190 MILLIÓ 5G-S ELŐFIZETÉS IS LEHET AZ ÉV VÉGÉRE

Egyre sürgetőbb a generációváltás

FORRÁS: BLOGS.WINDRIVER.COM

Orvosi konzultációk, ultrahangos vizsgálatok, egészségügyi felszerelést szállító automata járművek – többek között ezekre a feladatokra használták az 5G technológiát a koronavírus-járvány során több országban is. Az év végére 190 millióan fizethetnek elő az újgenerációs mobilszolgáltatásra, ami akár 140 milliárd eurós pluszt is jelenthet az EU GDP-jében.

Három nap alatt építettek új mobilhálózatot a kínai szükségkórházakban a Huawei 5G-eszközeivel

Évek óta napirenden van az ötödik generációs mobilhálózatok kiépítése, és főleg az a kérdés, hogy milyen hozzáadott értékkel bírnak majd az új rendszerek az egyéni és üzleti felhasználók, illetve az intézmények és kormányok számára. Korábban az ITBUSINESS-ben is többször írtunk arról, hogy az egyes piaci szereplők milyen felhasználási lehetőségeket látnak az 5G-ben, például a távgyógyítást, a legújabb ipari forradalmat, vagy a közlekedés átalakítását. Idén a koronavírus-járványban aztán a gyakorlatban is megtapasztalhatta a világ, hogy többek között mire lesz majd jó az újgenerációs hálózat. Szinte mindenki megélte az elmúlt hónapokban, mennyire fontos egy stabil, nagy le- és feltöltési sebességet kínáló, megbízható kommunikációs hálózat.

A Huawei számolt be arról, hogy a vállalat 5G-megoldásai a koronavírus-járvány miatt is felértékelődtek, a mobil technológiát többek között bevetették Olaszországban, Svájcban és természetesen Kínában is. Jellemző felhasználási terület volt a távorvoslás – az orvosi konzultációk, a konkrét vizsgálatok, például ultrahangos vizsgálat elvégzésében és a robotok (a kórház területén gyógyszereket és ételt szállító önjáró kocsik) távoli vezérlésében is segített az új technológia. A Huawei 5G-eszközeivel három nap alatt ki tudták építeni az új mobilhálózatot azokban a frissen létrehozott, kínai szükségkórházakban, ahol a vezetékes internet létrehozása minimum hetekig tartott volna. De nem csak az orvoslás, hanem a digitális oktatás és a távmunka területén is berobbant az 5G, és egészen biztos, hogy a következő években az utóbbi hónapokban szerzett tapasztalatokat a gazdaság számos területén alkalmazzák majd.

Verseny és veszteségek

Bár az 5G előfizetések növekedése a COVID-19 járvány hatására egyes piacokon lelassult, ezt ellensúlyozta a más területeken tapasztalt fellendülés, aminek eredményeként az Ericsson felfelé korrigálta az ilyen típusú előfizetések 2020 végi számára vonatkozó prognózisát. A társaság legújabb prognózisa alapján az év végére világszerte 190 millió 5G előfizetés lehet, 2025 végéig pedig 2,8 milliárdra nőhet ez a szám.

Ahhoz persze, hogy ennyien használhassák az újgenerációs mobilhálózatot, hatalmas infrastruktúra fejlesztésekre is szükség van. Ugyanakkor az is látszik, hogy a csak az Európai Unióban megvalósuló több százmilliárd eurónyi beruházás kapcsán nagyon kiélezett verseny várható a hálózati megoldásszállítók között.

A Huawei július végén adott ki egy elemzést, eszerint az Európában működő 39, aktív 5G hálózatból 28 épül a cég eszközeire, míg globális szinten 87-ből 55. Az Egyesült Államok és Kína közötti kereskedelmi háború ugyanakkor érzékenyen érinti a rádió-hozzáférési hálózatok (RAN) piacán 31 százalékos részesedéssel bíró vállalatot, hiszen az amerikaiak erősen lobbiznak azért, hogy rajtuk kívül más országok is tiltólistára tegyék őket.

Az Oxford Economics készített egy elemzés arról, hogy mivel járna Európában, ha kizárnák az egyik meghatározó piaci szereplőt a versenyből, és egészen ijesztő számokat közöltek. Az intézmény tanulmánya szerint a reális forgatókönyv alapján is 19 százalékkal nőnének a vizsgált 31 európai országban az 5G beruházási költségei, ami azt jelentené, hogy a következő 10 évben évente 3 milliárd euróval kellene többet költeni a hálózatok fejlesztésére. Az elemzés szerint Magyarország számára egy esetleges korlátozás mintegy 200 milliárd forint (55 millió euró) többletköltséget jelentene évente az 5G infrastruktúra kiépítése során. A költségek növekedése miatt a lakosság 5 százaléka, mintegy félmillióan maradnának 5G nélkül 2023-ban is, akik a korlátozás hiányában hozzáfértek volna a hálózathoz. A kalkuláció szerint a magyar GDP-növekedést pedig 1000 milliárd forinttal (300 millió euróval) vetné vissza 2035-ben, ha kitiltanák a piacról az egyik meghatározó szereplőt.

Bár az Oxford Economics számításai egyelőre csak egy lehetőséget vázolnak fel, jól érzékeltetik, mekkora hatással lehet az 5G az életünkre. A szervezet tanulmánya szerint az 5G technológia széleskörű elterjedése a következő gazdasági hatásoknak köszönhetően 140 milliárd euróval járulna hozzá az EU 28 tagállamának GDP-jéhez, és 2,3 millió új munkahelyet teremtene a közösségben.

Mindenki megélte az elmúlt hónapokban, mennyire fontos egy stabil, nagy le- és feltöltési sebességet kínáló, megbízható kommunikációs hálózat

Itthon is váltunk

Ezek alapján nem meglepő, hogy komoly versenyfutás van az újgenerációs mobiltechnológia bevezetésében, és egyelőre Magyarország nem áll rosszul. A zalaegerszegi Zala Zone tesztpályán már tavaly tavasszal lehetett tesztelni az 5G-t, múlt ősszel a Vodafone – éppen a Huawei eszközeit alkalmazva – Budapest belvárosában elindította kereskedelmi szolgáltatását, majd idén áprilisban, az 5G-s frekvenciatender lezárása után pár nappal a Magyar Telekom is csatlakozott riválisához. A fejlesztés pedig nyáron a nagyobb városokban és a Balaton mellett folytatódott, a Vodafone augusztus elején kapcsolta be siófoki 5G-s bázisállomásait. ■

FORRÁS: RG-ROBOTICS.COM

DÉL-KOREA ÁLL A LEGJOBBAN AZ AUTOMATIZÁCIÓRA VALÓ FELKÉSZÜLÉSBEN

Robotok milliói állnak munkába a következő években

Csak idén várhatóan 100 milliárd dollárt költenek különböző robotokra világszerte, a következő néhány évben pedig mintegy kétmillió ipari robotot helyeznek üzembe a gyárakban. A koronavírus-járvány tovább gyorsította az automatizációt és ezzel együtt a robotok bevetését, amelyek egyre több helyen jelennek meg.

Időről-időre megdöbbentő videókat tesz közzé a közösségi médiában a robotfejlesztés egyik úttörő vállalkozása, a Boston Dynamics. A legutóbbi rövid filmekben például azt láthattuk, ahogyan néhány „robotkutya” összedolgozva egy kamiont húz el, de megcsodálhattuk már a cég humanoid felépítésű robotjának akrobatikus képességeit is – az olimpián ugyan még nem indulhatna talajtornában, de néhány bukfenc, akadályok átugrása már nem okoz gondot neki. Az amerikai társaság a közelmúltban egy olyan videót is nyilvánosságra hozott, amely azt mutatja be, hogy milyen sokoldalúan alkalmazhatók a „robotkutyák” a gázszivárgás felderítésétől a veszélyes helyen található objektumok megközelítésén át színpadi előadásokig, attól függően, hogy mire programozzák őket.

A kínai kormány csak a múlt évben 577 millió dollárt fordított intelligens robotok fejlesztésének támogatására

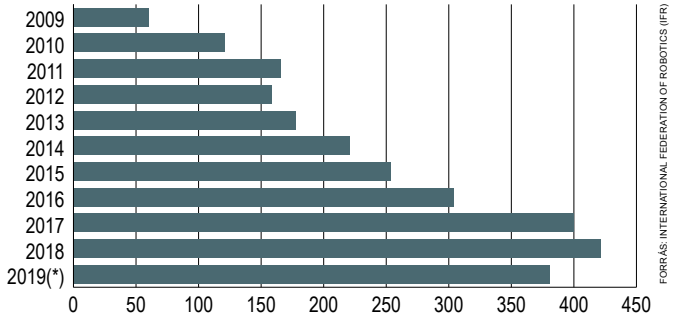
Pepper a gyógyításban

A koronavírus-járvány egyelőre nehezen felmérhető változásokat hozott a világban, de az egyik olyan terület, ahol alaposan felpörgette az innovációt – nemcsak a technológia, de az alkalmazási módok és az üzleti modellek kapcsán is –, az egyértelműen a robotrendszerek használata, illetve az automatizáció. Jó példa itthon is akad erre, az egyik budai magánrendelőben Pepper, az ember formájú robot is állást kapott, az volt a feladata, hogy előszűrje, kikérdezze az érkező pácienseket, és a koronavírus-gyanúsakat a protokoll szerinti orvoshoz irányítsa.

Bár itthon még egyedinek számít a humanoid robot alkalmazása, világszerte számos példa van ezek kihasználására. Pepper társai recepciósként dolgoznak belga, ausztrál, kanadai kórházakban, ahol szintén a rutinfeladatokban segítenek, vagy éppen játszani lehet velük.

Munkába állított ipari robotok száma

Globális szinten, ezer darab



*előzetes adat

Százmilliárd dolláros üzlet

Az elmúlt években világszinten tapasztalt munkaerőhiány jelentősen felgyorsította az automatizációs törekvéseket, illetve a robotok fejlesztését. Bár a koronavírus-járvány a munkaerő-piaci helyzetet alaposan átalakította, a karanténintézkedések miatt bezáró gyárak, illetve a személyes távolságtartás iránti igény nemcsak fenntarthatja a keresletet az ilyen jellegű megoldások iránt, de várhatóan még növeli is.

Az International Federation of Robotics (IFR) nevű szervezet várakozásai szerint a következő időszakban évente átlagosan 25 százalékkal bővül a robotok iránti globális kereslet, és idén várhatóan 100 milliárd dollárt költenek világszerte ilyen gépekre. Ha robotokról van szó, a legtöbben a gyárakban alkalmazott berendezésekre gondolnak, és valóban, az új ipari forradalom részeként az eddiginél is nagyobb mértékben jelennek meg a gyártásban ezek a gépek. Az IFR várakozásai szerint 2020 és 2022 között világszerte mintegy kétmillió új ipari robotot üzemelnek majd be a gyárakban.

Nemcsak a számokban lesznek nagy változások

Az IFR elemzése arra is rámutatott, hogy a robotok egyre okosabbak lesznek, a szenzoroknak, a nagy teljesítményű processzoroknak, a felhőkapcsolatnak, illetve a speciális szoftvereknek köszönhetően akár arra is lehetőség lesz, hogy közvetlenül oktassák ezeket a gépeket. Vagyis egy ember megmutatja, hogy pontosan milyen mozdulatsort kell végrehajtaniuk, azok pedig leutánozzák. De izgalmas új üzleti modellek is kialakulhatnak, mint például az RaaS (Robots as a Service), vagyis a robotokat szolgáltatásként vehetik majd igénybe a cégek, ami nagyfokú rugalmasságot, a termelési kapacitás gyors skálázhatóságát eredményezi.

