kezdve az internetszolgáltatói problémáktól, az optikai szálak megszakításán át egészen az egyszerű emberi mulasztásokig. Ráadásul a hálózati eszközök is egyre bonyolultabbá válnak. Az eszközökön futó szoftvereket gyakrabban kell frissíteni, ezáltal a hálózati biztonság egyre nehezebben tartható fenn.

FORRÁS: 123RF.COM

Kiberbűnözők támadhatnak, akik célzottan a gyenge és sérülékeny pontokra fókuszálnak, hogy bejussanak a vállalati hálózatokba – de maguk a felhasználók is egyre nagyobb kockázatot jelentenek.

Ha már megtörtént a baj

A „hálózati reziliencia/rugalmasság” mindenki számára egy kicsit mást jelent, de alapvetően az állásidő minimalizálására való törekvést értjük alatta, illetve azt, hogy hálózati hiba esetén bárhonnan elérhetjük az eszközeinket, és a problémát távolról is orvosolhatjuk. Az a valós cél, hogy minden eszközhöz hozzáférjünk, bárhol is helyezkedjen el a hálózaton. Ez többek közt arra is lehetőséget biztosít, hogy bármikor feltérképezzük a hálózat online és offline eszközeit is. A tradicionális eszközmenedzsment viszont legtöbb esetben magát a helyi hálózatot használja kommunikációs csatornaként – ezért hálózati üzemzavar esetén nem tudunk hibát javítani.

A helyzet sokszor egy gyors újraindítással megoldható, de amikor ez már nem elég, akkor értelmet kap az Out-of-Band menedzsment. Az **Opengear Out-of-Band menedzsment** segítségével külön kommunikációs síkot valósítunk meg az eszközkezelés számára, amelyet nem befolyásol a hálózat állapota, ez kiemelkedő jelentőséget kaphat egy esetleges kibertámadás esetén is. A távoli eszközök egyszerűen konfigurálhatóak anélkül, hogy bárkinek a helyszínre kellene utaznia. Ez manapság a pandémiás korlátozások kapcsán kiemelten fontos jelentőséggel bír. Amennyiben a leállással együtt az internetelérés is megszűnik, akkor a hálózati rezilienciát az Out-of-Band megoldásba integrált mobil átjárón keresztül lehet megvalósítani.

Több telephelyes környezet esetén további Out-of-Band eszközökre van szükség, amelyek kezelését szintén meg kell oldani. Ebben az esetben az **Opengear Lighthouse** központi menedzsmentszoftver segítségével egy konszolidált, biztonságos felügyeleti pontot tudunk kialakítani a teljes sávon kívüli infrastruktúrához, ezzel biztosítva, hogy további erőforrások bevonása nélkül is garantálni lehessen az átláthatóságot.

Természetesen az ilyen szintű reziliencia kialakítása extra költségekkel jár, de a megtérülése jelentősen meghaladhatja a befektetéssel járó kiadásokat. Érdemes azt is figyelembe venni, hogy a reziliencia kiépítése általában alacsonyabb invesztícióval jár, mint egy teljesen redundáns, esetleg geo-redundáns környezet kialakítása. ■

opengear
A DIGI COMPANY

Mit adhat nekünk egy CTI-platform?

Az IT-biztonsági megoldások között mindig találunk felkapott területeket. Az egyik ilyen aktuális téma a CTI, avagy a kiberhírszerzési platformok területe. Mostanában az aktuális történések miatt sajnos tényleg egyre nagyobb prioritást kell kapnia annak, hogy egy támadást képesek legyünk megelőzni vagy legalábbis a hatásait csökkenteni.

Egyre fontosabb, hogy az iparágunk ellen indított támadásokról hírt szerezzünk, és ha lehetséges, képesek legyünk reagálni is, illetve ne csak a biztonsági rendszereink gyártóira hagyatkozzunk. Az információk megszerzése ugyan első körben nem tűnik nehéz feladatnak, különböző Twitter- és Telegram-adatfolyamokat, illetve híroldalakat figyelve akár azt is hihetnénk, hogy ezt cégen belül is meg lehet oldani. A problémák akkor kezdődnek, amikor ezeket az információkat rendszerezni szeretnénk, illetve ha nem csak a felszínt kapargatva publikus forrásokból dolgoznánk.