Stratégiai szerep

Jól érzékelteti, hogy a robotok milyen fontos szerepet tölthetnek majd be a jövőben, hogy több, a technológiai fejlesztésben élenjáró ország kiemelt figyelmet szentel ennek a területnek, stratégiák készültek és valósulnak meg a robotfejlesztés felgyorsítására. A Kína ipari termelésének modernizálását célzó „Made in China 2025” program 10 kulcsfontosságú iparágat nevesít, amelyekre fokozott figyelmet fordítanak, ezek közül az egyik a fejlett robotok készítése. A kínai kormány csak a múlt évben 577 millió dollárt fordított intelligens robotok fejlesztésének támogatására.

Japánban azt a célt tűzték ki maguk elé, hogy a világ robotfejlesztésének a központjává váljanak – erre a célra tavaly 351 millió dollárnyi költségvetési forrást szántak –, és az IFR adatai szerint a szigetország meglehetősen jól áll, hiszen 2018-ban a világszerte munkába állított ipari robotok 52 százaléka náluk készült.

Elképesztő erőfeszítéseket tesz a robotizáció fokozására Dél-Korea is, ahol 2018-ban már 300 ezer ipari robot volt, ami azt jelenti, hogy ott öt év alatt megduplázódott az ilyen gépek száma. Dél-Korea az IFR összesítése szerint idén 126 millió dollárnyi állami pénzt szánt a robotok fejlesztésére. Az ázsiai ország egyébként a teljes automatizációt vizsgálva is élen jár, a The Economist Intelligence Unit „Automation Readiness Index” című felmérése alapján a vizsgált 25 ország közül ők állnak a legjobban. Németország és Szingapúr a második és harmadik. ■

ELEKTROMOS HÁLÓZAT HIBAFELISMERÉSE

Automatizáció nagy teljesítményű drónokkal

FORRÁS: HRP EUROPE KFT/DJI – HTTPS://DRON.HRP.HU/ENTERPRISE

Vállalati területen a drónok alkalmazását indokolhatja, ha emberi erőforrás számára monoton, éppen ezért hibalehetőséggel végezhető feladatot szeretnénk megoldani, ha szennyezett vagy veszélyes területen dolgozunk, illetve, ha a drón alkalmazásával a munka gazdaságosabban, gyorsabban elvégezhető.

Az E.ON több mint két éve használ drónokat az elektromos vezetékhálózat ellenőrzésére. A szolgáltató az üzemeltetésében álló nagyfeszültségű hálózatait évente, közép és kisfeszültségű hálózatait háromévente köteles bejárni és átvizsgálni, ellenőrizni. A drónok alkalmazása előtt az E.ON szakemberei földi hálózatbejárást végeztek, csak nagyfeszültségű hálózatoknál jellemző, hogy időszakosan helikopteres ellenőrzés történik. Utóbbi előnye, hogy felülnézetből, a földről esetleg nem észlelhető hibák, szakadások, elhasznált hálózati elemek is beazonosíthatók. Innen szinte adja magát, hogy ezeket a biztonsági hálózatbejárásokat egyszerűbben, gyorsabban, költséghatékonyabban lehet drónnal elvégezni.

A jelen drónjai és a jövő lehetőségei

Az E.ON jelenleg DJI Matrice 200-as gépeket alkalmaz egy hőkamerával és egy 30-szoros optikai zoomos kamerával. Az eszközöket, a „földre hozott” képeket az erre felkészített munkatársak kezelik és elemzik, és a döntéseket is ők hozzák. Az E.ON az eddigi tapasztalatok alapján tovább kívánja fejleszteni a rendszert, hogy minél inkább automatizálni tudja a hálózatellenőrzési feladatot. Már folyamatban van az az új projekt, amelyben a hálózatbejárást az úgynevezett gépi látással támogatják majd. A kisfeszültségű hálózatok esetében speciális felszereltségű autók, ún. „lidar” eszközökkel (digitális lézerszkennerekkel) mérik és ellenőrzik a vezetékeket.
A rendszert folyamatosan fejlesztik, „tanítják”, hogy képes legyen automatikusan azonosítani a hálózati hibákat, szakadásokat. Ugyanezt a munkát a nagy- és középfeszültségű hálózatoknál nagy teljesítményű drónok lesznek képesek elvégzeni. A rendszer már munka közben mérlegeli és tudja, az új adatokból pedig folyamatosan újratanulja, hogy mely helyzeteket kell rögzítenie, esetleg továbbítania. Fontos, hogy a felmérés képeit és videóit lehetőleg azonos távolságról és azonos szögből rögzítések, így az állapotváltozások jobban követhetőek. Természetesen a beállítások is hatékonyabban programozhatók drónok (gépi eszköz) autonóm munkája során.

Jön az MI, nő az akku és a teherbírás

Májusban jelent meg a DJI Matrice családjának a legújabb tagja, a Matrice 300 RTK. Az eszköz új standardot jelent az ipari drónfelhasználásban, mert egyesíti az intelligens repülést, a digitalizációt és a mesterséges intelligenciát. Az M300RTK az első olyan DJI fejlesztés, amely mesterséges intelligenciát használ. A drón 6 irányú akadályérzékelésre képes, akár 40 méteres távolságból. Maximális repülési ideje eléri az 55 percet, multitöltője 8 drón- és 4 távirányító-akkumulátort kezel, míg a gyorstöltés funkció lehetővé teszi a repülések folyamatos végrehajtását. A nagy kapacitású, intelligens, cserélhető TB60 akkumulátorok lehetővé teszik a kezelők számára, hogy kikapcsolás nélkül cseréljék az akkumulátorokat, időt spórolva a kritikus feladatok során.
A Matrice 300RTK „AI Spot-check” funkciója támogatja ugyanazon objektum többszöri automatikus villámellenőrzését azonos beállításokkal, így képes az objektum tárolt és aktuális állapota közötti legkisebb különbség kimutatására és elemzésére is. Maximális hatótávolsága 15 km, és teljesen megújult adattovábbítási rendszere háromcsatornás, 1080 pixeles videójel továbbítására is alkalmas. Az eszköz – eddig egyedülállóan – három hasznos teher, egyenként 2,7 kg súlyú munkaeszköz hordozására képes.

(X)

További információ a DJI drónok enterprise felhasználásáról:
https://dron.hrp.hu/enterprise/; https://enterprise.dji.com/

KULCS A JÖVŐHÖZ: BIZTONSÁGTUDATOSSÁG

A járványt nem kértük, de a magasabb kiberbiztonságot köszön(t)jük

FORRÁS: MIME ASIA

A világjárvány elméleti síkról a való életbe ültette át azokat a frázisokat, amelyek a jövőbeni kockázatokra való felkészülést szajkózták, és rámutatott a folyamatok szabályozása és kockázatalapú vezetés nélkül működő cégek válságállóságának problematikájára is. A Brightdea Solutions az információbiztonság oldaláról vizsgálta az elmúlt hónapok eseményeit, és megfogalmazták azt, hogy mely cégek lehetnek sikeresek a jövőben.

A COVID-19 sok dologra megtanította a cégeket, de ha valamit ki kellene emelni, az nem lenne más, mint az információbiztonság létfontossága és a biztonságtudatosság nélkülözhetetlensége. Ennek ellenére a viszony az információbiztonsági csapat és a vállalat többi területe között mégis kritikus. Az informatikai rendszerek védelménél a legnagyobb probléma még mindig az emberi tényező, mert főként az emberi figyelmetlenség, a felelőtlenség, esetleg a felkészítés hiánya miatt lehetnek sikeresek a kibertámadások.

A hatékony innovációhoz a kockázattal arányos intézkedések felső szintű, költséghatékony menedzselése elengedhetetlen, mert a működési hatékonyság javítása a cég növekedésének, illetve nyereségességének a záloga, mindamellett, hogy a döntéshozóknak alkalmazkodniuk kell az megváltozott körülményekhez. Előfordul ugyanis, hogy a menedzsment nem igazán tudja az IT-stratégiát szorosan illeszteni a vállalati stratégiához, ezért a vállalatok mégsem a kockázattal arányos módon priorizálják a lépéseiket. Ami tényleges veszélyt hordoz.

A Brightdea Solutions már hat iparág számára nyújt szolgáltatásokat. Vegyük példaként az agrár szektort: egy okosfarm-koncepció technológiai elemei akár kockázatként akár kihívásként is megjelennek. A cég tapasztalatai alapján nem is a különböző technológiai megoldások szigetszerű bevezetése, hanem a különböző gazdaságok eltérő igényei alapján készített információs és technológia mixe már nincs meg az együttműködéséhez. Tehát valójában nincsenek meg a kiberkockázatokat kiküszöbölő felmérések. A Brightdea véleménye szerint azok a gazdaságok lehetnek sikeresek, amelyek az információs és az új technológiákkal szemben támasztott igényeiket helyesen tudják alkalmazni.

A Brightdea Solutions célja, hogy partnereik ezeket a kockázatokat képesek legyenek komplexen és biztonságosan kezelni. Így olyan objektív információkat tud szolgáltatni a vállalatok vezetőinek, amelyek segítségével a kockázatok megfelelően besorolhatók, így a kibervédekezés fenntarthatósága hatékonyan javítható. ■

> A hatékony innovációhoz elengedhetetlen a kockázattal arányos intézkedések felső szintű, költséghatékony menedzselése

SECURITY OPERATION CENTER

Incidensek felügyelet alatt

A nagy informatikai rendszerek védelme, az incidensek figyelése jelentős szaktudást és erőforrásokat igényel, amit nem minden cég tud saját maga megoldani. Szolgáltatásként azonban sokkal szélesebb kör számára elérhető.

Információbiztonsági rendszereket ma már gyakorlatilag minden vállalat telepít. Sokan viszont még mindig beleesnek abba a hibába, hogy úgy képzelik: a telepített rendszerek egyszer és mindenkorra garantálják a biztonságot. Ez azonban nem így működik – oszlat el egy félreértést *Rózsa Roland,* a 4iG stratégiai cybersecurity tanácsadója. „Még a leginkább automatizált, mesterséges intelligenciával felvértezett, naponta többször frissített adatbázisokból dolgozó védelmi megoldás is jóformán haszontalan, ha az eredményeit nem dolgozzák fel, a riasztásokat nem vizsgálják ki. Megnyugtató, ha a rendszerünk megfogja az összes kártékony e-mailt. De ha nem vesszük észre, hogy a szokásos napi öt helyett a múlt héten már 15-öt kaptunk, ezen a héten pedig 30-at, akkor elmulasztunk egy fontos trendet. Valaki láthatóan támadni próbál bennünket, és ha az e-mail nem válik be, más támadási vektort fog keresni”, magyarázza a monitorozás egyik aspektusát a szakértő.

Adatok minél több forrásból

A biztonsági adatok értelmezése persze nem egyszerű feladat. Ha a vállalat nem engedheti meg magának IT-biztonsági szakemberek alkalmazását, már többféle menedzselt biztonsági szolgáltatás közül választhat (e-mail védelem, URL-védelem, egyebek). Az ilyen jellegű szolgáltatások csúcsa a Security Operation Center (SOC) igénybevétele.

FORRÁS: 4IG

RÓZSA ROLAND, 4iG

A SOC egy olyan környezetet jelent, ahol dedikált információbiztonsági csapat monitorozza és elemzi az ügyfél informatikai rendszereiben, hálózatában, alkalmazásaiban, adatbázisaiban folyó eseményeket, észleli a támadásokra, incidensekre utaló jeleket, majd ezekre reagál. Egy hatékonyan működő SOC-nak számos ismérvnek kell megfelelnie. Az egyik, hogy nemcsak a biztonsági rendszerekből érkező adatokat figyeli, hanem ideális esetben mindent: a hálózati eszközök, a szerverek, az adatbázisok, az alkalmazások naplóállományait és működési adatait. A következő fontos jellemző, hogy mindezeket az adatokat összeveti és egységesen elemzi, olyan összefüggéseket is feltárva, amelyek egyébként rejtve maradnának.

Óriási kihívás természetesen, hogy a rendkívül nagy mennyiségű adatból miként lehet kiszűrni a valóban relevánsakat, azokat, amelyek ténylegesen biztonsági incidensekre utalnak. Ehhez nem csupán fejlett – manapság már rendszeresen gépi tanulással és mesterséges intelligenciával megtámogatott – informatikai rendszerekre van szükség, hanem magasan képzett, tapasztalt szakemberekre is.

Végül a SOC feladata az is, hogy válaszoljon a támadásra. „Ez a válasz azonban nem feltétlenül az incidens elhárítását jelenti”, hangsúlyozza Rózsa Roland. A SOC javaslatokat tehet (ha kérik), például a hálózat szegmentálására vagy egyes szerverek, szolgáltatások lekapcsolására, de a konkrét lépéseket az üzemeltetési csapat teszi meg, miközben a SOC információval látja el őket. Ezért rendkívül fontosak a SOC működtetésében az átgondolt és előre lefektetett folyamatok, az egyes helyzetekre kidolgozott playbookok. Amikor bekövetkezik az incidens, nem szabad késlekedni, de kapkodni sem, hanem haladni kell a kész forgatókönyv szerint.

Halálcsillag

SOC-ot létrehozhat saját maga számára is egy vállalat, ám ezek kiépítése és működtetése olyan erőforrásokat és felkészültséget igényel, hogy csak a legnagyobbak választják ezt az utat; a hazai céges SOC-ok száma talán a tízet sem éri el, véli Rózsa Roland. Az igény azonban a kisebb vállalkozások körében is felmerülhet, és ilyenkor jöhetnek szóba a szolgáltatásként igénybe vett security operation centerek. „Ha egy vállalat már kidolgozott egy átfogó kiberbiztonsági stratégiát, eljutott a biztonsági érettség egy viszonylag magas szintjére, és 2-3 dedikált IT-biztonsági szakember felvételét fontolgatja, mindenképpen érdemes átgondolnia a menedzselt SOC-ot. Egy ilyen SOC ráadásul nem egy az egyben helyettesít 2-3 szakembert. A szolgáltatáscsomagban jellemzően 8-10 kolléga szakértelme és az ehhez való folyamatos hozzáférés is benne van, a szolgáltató munkatársai pedig több környezetet, több incidenst látnak, így szélesebb kitekintésük van”, mondja Rózsa Roland.

Az együttműködés az ügyfél igényeinek és környezetének felmérésével kezdődik. Mindenki szeret biztosra menni, de felesleges Halálcsillagot építeni, ha egy birodalmi csillagromboló is megteszi. A megoldásnak az üzleti igényekhez kell igazodnia: évi 50 millió forintos kockázatot nem érdemes évi 100 millió forintért elhárítani, fogalmaz a biztonsági szakember. A 4iG és az ügyfél közösen meghatározza a valóban megfelelő szolgáltatás tartalmát, majd erre kidolgozzák az implementációs és üzemeltetési tervet.

A szolgáltatások differenciálása több mérőszám mentén történik. Az egyik az időbeli lefedettség: csak munkaidőben (5×8, 5×10 órában) vagy folyamatosan (7×24 órában) kérhetik a rendszerek monitorozását. A második a változtatások száma: milyen gyakran változik az informatikai környezet, milyen sűrűn kell új rendszereket bevonni a figyelemmel kísért körbe. Végül a havonta kivizsgált incidensek száma is befolyásolja az árat, egy-egy kivizsgálás ugyanis idő- és erőforrás-igényes feladat.

Beavatkozás kérésre

A nagy kérdés persze az, hogy mi történik, amikor a SOC támadást észlel az ügyfél rendszerében. Ahogy arról volt szó, a SOC nem gyorsreagálású erő, elsődleges feladata a tájékoztatás. Gyakori, hogy az ügyfél csak értesítést kér az incidensekről, és utána saját hatáskörben dönt a további teendőkről. Ugyanakkor igény esetén a 4iG arra is tud javaslatot adni, hogy technikai szempontból mi lenne a hatékony megoldás.

Bizonyos szempontból még egyszerűbb a helyzet, ha a SOC-ügyfél számára a 4iG üzemelteti az informatikai infrastruktúrát. Ebben az esetben az értesítés a házon belüli üzemeltetési csapatnak megy, amelyik megbeszéli az ügyféllel a szükségesnek ítélt válaszlépéseket, és jóváhagyás esetén végre is hajtja azokat. Ilyen esetekben az ügyfélre jóformán csak a döntés feladata marad. ■

Minimális beruházással

A menedzselt szolgáltatásként igénybe vett SOC egyik szépsége, hogy az ügyfél részéről szinte semmilyen technológiai beruházást nem igényel. Egy közepes, 40-50 rendszerből álló környezet monitorozásához általában 1-2 virtuális szerver kell, erre telepítik a 4iG szakemberei a szükséges rendszerkomponenseket. A felügyelet során a szolgáltató szakemberei éles tranzakciós adatokhoz, adatbázisokhoz nem férnek hozzá: csupán metaadatokra és a naplóállományokból kinyerhető információkra van szükségük, így a SOC igénybevétele semmilyen adatvédelmi vagy szabályozói előírást nem sért.

KERUBIEL

GDPR-ÚJDONSÁGOK

Nem a polcra gyártjuk az adatvédelmi szabályzatokat

Egy átlagos magyar vállalat a minimum erőfeszítést mutatja adatvédelem területén, holott a hatóságok türelmi ideje már lejárt. Ha a komoly bírságok nem sarkallják a GDPR megfelelésre a vállalatokat, a vállalati adatvagyon megvédése mozgathatná őket – mondják Dellei László, a Kerubiel ügyvezető igazgatója és Vadász Gábor, a Kerubiel műszaki igazgatója.

FORRÁS: KERUBIEL

DELLEI LÁSZLÓ, KERUBIEL

– Milyen változásokra számíthatnak a vállalatok GDPR területén?

Dellei László (D. L.): Az adatvédelmi hatóságok kezdetben kellően türelmesek és elnézők voltak a vállalatokkal szemben. Az elmúlt időszak elegendő volt arra, hogy a vállalatok felkészüljenek a személyes adatok védelmére. Azt látjuk, hogy az eltelt időszakban sok incidens és adatszivárgás, adatlopás történt, melyről az adatvédelmi hatóságokat annak módja szerint a vállalatok értesítették is. De azt is látjuk, hogy a magyar hatóságok komolyan veszik tevékenységüket. Megszületett több komoly bírság is a türelmi időszak végén, és azt látjuk, hogy ez a szigorúság nem hagy alább. Szolgáltatásainkkal segítünk ezekre a megfelelésekre is felkészülni a vállalatoknak. Mi nem polcra gyártunk papírokat, adatvédelmi szabályzatokat, hanem a vállalat adatvédelmi auditálása során konkrét megoldásokat vezetünk be, ha ennek szükségét látjuk. A személyes adatok védelme kiemelt terület, és ezen a téren van mit fejlődjenek a magyar vállalatok.

– A magyar cégek komolyan veszik a személyes adatok védelmét?

Vadász Gábor (V. G.): - Vannak iparágak – mint például a pénzügyi szféra – ahol nagyon komoly intézkedéseket tettek azért, hogy biztosítsák, hogy a GDPR-nek megfelelően tárolják, kezeljék az adatokat. Láttam nagyvállalatokat is, ahol megnyugtatóan rendezték a kérdést. Tapasztaljuk, hogy az adatvédelmi tanúsítást, mint az átláthatóság egyik lehetséges igazoló eszközét, fontolóra veszik a nagyvállalatok. Azonban egy átlagos magyar vállalatnál jellemzően az alapvető minimum erőfeszítést mutatják adatvédelem területén. A vállalatoknak be kellene látniuk, hogy az adatok jelentik azt a vagyont, azt a pluszt, amely komoly versenyelőnyt adhat számukra, és a saját jól felfogott érdekük azokat megfelelően kezelni. Kevés cég tart ezen a fejlettségi fokon, sok a tennivalónk ezen a téren.

– Milyen területen vannak konkrétan hiányosságok?

D. L.: A vállalatok hajlamosak félvállról venni ezt a területet, pedig a hatóságok, mint említettem, komolyan ellenőrzik a területet, és bírságolnak is. Egy távközlési vállalatnál nemrég rekord mértékű bírságot szabott ki a hatóság, de más szektorok szereplői esetén is vastagon fogott a hatósági auditorok ceruzája. Az interneten barangolva olyan „low hanging fruit” megoldások implementálását sem látom, mint például a cookie-k megfelelő kezelését biztosító technikai intézkedések – holott ezzel megnyugtató benyomást tehetnénk a látogatóra.

De ha mélyebbre megyünk, akkor a vállalatoknál problémát jelent, amikor egy adatalany alapvető jogait szeretné érvényesíteni. Például az adatalany élni kíván a tájékoztatáshoz, a hozzáféréshez vagy akár az elfeledtetéshez való jogával, és ezzel összefüggésben kikéri, hogy róla milyen adatokat tárolnak. A hasonló kérdésekre nincs minden esetben kidolgozott ügymenet, triviális esetben valamilyen ticketing rendszerrel próbálják kezelni. Hasonlóképp, gondot okoz az adatok anonimizálása, ahogy az adattörlés is nehézkes, főleg technológiai szemszögből.

FORRÁS: KERUBIEL

VADÁSZ GÁBOR, KERUBIEL

A PRIME-VR2 célja

Jenny Rainbird, a projektpartner Inlecom szerint a PRIME-VR2 nagyon érdekes és fontos projekt a VR a betegek rehabilitációjában való alkalmazásában. Célja, hogy pozitív hatást gyakoroljon e társadalmi igény kielégítésére. Az Inlecom együttműködik a PRIME-VR2 partnerekkel annak biztosítása érdekében, hogy szilárd kereskedelmi terv létezzen, amely az IPR védelmére irányuló stratégiára támaszkodik szabadalmak bejelentésével, hogy fenntartható jövőt és növekedést lehessen biztosítani a projekt innovációk számára.

– A járványhelyzet is hozott új fejlesztendő területeket?

D. L.: Gyakori probléma, hogy a munkaadó elfelejti tájékoztatni a partnereket, kollégákat, hogy a publikus vagy irodai területeken kamerával vagy a munkahelyi hálózaton szoftveresen megfigyeli a munkavégzést, vagy annak bizonyos részeit monitorozza. Sok vállalat ugyanakkor felhőalapú szolgáltatást is igénybe vesz, ami költséghatékonyság szempontjából teljesen érthető üzleti döntés. A felhőszolgáltatások igénybevételénél azonban az adatkezelők sok esetben megfeledkeznek meggyőződni többek között arról, hogy az adatokat fizikailag az EU területén belül lévő adatközpontban tárolják-e. Ezekre a problémákra az adatvédelmi hatásvizsgálatok mind-mind fényt deríthetnek, és feltárhatóvá válnak az adatkezeléssel járó kockázatok.

– A Kerubiel nemrég két partnerséget kötött, ezek miért fontosak cégük életében?

D. L.: Még az elején szeretném leszögezni, hogy a Kerubielnél az adatkezelés területén szolgáltatásokra építve kínálunk értéknövelt tanácsadást, vezetői tanácsadást, ezen nem tervezünk változtatni. A magyar vállalatoknál tapasztalt GDPR-hiányosságokra reagálva éreztük fontosnak két partnerséget kötni: az egyik a világ legnagyobb szállítója GDPR területén, a OneTrust, a másik pedig a magyar kiberbiztonsági vállalkozás, a Black Cell. A OneTrust megoldása a GDPR teljes vertikumában szolgáltatásokat és egyedi megoldásokat nyújt adatkezelők részére. A felkészülés, rendszer bevezetés, az értettségi fok és kontrollok minőségének ellenőrzése területén egyaránt fontos partner, de a GDPR-auditori munkánkat is teljes mértékben támogatja. Miután a vállalatoknál feltárjuk az adatvédelmi hiányosságokat, rámutatunk a fejlesztendő területekre és elkészítjük a szabályzatokat, megoldásokat is tudunk biztosítani, melyek garantálják, hogy a vállalati GDPR-megfelelőséget a folyamatok is teljeskörűen támogatják.