Egy komoly CTI-platform, mint például a **Recorded Future,** több millió forrásból dolgozik, és mindezt automatizálva teszi. Ezek a források az előbb említett egyszerűen követhető nyílt adatfolyamokon kívül különböző zárt Telegram, IRC és egyéb chat-szobákon át a dark, illetve deep web legkülönfélébb, tipikusan hackerek és bűnözők fórumaira és honlapjaira is kiterjednek. Ha esetleg olyan információkkal találkozik a rendszer, amelyeket az automatizmusok nem tudnak kezelni, akkor kiegészítik a gépek képességeit az elemzők szakértelmével.

Az adatok gyűjtésén és rendszerezésén kívül felmerülhet a kérdés, hogy vajon mire képesek ezek a rendszerek és miért van rájuk szükség. Itt fontos megjegyezni, hogy a legtöbb CTI-megoldás különféle modulokat kínál számunkra. Ezt úgy kell elképzelni, hogy ha nekünk csak egy adott célra szükséges a megoldás, akkor kapunk előre megírt szűréseket és ezekkel tudunk hatékonyan dolgozni. Elég csak a legfontosabb használati példáknál maradni, mint a céges márka védelme, az általunk használt rendszerek sérülékenységeinek felderítése, ellopott kártya vagy hozzáférési adatokról történő riasztások. Gondoljunk csak bele, mennyivel egyszerűbb lenne a dolgunk, ha nem manuálisan kellene keresnünk a különböző forrásként használt oldalakat. Ellenkezőleg, a megoldás képes előre definiált listák alapján riasztani, például ha a cégünket érintő adathalász-támadást látnak az interneten, vagy esetleg a céges márkanevünkkel szeretne valaki visszaélni egy célzott támadással.

Megkülönböztető érték

A Recorded Future-nél dolgozó elemzők többsége korábban komoly hírszerző szerveknél tevékenykedett, ezért sokszor észrevesznek mások számára nem egyértelmű összefüggéseket, és találnak olyan nyomokat, amelyeket a gépek nem tudnak feldolgozni.

FORRÁS: 123RF.COM

Amellett, hogy a rendszer helyettünk őrködik, és ezért nekünk elég egy központi felületet figyelnünk, lehetőséget ad arra is, hogy az integrációknak köszönhetően a külsős rendszerünkbe is kapjunk riasztást. Ha már az integrációknál tartunk, akkor IT-biztonsági szempontból legalább ennyire fontos, hogy a különféle forrásból származó információhalmazok sokszor tartalmaznak olyan adatokat (például IP-címeket, hash-értékeket vagy domaineket), amelyeket a védelmi rendszereinkbe implementálva még hatékonyabban védhetjük meg a szervezetünket.

Az előbb felsorolt példákon kívül több más eszközt is kapunk a kezünkbe, ilyen például a geopolitikai információkhoz való hozzáférés. Ennek segítségével a számunkra érdekes földrajzi területeket, helyszíneket is figyelhetjük, és akár fizikai támadások, tüntetések esetén riasztani tudjuk a kollégákat vagy életbe tudjuk léptetni a megfelelő biztonsági eljárásokat az adott területen lévő irodával kapcsolatosan.

Az talán ebből a rövid cikkből is látszik, hogy a különféle információk felhasználási módjai gyakorlatilag csak a cégünktől és az igényeinktől függnek, ezért egy biztonságtudatos cég számára erősen ajánlott például egy Recorded Future hozzáférés beszerzése. ■

Recorded Future®

Mikroszegmentáció és Zero Trust

FORRÁS: ZEROUNO.COM

Hatalmas fejlődésen mentek keresztül a határvédelmi eszközök az elmúlt években. De tisztában kell lennünk azzal, hogy a határvédelem önmagában nem elegendő. Ha egy támadó valamilyen módon bejut a hálózatunkba vagy már eleve ott van, akkor a hálózaton belüli mozgását nem tudjuk a határvédelmi eszközeinkkel megakadályozni. Erre a problémára jelent hatékony megoldást a mikroszegmentáció.

A mikroszegmentálással gyakran az egyik végletből szeretnénk a másikba eljutni, vagyis a „hálózaton belül minden kommunikáció megengedett” felfogást szeretnénk lecserélni arra a módszerre, ahol a hálózat belsejében is a periméter-infrastruktúrához hasonló tűzfalszabály-készletet használunk. Ennek a megvalósítása gondos tervezést igényel, ugyanis a célunk az, hogy olyan hálózatot hozzunk létre, amely a támadók számára nehézkesen használható, de számunkra könnyen kezelhető lesz.

Mi szükséges a jó mikroszegmentáláshoz?

– Láthatóság az alkalmazások kontextusaiban: a szervezetek a vállalkozásuk működéséhez számos alkalmazást futtatnak. Ezek az alkalmazások kommunikálnak és adatokat osztanak meg egymással. De vajon tisztában vagyunk vele, hogy ez hogyan történik? Sokszor sajnos nem. A hálózatért felelős csapat szinte biztos, hogy nem ismeri ezeket a folyamatokat, de talán még a hálózatbiztonságért felelős csapat sem. Talán az alkalmazásfejlesztők tudják, de ők sem mindig. Ha mégis, akkor pedig ennek a biztonsági problémáit nem látják át.

– Skálázható architektúra: magát a mikroszegmentációt többféleképpen is megvalósíthatjuk. Amit minden esetben figyelembe kell venni, az a bővíthetőség, a megoldás hatékonysága és ár/érték aránya. Szegmentálhatunk *a hálózat* segítségével, amikor az egyes hálózati eszközökön ACL-eket használunk. Működni ugyan fog a megoldás, viszont nem lesz túl hatékony, ugyanis a hálózat alapvető célja, hogy a lehető leggyorsabban szállítsuk a csomagokat A pontból B pontba, ehhez képest gyakorlatilag minden egyes csomagot megállítunk minden egyes csomópontban, hogy eldöntsük róla, mehet vagy sem.
Szegmentálhatunk *SDN segítségével,* ahol némi automatizmust tudunk a konfigurálásba csempészni, de gya-

korlatilag hasonló hatást érünk el, mint a hálózati szegmentáció esetében. Használhatunk *hoszt alapú* mikroszegmentációt is. Ez egy másfajta megközelítés. Ebben az esetben a hosztok beépített tűzfalain kényszerítjük ki a szabályokat. Mivel a hálózat széle nem a külső tűzfalnál van, hanem a belső szegmenseknél, így minél kisebbek a szegmensek, annál jobb a védelem. Ha tovább görgetjük ezt az ötletet, akkor hamar rájövünk, hogy az egy elemből álló szegmens a legjobb, így gyakorlatilag a workload lesz az új perimeter. Tehát a forgalom engedélyezése vagy tiltása magán a workloadon történik. A hoszt-alapú rendszerek pontosan így működnek.

– Absztrakt biztonsági szabályok: a hagyományos megközelítés alapján hálózatbiztonságról beszélünk, ami azt jelenti, hogy a hálózatot és a biztonságot összedrótozzuk egymással, de ha belegondolunk, akkor a két „összetevőnek" egymással ellentétes céljai vannak. A hálózat a sebességről és az áteresztőképességről szól, míg a biztonság az elszigetelésről és a megelőzésről. Igen, így szoktuk használni, de mi lenne, ha nem így csinálnánk?

– Részletes kontrollálás: mivel üzleti szempontból eltérő kritikusságú alkalmazásokkal rendelkezünk, így fontos, hogy a biztonsági követelményeket is ezeknek megfelelően tudjuk szabályozni. Néha elegendő, ha a különböző környezeteket elszeparáljuk egymástól (például a fejlesztést elkülönítjük a termeléstől). De akár az is előfordulhat, hogy a különböző alkalmazásszinteket (web, feldolgozás, adatbázis) kell egymástól elválasztanunk, és azt kell szabályoznunk, hogy melyik szint melyik másik szinttel kommunikálhat.

Segít az Illumio!

A fenti ötletek egyszerűen megvalósíthatók az **Illumio Core** megoldással. Az Illumio úttörő és egyben piacvezető is a Zero Trust szegmentáció területén. A céljuk, hogy megakadályozzák a kibertámadások és zsarolóvírusok alkalmazások, tárolók, felhős környezetek, adatközpontok és végpontok közötti terjedését. Nézzük meg részletesebben, hogyan felel meg az Illumio a mikroszegmentálás megvalósításához kapcsolódó feltételeknek!