– És a Black Cell partnerség?

V. G.: Ez a partneri viszonyunk eléggé friss, pár hete kötöttünk megállapodást, amely speciális IT biztonsági és kibervédelmi megoldások, SOC, illetve kritikus infrastruktúra védelem területére egyaránt kiterjed. Az adatvédelem szorosan összefügg az IT biztonság kérdésével, és azt tapasztaltuk, hogy a kkv-k részéről egyre gyakrabban merül fel az igény egy Security Operations Center jellegű szolgáltatás igénybevételére – ezt viszont saját erőből, nulláról felépíteni rendkívül költséges, időigényes munka lenne. A Black Cell SOC szolgáltatásait „white label” partneri viszony keretében tudjuk akár a kkv-szektorban is értékesíteni, melynek segítségével a kiberbiztonsági kockázatokat a vállalat hatékonyan tudja kezelni. Az új partneri megállapodásaink azokon a fókusz területeken is segítenek, ahol pénzügyi intézményeket támogatunk az MNB engedélyeztetési eljárásokban.

– A Kerubielnél komoly K+F tevékenység is folyik, erről elárulna többet?

V. G.: A közelmúltban több innovatív projektet is sikeresen zártunk a mesterséges intelligencia, és az IoT területeken. A PRIME-VR2 fejlesztési projektet az Európai Bizottság finanszírozza, tavaly ősszel indult. A projekt célja egy virtuális valóság alapú platform fejlesztése, melyet rehabilitációs célokra használhatunk. A kutatások azt mutatják, hogy a virtuális valóság játékok komolyan segíthetik a stroke-on átesett betegek rehabilitációját, a forgatókönyveket kutatóorvosok, orvoscsapatok dolgozzák ki. A Kerubiel feladata ebben a rendszerintegrációs platform megvalósítása. Ha minden a tervek szerint halad, jövő év folyamán már lesz tesztelhető prototípusa a rehabilitációs virtuális játéknak. Addig is keressük azokat a hazai partnereket, intézményeket, rehabilitációs központokat, a stroke területén kutató orvosokat, akik nyitottak a megoldás tesztelésére. *(X)*

FÓKUSZBAN A TÁVOLI ESZKÖZÖK VÉDELME

Megszűnt a bizalom a hálózaton

Amíg a járvány, a home office, a karantén office időszaka tart a vállalatoknak a mobil eszközök és dolgozók védelmére kell összpontosítaniuk. Megnő a natív, felhő alapú védelmi technológiák iránti kereslet, és nagyobb szerep jut az automatizációnak.

FORRÁS: WRIKE.COM

Míg a járványhelyzet kezdetén nagyon sokan azt gondolták, egy átmeneti időszak után az élet visszatér a normális kerékvágásba, most már látjuk, hogy véglegesen átalakult a vállalatok munkavégzése, ami befolyásolja, mire is kell az IT-biztonság terén összpontosítani. Sok vállalat belekóstolt a távmunkába, és megtapasztalhatták, hogy a munkavégzés hatékonysága nem szenvedett csorbát, viszont a munkatársak megtanulták jobban összeegyeztetni a munkát a magánélettel. Az otthonról dolgozó emberek száma 2005 óta 140 százalékkal nőtt a járvány nélkül is (a Global Workplace Analytics tanulmány szerint), a munkavállalók 52 százaléka legalább hetente egyszer otthonról dolgozik.

Távolra nyúló biztonság

Ez azt jelenti, hogy a helyi hálózat, vagyis a LAN-kapcsolatok helyett olyan eszközök védelmét kell biztosítaniuk az IT-biztonságiy csapatoknak, amelyek távolról kapcsolódnak a vállalati hálózatba, és felhő alapú megoldásokat használnak. Ugyanakkor nagyon sok olyan digitális projekt vagy digitalizáció-elképzelés indult, melyeknek az a célja, hogy a személyek közötti kapcsolatokat minimálisra csökkentse – ezek biztonságát is garantálni kell. A Gartner kutatása szerint emiatt megnövekedik a zero-trust network acces (ZTNA) megoldások iránti kereslet, amelyek a hagyományos VPN-kapcsolódást váltják ki. A ZTNA segítségével a vállalatok könnyebben ellenőrzik az adott alkalmazáshoz történő távoli csatlakozást. Ez azért biztonságosabb lehetőség, mert elrejti az alkalmazást az internet elől – a ZTNA csak

A rögzített videókonferencia GDPR adat! Nem is lehet kamera elé kötelezni a dolgozókat, hiszen van alternatíva: a telefon

a ZTNA szolgáltatóval kommunikál, és csak a ZTNA biztosította felhőszolgáltatáson keresztül vehető igénybe. Ezzel csökkenthető az a kockázat, hogy egy támadó a VPN-csatlakozásra „ráülve” támadja meg a többi vállalati alkalmazást. A ZTNA teljes körű vállalati elfogadása azt feltételezi, hogy a cégnek pontos nyilvántartása van arról, hogy mely alkalmazottnak milyen alkalmazáshoz kell hozzáférés – ami lassíthatja a technológia terjedését. Ugyancsak a home office miatt a hálózati biztonság fókusza a LAN alapú eszközvédelmi modellről a Gartner által SASE-nak nevezett modellre vált. A SASE a „secure acces service edge” technológiát jelenti, amely lehetővé teszi a vállalatoknak, hogy jobban védjék a mobil dolgozókat és a felhő alkalmazásokat azzal, hogy a forgalmat egy teljesen felhő alapú biztonsági megoldáson terelik át. A SASE-t szolgáltatásként lehet igénybe venni az erre szakosodott cégektől: a felhasználók és a hálózati eszközök a központosított, felhő alapú biztonsági szolgáltatáshoz csatlakoznak. Ezzel az otthonokba kiterjesztett vállalati erőforrások és adatok is egyaránt védve lesznek.

Felértékelődik az automatizáció szerepe

A biztonság területére is jellemző munkaerőhiány miatt egyre nagyobb szerep jut az automatizációnak. Az előre meghatározott szabályokon és template-eken alapuló, számítógép-centrikus biztonsági feladatok megfelelő megoldásokkal könnyedén automatizálhatók, így azokat gyorsabban és kevesebb hibával lehet elvégezni, könnyebben lehet méretezni. A repetitív feladatokat a megoldásokra, eszközkészletekre bízhatjuk, a biztonsági szakembereknek meg több idejük marad a kritikus biztonsági kérdésekkel foglalkozni.

Adatszivárgások

– Az adatszivárgások 72 százaléka nagyvállalatoknál történt
– Az adatszivárgások 28 százaléka kis és közepes vállalatokat érinti
– Az adatszivárgások 81 százalékát egy nap vagy kevesebb idő alatt hárították el
– Az áldozatok 58 százalékánál személyes adatok is kikerültek

FORRÁS: VERIZON 2020 DATA BREACH INVESTIGATIONS REPORT

Az MI és a gépi tanulás a biztonság területén is kiegészíti és automatizálja az emberek döntéshozatalát. A technológia szakszerű használatához azonban biztonsági szakértők bevonására van szükség, három, vállalatokat érintő probléma esetén: megvédeni az MI működtette digitális üzleti rendszereket, az MI a meglévő biztonsági termékekkel közösen növelje a vállalat biztonságát, és megelőzze az MI támadó célú használatát.

Pontosabban észleljük a támadásokat

A Gartner meglátása szerint vállalati szinten megjelennek a kiterjesztett jelző- és reagáló (extended detection and response, XDR) biztonsági megoldások. Ezek automatikusan gyűjtik és vetik össze az adatokat a vállalat összes biztonsági termékéből, ezzel is gyorsítva a fenyegetettségek időben történő felismerését, és a a gyors válaszadást az esetleges incidensre. Például egy támadás, amely riasztást generált az email-megoldásban, a végponton és a hálózaton egyaránt, egy incidensbe kombinálható. Az egyébként egyenként elhanyagolható fontosságú riasztások együttesen egy olyan eseményt rajzolhatnak ki, mellyel már érdemes komolyan foglalkozni. Az XDR-megoldások elsődleges célja a támadás észlelési pontosságnak és a biztonsági műveletek hatékonyságának növelése. ■

NEMCSAK BIZTONSÁGI PLATFORM, ÉRTÉKNÖVELT SZOLGÁLTATÁS

Védjük meg ipari rendszereinket!

Az ipari vezérlőrendszerek (Industrial Control Systems, röviden ICS) védelmére fejleszt a Balasys olyan biztonsági koncepciót, amely az ügyfelek igényeinek megfelelően alakítható. Az eszköz megoldást jelent a vezérlőrendszerek magas szintű biztonságára – mondja Cseledi Sándor ügyvezető igazgató.

FORRÁS: BALASYS

CSELEDI SÁNDOR, BALASYS

– Milyen új termék fejlesztésével foglalkozik a Balasys?

– A legújabb k+f tevékenységünk az ipari rendszereket kiszolgáló IT hálózatokra összpontosít. Ami régebben csak a jövőkutatók fejében létezett, mára már kézzel fogható valósággá vált: az ipari környezetünket is átszövik már az egymással összefüggő hálózatok. Gondoljunk csak a vízellátásra, a villamos áramra, a közlekedési rendszerekre vagy a távközlési hálózatokra – minden összefügg mindennel.

Az ipari vezérlőrendszerek (Industrial Control Systems, ICS) képezik az alapját a kritikus infrastruktúrának, többek között az energia- és vízellátás, a közlekedés és az ipari termelés terén is. Könnyen belátható tehát, hogy az ICS elleni kibertámadások következményei miért romboló hatásúak. Ezért az ipari vezérlőrendszerek biztonságára összpontosítva dolgozunk egy olyan tűzfal-koncepción, mely ezt a speciális piaci igényt lefedi.

– Milyen kihívásoknak kell megfelelni egy ennyire speciális termék fejlesztése során?

– Ha egy ipari környezetet támadás ér, könnyen lehet, hogy az irányítás elvesztése lesz a legkisebb gondunk. A támadások hibás működést eredményezhetnek, vagy akár a termelés teljes leállásához is vezethetnek, személyi sérülést, illetve környezeti kárt okozhatnak. Sajnos, minden ipari rendszer ki van téve hálózati támadásoknak.

Az egyre szofisztikáltabb, célzott, APT-támadások mellett az ICS/SCADA rendszereket fenyegető kártevők és zsarolóvírusok megjelenése, és a folyamatosan gyorsuló ipari digitalizáció különösen sürgetővé és fontossá teszi egy erre megoldást jelentő termék piaci bevezetését. Célunk, hogy az ICS-ek IT-biztonságát a lehető leghatékonyabban növeljük. Ezért a Balasys által fejlesztett biztonsági átjáró igazodik az adott környezet jellemzőihez, miközben nem feledjük: a biztonsági intézkedések sosem mehetnek az ipari folyamatok kárára.

– Kinek javasoljátok az új megoldást?

– Biztonságtudatos hazai iparvállalatoknak és közműszolgáltatóknak. Az ismert támadások és anomáliák kiszűrésére és a korszerű fenyegetések vizsgálatára fejlesztett átjárónk határvédelmi feladatokat is ellát, általa magas biztonsági szint érhető el. Eszközünk megoldást jelent az ICS hatékony védelmére – legyen az akár önálló rendszer, vagy kapcsolódjon egy már meglévő kiberbiztonsági rendszerhez.