Láthatóság az alkalmazások kontextusaiban: az Illumio valós idejű alkalmazásfüggőségi térképe világosan megmutatja, hogyan lépnek egymással kölcsönhatásba és hogyan kommunikálnak egymással a különböző alkalmazáskomponensek. Ez az „Illumination" néven ismert térkép nemcsak páratlan átláthatóságot biztosít, hanem meghatározott részletességű irányelveket is ajánl. Az egyes szabályokat közérthető címkék határozzák meg, amihez nincs szükség hálózat rétegbeli (L3) információkra (például IP-címre).

Skálázható architektúra: az Illumio hamar felismerte, hogy a granuláris mikroszegmentáció elérésének egyetlen skálázható módja a hoszt-alapú architektúra. Ez a fajta megközelítés helybe hozza a biztonságot, és az ellenőrzéseket a hálózattól függetlenül végezhetjük el. Ezzel a megoldással kiküszöbölhetjük az olyan torlódási pontokat is, amilyeneket a tűzfalak és hálózati eszközök jelenthetnek.

Absztrakt biztonsági szabályok: az Illumio megoldásával a szegmentálást függetlenítjük a hálózattól, ennek segítségével könnyen érthető, címkéken alapuló házirendeket hozhatunk létre. Az egyes workloadokat a címkék négy dimenziójával tudjuk jellemezni (role/application/environment/location) és a szabályokat ezeknek a címkéknek a felhasználásával írjuk meg. Mielőtt az egyes szabályokat érvényre juttatnánk, arra is van lehetőségünk, hogy letesztelük, milyen hatással lesz a forgalomra az adott szabály. Ezzel biztosíthatjuk, hogy a mikroszegmentálás az alkalmazások tönkretétele nélkül valósuljon meg.

Részletes kontrollálás: az Illumio házirendmodellje egyszerű, könnyen használható, mégis hatékony megoldást kínál. Az alkalmazásfüggőségi térkép nemcsak az alkalmazásréteg átláthatóságát biztosítja, hanem különböző opciókat felkínálva támogatja az egyes házirendek létrehozását is.

Ezeken felül a megoldás hely- és workload-független, ami annyit jelent, hogy az egyes workloadok bárhol elhelyezkedhetnek a hálózaton belül, illetve, ha mozgatjuk azokat, akkor a rájuk vonatkozó szabályokra például nem lesz hatással egy esetleges IP-cím változás, így a szabály továbbra is érvényes marad. API-alapú megoldásként könnyen integrálható a szervezet nagyobb ökoszisztémájába is.

A mikroszegmentáció nagyon hatékony megközelítés jogosulatlan oldalirányú mozgások megakadályozására a szervezeten belül, nem véletlen, hogy a Zero Trust keretrendszer egyik legfontosabb alapelvévé vált. A legtöbb nagy horderejű hálózati betörés azért hat súlyosan a szervezetekre, mert a támadó akár heteken keresztül mozoghat észrevétlenül a hálózaton belül, és eszközről-eszközre haladva férhet hozzá a legértékesebb erőforrásainkhoz. A mikroszegmentálással megelőzhetjük ezt a fajta támadást, így elkerülhető, hogy az Önök cége legyen a következő áldozat. ■

illumio

XDR és saját CTI-szolgáltatás a Rapid7-től

A digitális transzformáció és a vele járó növekvő felhőhasználat, a terjedő otthoni munkavégzés gyökeresen átalakítja az informatikai struktúrákat, és új kihívások elé állítja az IT-biztonsági csapatokat. Azáltal, hogy az informatikai rendszerek egyre jobban eloszlanak, és a szervezetek telephelyein kívül egyre nagyobb számban működnek szolgáltatói adatközpontokban és felhőszolgáltatások keretében (privát és nyilvános felhőben is), valamint a végpontok jelentős része home office-ból éri el az erőforrásokat, számos tradicionális megoldás megy jelentős változáson keresztül.

FOKI TAMÁS
SZENIOR RENDSZERMÉRNÖK

FORRÁS: CLICO MAGYARORSZÁG

Ilyen változó termékkategória a SIEM- (security information and event management) rendszereké. A Gartner tanulmányai alapján a modern SIEM funkcionalitása jelentősen kibővült, nem elég már a hagyományos biztonsági logok gyűjtése és a bennük való keresésekkel és korrelációkkal riasztások generálása. Elvárt, hogy a végponti eszközök logjai is elérhetők legyenek, és a SIEM-megoldás rendelkezzen viselkedés-analitikai funkcióval ahhoz, hogy teljesebb képet kapjon a hálózati forgalomról és a kapcsolatokról. Nem elég csak a tűzfal logokra támaszkodni, mert akkor egy adott szegmensen belüli forgalomról nem lesznek adataink, tehát valamilyen hálózatforgalom-analitikai (network traffic analyzer, NTA) eszközre is szükségünk lesz, amely például egy hálózati switchen a kitükrözött teljes hálózati forgalmat képes elemezni.

Szabályok és csapdák

A **Rapid7 InsightIDR** megoldását mindezek figyelembevételével alakították ki és fejlesztik folyamatosan. A legkülönbözőbb biztonsági eszközökből érkező logokon kívül rendelkezik egy agenttel, amely a végponti logok gyűjtése mellett a végponti beavatkozások lehetőségét is megteremti.
A megoldás része egy NTA, továbbá egy erős viselkedésanalitikai motor is, amely a felhasználói viselkedésen kívül a logok és a hálózati forgalom elemzésével úgynevezett „támadó viselkedés-analitikát" is végez, rosszindulatú tevékenységet észlelve pedig riaszt. Mivel a Gartner ajánlásában szereplő deception-megoldás (csali- vagy honeypot- „mézesbödön" rendszer) is elvárás egy modern SIEM-rendszertől, ezért természetesen saját honeypotok kialakítására is van lehetőség, továbbá létrehozhatunk csali felhasználókat, fájlokat, vagy az InsightAgent segítségével akár hamis azonosító információkat is helyezhetünk az eszközök memóriájába, amelyek használatát észlelve a rendszer riasztásokat generálhat.
A megoldás alapból ismeri több száz biztonsági gyártó logjait, ezekre előre megírt és a gyártó által folyamatos bővített és karbantartott korrelációs szabályok tartoznak, ami jelentősen leegyszerűsíti és gyorsítja a bevezetést. A különböző modulok által keletkezett riasztásokat a MITRE-keretrendszert használva jeleníti meg, és a logokhoz biztosított erős keresési funkciókkal segítve hatékony nyomozásokat tesz lehetővé.
Látható tehát, hogy az InsightIDR a fejlett EDR- (endpoint detection and response), NDR- (network detection and response), UEBA- (user and entity behaviour analytics) funkciók miatt, valamint amiatt, hogy a különböző modulok által észlelt eseményeket és riasztásokat a MITRE-keretrendszert használva jeleníti meg és a logokhoz biztosított erős keresési funkciókkal segítve hatékony nyomozásokat tesz lehetővé, teljes joggal nevezhető teljes körű XDR- (Extended Detection and Response) rendszernek.
Az InsightIDR egy felhős platform, így nincsenek jelentős infrastruktúra igények, nincsenek upgrade problémák, „Pay as You Grow" alapon licencelődik, tehát a menet közben növekvő igények nem okoznak folyamatos hardveres bővítési kényszert a felhasználónál. Valamint a Rapid7 Insight

FORRÁS: 123RF.COM

Platformja lévén a gyártó más termékeivel könnyen integrálható, például az InsightConnect nevű SOAR-megoldással, melynek segítségével a beépített automatizmusok mellett szabadon lehet egyedi automatizálási folyamatokat létrehozni.