Az átjáró ráadásul a SOC, SIEM, CDM (Continuous Diagnostics and Mitigation) és az egyre népszerűbb monitoring rendszerek számára is adatokkal szolgál. Bevezetése olyan vállalatok számára javasolt, amelyek több telephellyel és kiterjedt ICS-infrastruktúrával rendelkeznek, vagy korlátozott erőforrással bíró termelő-, illetve ipari cégek.

– Hogyan kell elképzelni egy ilyen megoldást?

– A legkülönfélébb ipari és közüzemi vállalatokról van szó, így nem egy dobozos terméket fejlesztünk. A projekt szerves részei az algoritmusok, az implementációhoz szükséges szoftverrendszerek, illetve egy a fenti rendszereket futtató platform. De nemcsak egy biztonsági platformról beszélünk, hanem értéknövelt szolgáltatásokról is, ezt másképp nem is lehet. A bevezetési és támogatási szolgáltatásokon túl, konzultációval, testre szabással, sőt akár egyedi fejlesztéssel is kiegészülhet egy ilyen projekt. Ha valaki érdeklődik a megoldás iránt, akkor bátran vegye fel velünk a kapcsolatot, és az iparágára jellemző sajátosságokat figyelembe véve együtt testre szabjuk, finomítjuk a megoldást. ■

VAJON CSÚNYÁK-E MALWARE-BITEK KÖZELRŐL?

Másképp látni

„Bocsássák meg nekem, eldurrantom azt a közhelyet, hogy a 2020-as év úgy fog bevonulni a történelembe, mint amelyik sokunkat megtanított másképp látni bizonyos dolgokat. Kora tavasz óta meghatároz minket a pandémia, ehhez kellett igazítanunk a privát és a professzionális életünket is. Tegye fel a kezét, aki meg sem próbálta elképzelni vizuálisan, hogy hogyan terjed a kórokozó, mi történik, amikor bejut a szervezetünkbe", vezeti be mondandóját Csinos Tamás, a CLICO ügyvezetője.

FORRÁS: CLICO

CSINOS TAMÁS, CLICO

„Mindig lenyűgözve néztem azokat az ismeretterjesztő dokukat, ahol a szóban forgó tárgytól, legyen például az emberi test, a felvétel messziről indul, és ilyen »fly over« módban, egyre jobban közelit, nyilván a megfelelő pillanatban csodálatos animációkra vált, tengeralattjáróként megjelenünk a véráramban, ahol közelről szemlélhetjük a vörös és fehérvérsejtek küzdelmét a betolakodókkal, drámai aláfestő zenékkel, érdekesebbnél érdekesebb kameraállásokból. Az informatikai hálózatokban majdnem ilyen izgalmas tudna lenni a bitek és bájtok, a csomagok, a munkamenetek – sessionök – megfigyelése. Bárcsak erről is forgatnának ilyen érdekfeszítő filmeket, gonosz, soklábú lényeknek ábrázolva a behatolók rosszindulatú eszközeinek kommunikációját, ami ellen a mi hős TCP-fejléceink és csillogó UDP-páncélunk varázsütésre felveszi a harcot, és leállítja, meggátolva a kór terjedését", folytatja Csinos Tamás.

Ha ezt az allegóriát megpróbáljuk kicsit a realitáshoz közelíteni, akkor az első problémánk, hogy szükségünk lesz különböző „mikroszkópokra", amelyekkel belenézhetünk a rendszereinkbe. Más eszköz kell, hogy a hálózatunkra és a csatlakozó eszközökre lássunk rá, más, hogy a felhasználói tevékenységet lássuk, más, hogy az üzemeltetőinket láthassuk.

Más kontextusok derülnek ki, ha a felhasználói tevékenységeket a munkaállomáson monitorozzuk, más, ha az üzleti alkalmazások és a használójuk szerepköre függvényében vizsgáljuk. Az IT – és ezen belül az IT-OT biztonság – nem annyira kiforrott, régi tudomány, mint az orvoslás vagy természetismeret. Itt még nem véglegesek sem az alkalmazott eszközök, sem az azokat használni képes szakemberek csoportosításai. (V.ö.: szakorvosi rendszer például…) Majdnem mindenkinek egyszerre kell specialistának és generalistának is lennie, folyamatosan új és újabb koncepciók, eszközök, eljárások jelennek meg és tűnnek el.

A magunkfajta sárkányfűárusok abban tudnak talán az olvasó segítségére lenni, hogy egy-egy problémára a megfelelő eszközt és a partnereink közül a legalkalmasabbat ajánljuk a tárházunkból, amivel remélhetőleg könnyebb lesz a céges véráramba igyekvő rosszindulatú dolgok kiszűrése, és az ellenük való küzdelem. ■

A MÁSODIK HULLÁMRA FELKÉSZÜLNI FÉLNETEK NEM KELL JÓ LESZ

Vírusok árnyékában – az első hullám

FORRÁS: ITB

SCHNECK ZSOLT, SHIELD INFORMATICS

COVID. Ez a mozaikszó alapjaiban írt felül sok mindent, amit eddig tettünk, vagy gondoltunk. A világ megváltozott. Ezt mára biztosan elmondhatjuk. Nem egészen fél év alatt változtatni kényszerültünk az életmódunkon, a szokásainkon, megváltoztak a munkakörülmények és gyökeresen megváltozott a gondolkodásmódunk azzal kapcsolatban is, hogy milyen az ideális, immáron távmunkára felkészített IT-környezet. (A cikk szerzője: Schneck Zsolt, a Shield Informatics ügyvezetője)

Nem volt egyszerű. Azok a vállalkozások, amelyek nem vették komolyan az Ázsia felől érkező híreket és fenyegetést, bizony komoly lépéshátrányba kerültek. Akik viszont időben léptek, akár komoly versenyelőnyt szerezhettek a piacon. Az IT-szektor szinte azonnal mozgásba lendült, és sorra készítette fel a bajban lévő cégeket az otthoni munkavégzésre, hiszen Európa déli részén már volt tapasztalat, jól lehetett látni, hogy nem lesz elkerülhető a karantén.
Nagy munkát végeztünk, mi üzemeltetők is. Két héttel a korlátozások bejelentése előtt már teljes fordulatszámon pörgött mindenki, sorra készítettük föl home office üzemmódra a számítógépeket és a felhasználókat, és mire megtörtént a tényleges bejelentés, partnereink készen álltak arra, hogy az üzletmenetük gyakorlatilag a dolgozóik otthonába költözzön. Megérkezett az első hullám.
Úgy gondoltuk, hogy jó munkát végeztünk, kicsit kifújjuk magunkat, és majd megy minden szépen a maga útján. Nem is tévedhettünk volna nagyobbat. Hamar kiderült, hogy bár az általunk tervezett és épített infrastruktúrákat a rugalmasságukból adódón gyorsan és hatékonyan át tudjuk állítani, sem a cégeknél sem pedig a dolgozóknál nincs igazán kultúrája a home office-nak. Sem a feladatok kiosztása, sem pedig az ellenőrzés nem ment gördülékenyen, így a dolgozók sem igazán tudták mit kezdjenek a rájuk szakadt látszólagos szabadsággal.
Gyakori eset volt, hogy sokkal többet dolgoztak, mint amennyit a munkahelyükön tették volna, és ez bizony könnyen felborította a munka és a családi élet kényes egyensúlyát. Természetesen ennek az ellenkezője is előfordult, de egyáltalán nem ez volt a jellemző. Azonban minden nehézség ellenére úgy tűnt, hogy az átállás nem volt minden esetben zökkenőmentes, a világ nem állt meg, és a munka is szépen haladt az új körülmények között.

A home office mellékhatásai

Persze, ha jön a baj, akkor jön csőstül. Ahogy arra sokan számítottunk, kihasználva a kialakult zavaros helyzetet és a könnyebben támadható otthoni munkakörnyezeteket, a kibertérben dolgozó bűnözői csoportok is elkezdtek stratégiát váltani. Egyre nagyobb számban jelentek meg a szemlátomást nagy energia- és időbefektetéssel előkészített phising támadások, és minden eddiginél nagyobb intenzitással tértek vissza a zsarolóvírusok, nyomást helyezve a kiemelt területekre.
Kórházak, húsüzemek és egyéb kritikus szolgáltatást nyújtó vállalkozások és közintézmények estek áldozatul a célzott támadásoknak, komoly fejtörést okozva a biztonsági szakembereknek és a rendszergazdáknak. Nem vitás, a kiberbűnözők nagy erőket mozgattak meg, hogy a lehető legnagyobb bevételt realizálják a világban zajló virulens időszak alatt. Tehették mindezt úgy, hogy az IT nem, vagy csak nagyon nehezen tudta megvédeni a már shadow IT-ként működő, otthoni munkavégzésre ítélt munkavállalók informatikai eszközeit. Rémálom.
Hiszen gondoljunk csak bele. Mi minden lehet egy felhasználó otthoni gépén? Nem tudjuk. Nem is tudjuk megvédeni őket. Hamar át kellett gondolni a stratégiát, így a legtöbb energiát kellett átcsoportosítani a központi rendszerek védelmére; valamint kiemelt jelentőséget kaptak a személyes vesszőparipáim, ugyanakkor a cégvezetők által többnyire marginálisnak tartott megoldások, a biztonsági mentés, valamint a határ- és a vírusvédelem. A terv végül sikerült, a partnereink adatvesztés nélkül vészelték át ezt a nehéz időszakot. Lassan de biztosan, kezdett helyreállni a rend. Mintegy három hónap után visszatért az élet a vállalkozásokba.

Azért kell hosszasan elemezni a múltat, hogy minél pontosabban lássuk a jövőt

Vajon megnyugodhatunk?

Találkozhattunk a barátainkkal, beülhettünk egy korsó sörre. Magyarországon látszólag helyreállt újra a béke. Csakhogy a szakemberek nem hiába figyelmeztetnek, hogy ez a béke meglehetősen törékeny, várható a második hullám. Meglehet, hogy így lesz, de akár az is elképzelhető, hogy a vírus most már velünk marad, az életünk része lesz. Nem tudhatjuk. A mi dolgunk, hogy megtegyünk mindent, ami IT szempontból lehetséges, hogy ha tényleg újra változtatásra kényszerülünk, akkor a reakció a lehető leggyorsabb és leghatékonyabb legyen.
Mi, a Shieldnél, úgy gondoljuk, hogy azért kell hosszasan elemeznünk a múltat, hogy minél pontosabban lássuk a jövőt. Tanultunk az első hullám okozta sokkból, így készen állunk a feladatra. Tudjuk, hol és hogyan kell megerősíteni a védelmi vonalakat. Azt is, hogyan és milyen eszközökkel kell majd segítenünk a cégvezetők munkáját. Folyamatosan értékeljük a kockázati tényezőket, hogy ha mégis eljön az idő, akkor a lehető legjobb megoldásokat tudjuk szállítani, és hasonlóan sikeres legyen a válságmenedzsment, mint az első hullám esetén.
Sokan kérnek tőlem tanácsot, hogy mit lehetne tenni a jelenlegi helyzetben. Én egyértelműnek látom a helyzetet. A legfontosabb dolog, hogy felmérjük, kiértékeljük és tanuljunk az elmúlt hónapokból és levonjuk a tanulságokat. Mikor hoztunk helyes döntést? Mikor hibáztunk? Nézzük meg, milyen IT-biztonsági eszközök állnak rendelkezésünkre, amelyekkel a lehető legnagyobb biztonságot tudjuk adni a szervezetnek. Végül azt is gondoljuk végig, hogy ezek a megfelelő számban és minőségben állnak-e rendelkezésre a tervünk végrehajtásához.
Mert ahogy mindig, a második hullámban is egy dolog áll majd a középpontban. Az ember. *(X)*

JELENTŐSEN VISSZAESIK AZ ÜZLETI ÉLETBEN A SZEMÉLYES TALÁLKOZÓK SZÁMA

Új sztárok a kommunikációban

FORRÁS: MICROSOFT.COM

Pár hónap alatt közel tízszeresére nőtt a Teams használata, a Zoom majdnem hétszeres bővülést ért el – ezek a számok is jól érzékeltetik, mekkora karriert futottak be az elmúlt időszakban a kommunikációs szoftverek. Kiemelt szerepük lehet a következő években is, a személyes üzleti találkozók aránya ugyanis várhatóan jelentős mértékben csökken majd.