Mindent is megfigyel

Egy másik fontos integráció a Rapid7 frissen vásárolt saját CTI-rendszerével, a Threat Commanddal hozható létre. De mi is az a CTI? Az angol „cyber threat intelligence" kifejezést magyarul kiberhírszerzési szolgáltatásnak szoktuk hívni. Ezt a szolgáltatást az az igény hozta létre, hogy a szervezetek által használt biztonsági eszközök „figyelme" jellemzően csak a saját környezetükre terjed ki, és nem képesek kezelni az olyan támadásokat, amelyek ezen kívül esnek.
Korábban csak a legnagyobb szervezetek engedhettek meg maguknak ilyen, jelentős személyi és tudásbeli erőforrást igénylő szolgáltatást. Egy ideje viszont megjelentek az üzleti CTI-szolgáltatást nyújtó rendszerek, amelyek bármelyik vállalat, szervezet számára elérhetőek. A **Rapid7 Threat Command** szolgáltatása is – a többi CTI-vendorhoz hasonlóan – több száz forrásból érkező információt, OSINT- (open source inteligence), Social Media Intelligence forrásokból, publikus nyílt és dark webes fórumokat, IRC-csatornákat, malware repository-kat, illegális internetes aukciós forrásokat, alkalmazásboltokat monitoroznak, ezernyi nyílt, dark, deep webes keresést futtatnak, valamint saját elemzői csapatukra támaszkodva számos nem publikus forrásból is képesek információkat szerezni. Ezt a hatalmas adatmennyiséget elemzik automatikus gépi tanulással, valamint mesterséges intelligenciát is használó, saját fejlesztésű adatbányászati módszerekkel, és természetesen saját szakértői gárdájukkal. Az így létrejött átfogó, kontextusba helyezett és könnyebben felhasználható adatokból képesek közel valós időben riasztást adni az ügyfél digitális jelenlétét célzó akciókról (többek között adatszivárgások észleléséről, márkavédelemről, vezető tisztségviselők hamisított social media profiljairól, hamisított és kártékony kóddal fertőzött alkalmazásokról és weboldalakról, a szervezetet érintő adathalász kísérletekről, ellopott hitelesítési adatokról stb.)
A Threat Command nemcsak intuitív módon használható, könnyen átlátható felületen figyelmeztet, hanem részletes magyarázatokat ad az adott támadás pontosabb megértéséhez, javaslatokat tesz azok elhárítására és menedzselt szolgáltatásokat biztosítva aktívan segít is a megoldásban. Kérdés esetén a cég szakértői bármikor (24×365 szinten) elérhetőek, és segíteni tudnak például a social media profilok letiltásában vagy a kártékony, hamisított alkalmazások alkalmazásboltból való eltávolításában is.
Az Insight Platform integráció révén a Threat Commandból érkező információk közvetlenül felhasználhatók. A Threat Commandba érkező riasztások az InsightConnect révén már automatizáltan a megfelelő csapathoz kerülhetnek és szabadon szerkeszthető incidens-reagálási folyamatokat indíthatnak be, ezzel gyorsítva és egyszerűsítve a csoportok munkáját. ■

CLICO

MAGYARORSZÁGI PORTFÓLIÓ:

ARISTA

ARMIS

COMMSCOPE® RUCKUS®

cryptme

Cryptshare®

CYBERARK®

DIGI

Fidelis Cybersecurity

Forcepoint

FORESCOUT

GREYCORTEX Security for Professionals

imperva

Infinera

IronNet

ivanti

JUNIPER driven by Mist AI

MICROSENS euromicron group

CIPHER AN ENTRUST DATACARD COMPANY

opengear A DIGI COMPANY

paloalto® NETWORKS

radware

RAPID7

Recorded Future®

rubrik

SailPoint

SentinelOne™

THALES

tufin

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

ITBUSINESS PODCAST

Stúdióminőségben rögzített beszélgetések
Portrék, interjúk
Stúdióbeszélgetések
Élő podcast felvételek

Műsorvezető:

Mester Sándor

Letölthetők, streamelhetők:

Platina szponzor

IBM

INTER COMPUTER CSOPORT

Arany szponzor

CLICO paloalto CYFIRMA EXCLUSIVE NETWORKS LSK HUNGÁRIA PRIANTO solarwinds sch schönherz TOPdesk

Szakmai támogató

mVISZ

Ezüst szponzor

ASPECTIS autsoft brightidea.hu DELL Technologies grape PORION Progress Flowmon shiwaforce sealpath

Bronz szponzor

Szakmai partner

HT SYSTEMS PROJECTCOACH Qualysoft Quattrosoft