A legjobban sikerült nyaraláson készült szuper fotó, egy közismert épület belseje, vagy egy lélegzetelállító természeti látványosság – valószínűleg a legtöbb irodai dolgozó, aki hónapokra otthoni munkavégzésre kényszerült, találkozott ilyen háttérképekkel és valószínűleg saját maga is használt hasonlókat, hogy így dobja fel a videókonferenciák hangulatát, vagy egyedivé tegye saját bejelentkezését.

A koronavírus-járvány egyik legszembetűnőbb hatása lett, hogy kisebb-nagyobb mértékben szinte mindenkinek szakértővé kellett válnia a csoportos virtuális megbeszéléseket támogató szoftverek használatában és persze

a gyártók is nagyon hamar ráéreztek a lehetőségre, és gőzerővel fejlesztették az olyan kiegészítő funkciókat, amelyeknek köszönhetően a vicces, vagy éppen meghökkentő, egyedi hátterek megjelenhettek a munkahelyi megbeszélések során a képernyőkön, és megvalósulhattak több tucat, vagy akár több száz fős konferenciahívások is, például a felsőoktatásban.

Még az idén 25 százalékkal nőhet a felhőalapú konferenciamegoldások piaca

Drasztikus növekedés

A távmunkára és digitális oktatásra történő átállás egészen elképesztő növekedést hozott a kommunikációs szoftverek esetében. Az Aternity nevű, a digitális élmények elemzésével és javításával foglalkozó cég felmérése alapján a Microsoft Teams használata 2020. február 17. és június 14. között 894 százalékkal nőtt, míg a Zoom esetében 677 százalékos bővülést mértek.

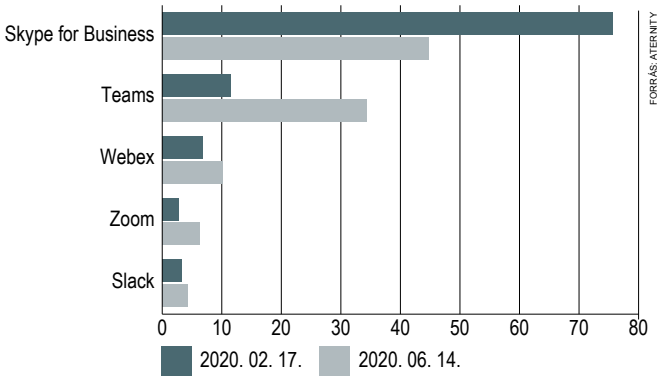
Vagyis a korábban jelentős fölénnyel vezető Skype for Business sokat veszített piaci részesedéséből, és az Aternity azt prognosztizálta, hogy a Teams – vagyis egy másik Microsoft-megoldás – valószínűleg át is veszi a vezető helyet ebben a szegmensben. De látványos fejlődést tudott felmutatni a Cisco Webex alkalmazása is, a cég közlése szerint az ezen keresztül lebonyolított különböző hívásokban áprilisban már 500 millióan vettek részt, és összesen 25 milliárd percig használták.

Nagy kérdés, hogy mit hoz a jövő a csoportmunkát, illetve a kommunikációt támogató szoftvereknek. A munkavállalói és munkáltatói visszajelzések alapján nagyon valószínű, hogy az irodai munkában nem áll vissza a helyzet a járvány előtti időszakra, vagyis a jövőben is szükség lesz ezekre a megoldásokra, persze, nem feltétlenül ekkora intenzitással.

A Gartner prognózisa szerint egyébként drámaian csökkenni fog az elkövetkező néhány évben az üzleti kapcsolattartásban a személyes jelenléttel járó találkozók száma. A kutatócég előrejelzése szerint míg a pandémia előtti időszakban az ilyen üzleti események mintegy 60 százalékban személyes találkozással jártak, addig 2024-re az ún. kontakt találkozók aránya mindössze 25 százalék lesz.

Kommunikációs szoftverek használata

Százalék, a használat arányában



A Zoom esete

A cég 2021-es üzleti évének első negyedéve április végén zárult, vagyis pont arról az időszakról volt szó, amikor kiderült, hogy világméretű krízisről van szó, és például Kínában és Európában szinte minden iroda, illetve oktatási intézmény kiürült. A vállalat ebben a periódusban 328,2 millió dolláros árbevételt ért el, ami az amerikai technológiai óriások sokmilliárd dolláros forgalmához képest persze elenyésző, azonban 169 százalékkal múlta felül az egy évvel korábbit. De talán még érdekesebb, hogy a tíznél több munkatárssal rendelkező fizetős ügyfeleik száma átlépte a 265 ezret, ami éves összevetésben már 354 százalékos bővülést jelent.

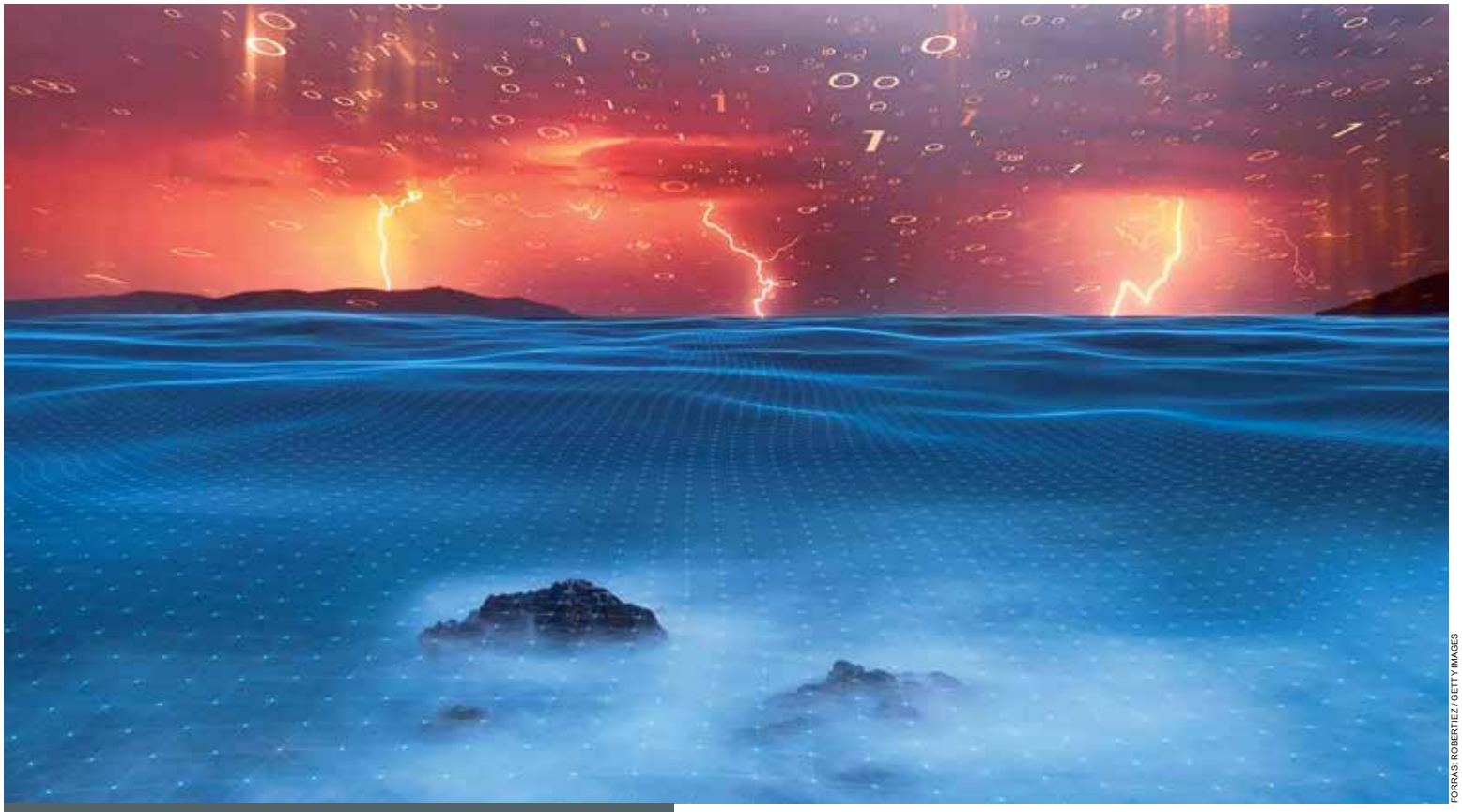
Színezik a képet a Zoommal kapcsolatos IT-biztonsági aggodalmak, amelyek akkor is befolyásolják a piacot, ha minden hibát régen (hónapok óta) megoldott a cég, és a felhasználói oldalon is kialakultak a jó gyakorlatok.

Megoldásra váró kihívások

A Gartner felmérte azt is, hogy a kommunikációs szoftverek piacára milyen hatással lesz a megváltozott helyzet. Elemzésük szerint a felhőalapú konferenciamegoldások esetében idén majdnem 25 százalékos bővülés jöhet, ugyanakkor továbbra is egy viszonylag kis szegmensről beszélhetünk. Míg tavaly világszinten 3,3 milliárd dollárt költöttek ilyen rendszerekre a vállalkozások, addig idén ez az összeg 4,1 milliárd dollár körül alakulhat.

A március-áprilisi események azt is jól megmutatták, hogy melyek azok a területek, ahol fejlődésre van szükség ezeknél a szoftvereknél. Szinte mindenki szembesült azzal, hogy időnként akadozott a hang, elment a kép, esetleg megszakadt a kapcsolat. A távmunkára és digitális oktatásra történő átállás során akkora terhelést kaptak a távközlési hálózatok, ami rontotta a kommunikációs szoftverek felhasználói élményét is, épp ezért érdemes elgondolkodniuk a gyártóknak, hogy milyen eszközökkel lehet kezelni ezt a problémát.

A másik fontos kérdés a biztonság, ami a tűzoltás-szerű átállás során talán kevesebb figyelmet kapott, de a helyzet normalizálódásával kulcsfontosságú lesz, hiszen az IT-biztonsági cégek jelentéseiből jól látszik, hogy a kiberbűnözők is meglátták a lehetőséget a járvány miatti megváltozott helyzetben, és kifinomult támadásokkal igyekeznek behatolni a vállalati rendszerekbe, amihez például jó „kiskapukat” kínálhat a távmunka. ■



FORRÁS: ROBERTIEZ / GETTY IMAGES

FELHŐTECHNOLÓGIA

A mindennapok hőse

Míg az év elején még az elérhető költségcsökkentés terelte a felhőtechnológia felé a vállalatokat, a járványügy intézkedések erőteljesen megnövelték a felhő iránt érdeklődő vállalatokat. A magyar piacon a felhő megoldások iránti bizalmatlanság fogja vissza a technológia térnyerését.

Ha nagy szavakat szeretnénk írni, akkor a felhőtechnológiát is a mindennapi hősök között kellene ünnepelnünk. „Ő" tette ugyanis lehetővé, hogy a járványhelyzetben a gazdaság ne álljon le teljesen, az emberek tudjanak otthonról is dolgozni, vagy online vásárolni, konferenciákon részt venni. Vagyis életben tartotta a gazdaságot.

A távmunka-megoldások népszerűek

Nem meglepő, hogy a Gartner júliusban publikált adatai szerint publikus felhőszolgáltatás terén desktop as a service (DaaS) szolgáltatás piaca idén 95,4 százalékkal bővült. A DaaS költséghatékony lehetőséget biztosít azoknak a vállalatoknak, amelyek távolról dolgozó munkatársaikat szeretnék biztonságos és hatékony eszközökkel ellátni, hogy segítségükkel több helyről és több eszközről is elérhessék a vállalati erőforrásokat. A járványhelyzet kezdetén a technológia kicsit megbicsaklott a hirtelen megnövekedett terhelés alatt, de a kezdeti nehézségeken túllépve azt adta a vállalatoknak, amit elvártak tőle: rugalmas, igény szerint növelhető erőforrásokat, melyek költsége menet közben, igénybevétel szerint alakul.
Miután a vállalatok a biztonságos távoli munkavégzési eszközökkel ellátták

otthonról dolgozó munkatársaikat (akik egy része nem is tér már vissza az irodába: a vállalatok 74 százalékánál az alkalmazottak 5 százaléka állandóan home office-ből dolgozik), a többi eszközökön a sor. A Gartner becslése szerint 2020 második felében a vállalatok a kollaborációs eszközök távoli munkavégzésre történő kiterjesztésén, a mobileszköz-menedzsment központosításán dolgoznak gőzerővel. Előtérbe kerülnek a távoktató megoldások, a biztonság és a mindehhez szükséges infrastruktúra felhő alapú igénybevétele.

Egy felhő is jó, de a több felhő jobb lehet

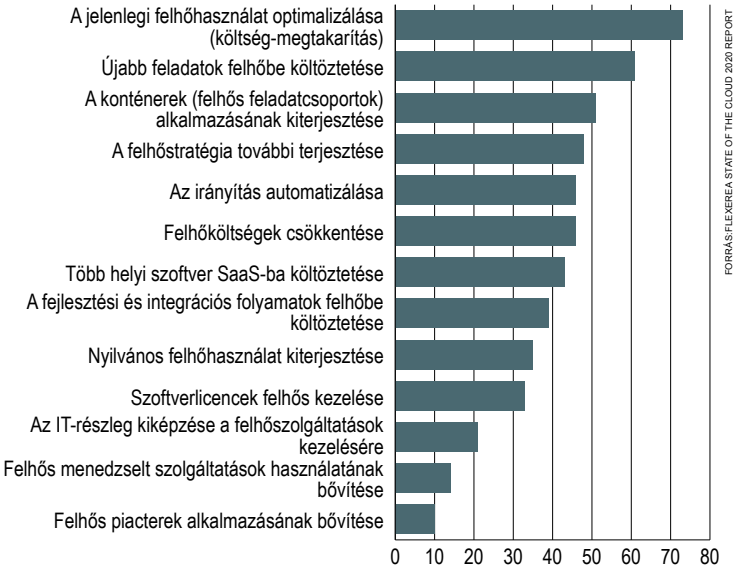
A járványon túltekintve a vállalatoknak érdemes a multicloud megoldások iránt érdeklődni. Segítségükkel a vállalatok kétharmada csökkenti függőségét az különböző gyártóktól, azonban az alkalmazások hordozhatósága csak részben valósul meg.

Az alkalmazások hordozhatósága azt jelenti, hogy egy vállalati appot változtatás nélkül lehet egyik platformról a másikra költöztetni, és a multicloud stratégia előnyeként tekintenek rá a cégek. Azonban a valóság az, hogy nagyon kevés alkalmazás költözik egy másik platformra, ha azt egyszer már a termelésben, a napi tevékenységben aktívan használja a vállalat. A multicloud stratégiák többsége inkább a beszerzésre, működésre és kockázatkezelésre összpontosít, kevésbé fontos a hordozhatóság.

Azok a vezetők, akik a multicloud stratégia mentén szeretnének haladni, el kell döntsék, hogy milyen problémát szeretnének segítségével orvosolni: csökkenteni a gyártótól való függést vagy a szolgáltatás leállásának kockázatát kezelnék. A vezetőnek meg kell értenie, hogy a multicloud stratégia nem oldja meg automatikusan az alkalmazás hordozhatósági kérdéseket.

A legfontosabb felhőalkalmazási motivációk 2020-ban

A 750 válaszoló százalékában



A szakértelem hátráltatja a technológia terjedését

A Gartner szerint 2022-ig még mindig kevés lesz a felhőtechnológiához értő szakember a piacon, így az infrastructure as a service (IaaS) piacon legalább két évet késik a vállalatok felhőbe költözése. Az mai cloud migrációs stratégiák inkább a költözésről, mintsem a folyamatok modernizálásáról, átalakításáról szólnak. A költözés nem fejleszti a natív felhő képességeket. Olyan piac alakul ki emiatt, amelyen a szolgáltatók nem tudják elég gyorsan képezni és tanúsítani a szakembereket az erős kereslet miatt.

A megoldás olyan rendszerintegrátor vagy menedzselt szolgáltatók igénybevétele, amelyek az adott iparágban már rendelkeznek tapasztalattal, van kész projektjük az adott területen. Ezek a partnerek eléggé tapasztaltak abban is, hogy a várható költségekről és az elérhető megtakarításokról valós adatokat szolgáltassanak.

Közelebb az ügyfélhez

A felhőszolgáltatók egyre közelebb költöznek a kiszolgált ügyfélhez, nagyon sok service provider arra összpontosít, hogy szinte minden utcasarkon elérhető legyen egy adatközpontjuk. Egyre több régiót fednek le közvetlen jelenlétükkel: például, ahol nagyon sok vállalati ügyfél veszi igénybe szolgáltatásukat, ott állandó adatközpontokat állítanak fel. Egy-egy kiemelt esemény helyszínén az ideiglenesen megnövekedett igényeket ún. pop-up adatközpontokból szolgálják ki. A közelség azt is jelenti, hogy a szolgáltatások késleltetése már-már elhanyagolhatóvá válik, esetenként közvetlenül a felhőszolgáltató natív központjából, infrastruktúra kiépítése nélkül vehetők igénybe a felhőmegoldások. ■

A magyarok félnek költözni

A magyar vállalatok a kedvező tapasztalatok ellenére sem mernek a felhőbe költözni, mert jellemzően nincs üzemeltetési tapasztalatuk, bár azt elhiszik, hogy felhőben sokkal magasabb a biztonsági szint. Nincs jelentős konfigurációs tapasztalat, nem tudják, pontosan hogyan kell védekezni felhőben. Nem ismerik pontosan, hogyan oszlik meg a felelősség felhőszolgáltatás esetében – pedig ez egy jól szabályozott terület. Már léteznek általánosan elfogadott gyakorlatok: például, ha valaki software-as-a-service jellegű szolgáltatást vesz igénybe, akkor a szolgáltatáshoz való hozzáférésért, a felhasználók autentikációjáért az ügyfél a felelős, míg a többiért a szolgáltató. Ha viszont csupán erőforrást vesz igénybe az ügyfél a felhőből (CPU-t, tárolást), akkor az ügyfél felelőssége a nagyobb. Emiatt a magyar piacon továbbra is az óvatosság jellemző a felhőalkalmazásban.

vmware

FORRÁS: WIRE19.COM

BIZTONSÁGOS TÁVOLI MUNKAVÉGZÉS

Végpontok a felhőből védve

A távoli munkavégzés biztonságának garantálása az egyik legfontosabb információbiztonsági feladat lett az elmúlt hónapokban. A mobil végpontok védelmére olyan technológiát érdemes használni, amely mindenhova képes követni a felhasználót.

A digitális munkahely ma már nem csak az irodára korlátozódik. Még ha el is tekintünk a COVID vírusjárvány okozta hirtelen, de minden jel szerint tartósan velünk maradó változásoktól, a munkavégzés helyszínei már régóta magukba foglalják a partnerek, ügyfelek irodáit, a repülőtereket, szállodákat, az otthonokat, a kávézókat.
A vállalat és a szervezet határainak elmosódása viszont minden korábbinál nagyobb lehetőségeket kínál a kiberbűnözőknek. A világ vezető információbiztonsági szakértői szerint egyre gyakoribbak lesznek az olyan kifinomult támadások, ahol a hekkerek a hálózaton „oldalirányban" mozogva keresik az új célpontokat, egymástól (elvileg) elszigetelt rendszerek között ugranak át vagy éppen kikerülik a megállításukra indított lépéseket. Mindezeken túl a fejlett phishing-technikák, a bothálózatok és a zsarolóvírusok is mind sűrűbben fenyegetik a mégoly felkészült szervezeteket is.

Minél több adatból

A VMware Digital Workspace ONE rendszere egységes környezetet teremt a vállalati dogozóknak, végezzék munkájukat bárhonnan, bármilyen eszközről. Egy ilyen integrált környezet természetesen nem létezhet fejlett információvédelmi megoldás nélkül: ezt kínálja a VMware Workspace Security.
A megoldás sokat merít a VMware által nemrégiben felvásárolt Carbon Black technológiájából is. Onnan veszi például a végpontok telemetriai adatait és a gyanús vagy rosszindulatú viselkedésre utaló jeleket, majd ezeket az információkat összeveti a Workspace ONE egyéb natív vagy külső felektől származó adataival. Ennek révén mélységeiben, mégis jól áttekinthető módon tudja megjeleníteni a digitális munkakörnyezet biztonsági állapotát és olyan információkkal szolgál, amelyek megkönnyíti az adatokra alapozott döntések meghozatalát.
A teljes megoldásnak két fő komponense van: a VMware Workspace ONE Intelligence és a VMware Carbon Black Cloud. Előbbi mély betekintést tesz lehetővé a teljes digitális munkakörnyezetbe, illetve elemzi az összes alkalmazás viselkedését. Az erőteljes automatizációnak köszönhetően segít optimalizálni a védekezésre rendelkezésre álló erőforrásokat és megerősíteni az infrastruktúra védelmét.
A Carbon Black Cloud egy felhőben futtatható végpontvédelmi platform. Míg más végpontvédelmi technológiák csak az ismert fenyegetettségekre, veszélyekre vonatkozó és utaló adatokat gyűjtik be, a Carbon Black Cloud folyamatosan és átfogóan gereblyézi be a végpontok működéséről az információkat. Ez azért különösen fontos, mert a hekkerek előszeretettel álcázzák támadó tevékenységüket úgy, hogy az teljesen ártalmatlannak tűnjön. Ezt a viselkedési mintát elemezve képes felismerni és megállítani azokat a támadásokat is, amelyekkel korábban még soha nem találkozott.

Mire használható a Workspace Security?

– Megállítja a kártevőket, a zsarolóvírusokat és az egyéb támadási formákat.
– Automatikusan megelőzi a támadásokat, online és offline egyaránt.
– Blokkolja a vadonatúj, máshol még nem látott támadásokat, amelyeket más eszközök esetleg átengednének.
– Leváltja a nem kellően hatékony víruskereső megoldásokat.

FORRÁS: WIRE19.COM

Védelem és felügyelet

A Carbon Black szoftverszenzor automatikusan telepíthető a végpontokra, amikor azokat hozzáadják a VMware Workspace ONE környezethez. A szenzor telepítése után kezdődik meg a végpont telemetriai adatainak részletes gyűjtése és azok továbbítása a Carbon Black Cloud-ba. A Workspace ONE Intelligence rendszeresen, minden néhány percben lekérdezi az új riasztásokat és értesítéseket a felhőből. Utána ezeket az adatokat összeveti a saját magából, más VMware termékekből és a megbízható partnerektől származó adatokkal, így alkotva meg a teljes képet. Szükség esetén a korrelációk alapján automatikus válaszlépések is indíthatók. Innentől kezdve a technológia megkönnyíti a biztonsági kitettség csökkentését és a támadásokra való villámgyors reagálást, függetlenül a végpontok földrajzi elhelyezkedésétől.

A távoli munkavégzés sokszor megbízhatatlan hálózati kapcsolatokon keresztül zajlik. A Carbon Black-et használva a felhasználó akkor is védve lesz, ha a hálózat nem kellően stabil. A hagyományos végpontvédelmi eszközök nem frissítik magukat, ha nem tudnak kapcsolódni a vállalati hálózathoz. A Carbon Black Cloud gondoskodik arról, hogy minden eszköz a lehető legfrissebb védelemben részesüljön, bármikor, bárhol a világon.

Könnyen előfordulhat, hogy a munkatársak kénytelen az éppen rendelkezésre álló eszközről végezni munkájukat – ami azt jelenti, hogy kevésbé biztonságos, otthoni használatra szánt gépekről érnek el kulcsfontosságú vállalati adatokat, erőforrásokat. Ez alapesetben óriási veszélyt jelentene, de a Carbon Black Cloud szenzorait gyorsan telepíteni lehet bármelyik eszközre, és attól kezdve a dolgozó otthoni tabletje vagy laptopja vállalati szintű biztonsággal fog rendelkezni.

Nem csak a védekezésre használható a Carbon Black Cloud. Segítségével az informatikai üzemeltető csapat az irodán kívül tartózkodó mobil eszközöket is folyamatosan nyomon követheti. Nem csak azt láthatják, mi történik velük és rajtuk (természetesen a személyiségi jogok betartása mellett), hanem a távolból lesznek képesek sérülékenységeket azonosítani, hibajavítást telepíteni és validálni a konfigurációs beállításokat. És ami még jobb, az akkor is működik, ha az üzemeltetési vagy biztonsági csapat maga is a távolból dolgozik, ami járványidőszakban könnyen előfordulhat.

Üzemeltetés és biztonság kéz a kézben

A Carbon Black egyedi prevenciós technológiája tökéletesen alkalmas arra, hogy leváltsa a hagyományos vírusirtó rendszereket. Prediktív modellező módszere révén képes azonosítani és elhárítani a végpontok ellen indított legtöbb ismert és nem ismert támadást, beleértve a kártevőket, a fájl nélküli támadásokat és a zsarolóvírusokat. A részletes telemetriai adatoknak köszönhetően átfogó, mégis világos képet kínál a végpontokon zajló tevékenységekről. Használatával egyszerűen megkereshetjük és megvizsgálhatjuk a kérdéses végpontokat, nyomon követhetjük a támadás folyamatát és megtalálhatjuk a mélyen fekvő okot, hogy a ténylegesen gondot okozó biztonsági rést zárjuk be.

A Carbon Black segít lerombolni a falakat az IT-üzemeltetés és a biztonsági csapat között: egyszerű munkafolyamatai és beépített eszközei révén a két csapat együttműködésben adhat valós idejű választ az incidensekre, és azonnal kivizsgálhatják a támadásokat. *(X)*

TAKÁCS GERGELY

PRIBOJSZKI MÁRIA

BERECZ ÁDÁM

CZUCZUMANOV VALENTIN

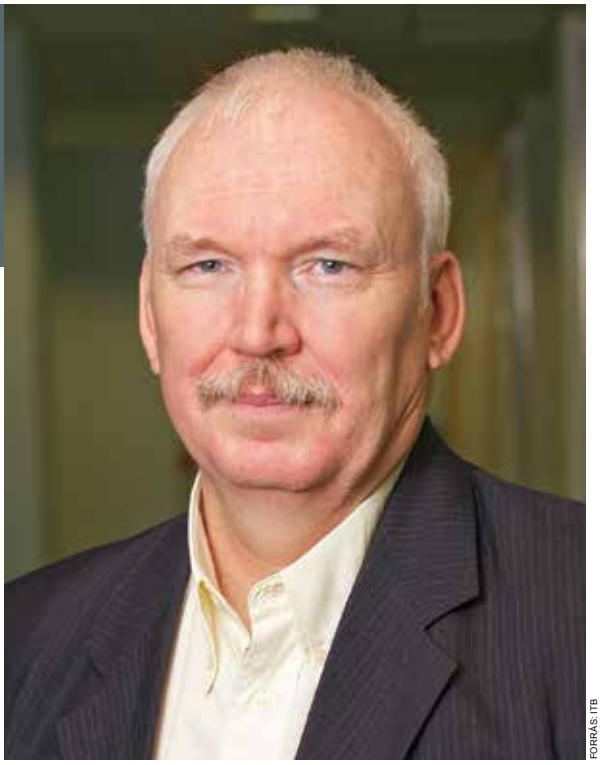
JUHÁSZ JÁCINT

FORRÁS: ITB

MÁR ITTHON IS ELÉRHETŐ AZ ALSO FELHŐ PIACTÉR

Több ezer viszonteladó használja Európában a szolgáltatást

Rengeteg felhőszolgáltatás egy helyről, értéknövelt szolgáltatások a platform fejlesztőjétől, a gyors piaci bevezetés lehetősége – többek között ezeket az előnyöket kínálja a partnerek számára az ALSO Felhő Piactere. Az itthon július eleje óta elérhető platformon folyamatosan jelennek meg újabb gyártók szolgáltatásai.



FORRÁS: ITB

NYIKES TAMÁS, ALSO HUNGARY

Július elején tette elérhetővé Magyarországon is Felhő Piacterét Európa egyik legnagyobb felhőplatform-szolgáltatója. Az ALSO megoldása lehetőséget kínál a felhőszolgáltatók, a felhőszoftvereket fejlesztő vállalkozások és a viszonteladó partnerek számára, hogy gyorsan, egyszerűen juttassák el szolgáltatásaikat ügyfeleik számára.

„A viszonteladó partnereink számára nagy előny, hogy nem a nulláról kell felépíteniük egy értékesítési felületet, hanem az ALSO által fejlesztett platformot használhatják ahhoz, hogy nagyon egyszerűen, mindössze néhány gombnyomással, webes felületen elérhetővé tegyék az általuk kínált felhőtermékeket és beárazzák azokat. Lényegében egy one-stop-shop megoldást nyújtunk számukra, amelyben gyorsan és egyszerűen állíthatnak össze szolgáltatáscsomagokat", mondta el *Nyikes Tamás,* az ALSO Hungary Kft. felhő szolgáltatások értékesítési vezetője.

Az ALSO 2014-ben hozta létre felhőszolgáltatási piacterét (az ACMP-t – ALSO Cloud Marketplace-t), ami lehetővé teszi, hogy viszonteladó partnerei saját ügyfeleik számára a lehető leghatékonyabb és legversenyképesebb módon nyújtsanak felhőszolgáltatásokat. A megoldást több ezer európai viszonteladó alkalmazza, és az idei második negyedév végén már közel ötmillió, az ACMP-n keresztül vásárolt licencet használtak, további 14 millió licenc pedig az ingyenes próbaidőszak szakaszában volt. Jelenleg már közel 90 gyártó szolgáltatásaiból válogathatnak a partnerek a platformon keresztül. A júliusban indult magyarországi Felhő Piactéren is már számos gyártó kínálata érhető el, és a következő időszakban is folyamatosan bővül majd ez a kör. ■

FELHŐ, KEDVEZMÉNYEKKEL

Cloud, startup, inkubáció

Könnyű egy startupnak, mert nincsenek öröklött informatikai rendszerei, amelyek akadályoznák a gyors fejlődésben. Nehéz egy startupnak, mert nincsenek öröklött informatikai rendszerei, amelyek biztosítanák számára a stabil, megbízható mindennapi működést. A legjobban persze akkor jár a startup, ha sikerül rugalmas, mégis stabil környezetet kialakítani maga számára, amely képes együtt nőni az igényekkel.

FORRÁS: ARUBA

A bevezetőben foglaltak miatt szokás azt tanácsolni a kezdő technológiai vállalkozásoknak, hogy az első években mindenképpen felhőmegoldásokat válasszanak. Nincs nagy beruházás, könnyen lehet új elemekkel bővíteni a szolgáltatáscsomagot, esetleg lemondani azokat, amelyekre már nincs szükség. Ilyen felhőszolgáltatást persze számtalan helyről igénybe lehet venni. Az Aruba azonban nemcsak a technológiát kínálja a startupoknak, hanem az üzleti tervek kidolgozásában és megvalósításában is segít nekik – mondja *Gyepes Máté,* az olasz központú felhőszolgáltató hazai képviseletének szenior marketing menedzsere. A több éves „We START you UP" program keretében technikai támogatás, oktatás és több millió forint értékű cloud kredit is jár a startupoknak.

FORRÁS: ARUBA

GYEPES MÁTÉ, ARUBA

Indulj be!

A jelentkezés fő feltételei, hogy a cég háromévesnél fiatalabb legyen, és innovatív technológiai területen működjön. A jelentkezés egyszerű online űrlap kitöltésével történik, és az sem akadály, ha a vállalkozás részt vesz valamilyen akcelerátor programban. A programot olyan vállalkozásoknak szánják, amelyek jelentős előnyöket szerezhetnek a felhő architektúrában történő működtetésből, mert például nem látják előre, milyen ütemben nő az informatikai erőforrások iránti igény, vagy a külföldi piacok meghódításához szükség van a globális infrastruktúrára, ismerteti az alapelveket Gyepes Máté. A program első része, a START szakasz, legfeljebb három évig tart. A kiválasztott startupok a program időtartama alatt minden évben kapnak egy 1 millió forint értékű cloud kreditet, amelyet az Aruba Cloud bármely szolgáltatására felhasználhatnak – vagyis összesen hárommillió forint értékű ingyen szolgáltatásban részesül az arra érdemes vállalkozás. Mindezt képzési anyagok, videók és folyamatos technikai támogatás egészítik ki. Az elérhető szolgáltatások között van a számítási kapacitás igénybe vétele, virtuális privát szerver, tárterület és monitoring.

Irány felfelé!

A legjobbaknak azonban tovább is vezethet az útjuk a program második, UP szakaszába. Az Aruba minden évben kiválaszt három, ígéretes startupot azok közül, amelyek már egy éve részt vesznek a START szakaszban. Ehhez először át kell jutni egy online szűrőn, majd a Pitch Dayen személyesen is be kell mutatni az üzleti tervet, és meg kell győzni a döntéshozókat, hogy rejlik potenciál a vállalkozásban – és valóban kamatoztatni tudja növekedésében a felhőtechnológia kínálta előnyöket. A győztesek ezúttal két évig érvényes, 15 millió Ft értékű cloud kreditet nyernek, emellett ingyenes konzultációs lehetőséget kapnak az Aruba szakértőitől, hogy optimalizálják az infrastruktúrát, és a lehető legtöbbet hozzák ki az Aruba Cloud megoldásokból. Mindezeken túl az Aruba a programon belül külön fejezetet szentel a győzteseknek, ezzel is erősítve a startup profilját és ismertségét. ■

DIGITÁLIS EGÉSZSÉGÜGY

Egy vírus és következményei

Az idei év már alighanem a COVID-19 jegyében és árnyékában telik el. A világjárvány az egészségügyi digitális megoldások amúgy is dinamikus fejlődésének is új lendületet adott.

FORRÁS: PHYSICSWORLD.COM

Személyre szabott gyógyszerek, egyedi génterápia, mesterséges szervek és végtagok, a távolból, robotokkal végzett műtétek – a digitális orvosi megoldások fantasztikus lehetőségeket ígértek. Aztán jött a COVID-19, és kiderült, hogy az egészségügyi rendszereket egy kicsit komolyabb globális influenza-járvány is szinte megoldhatatlan feladat elé állítja. Ezzel együtt viszont arra is ráirányította a figyelmet, hogy a digitális egészségügyi megoldások milyen óriási mértékben segíthetik az orvoslás minden területét, a megelőzéstől az ellátás szervezéséig.

A távolság nem akadály

A digitális orvoslás számos, amúgy korábban is ígéretesnek tartott területe jókora szteroid-injekciót kapott a járvány idején. Az egyik jellemző példa a telemedicina. Amikor a szokásos panaszokkal nem, vagy csak körülményesen lehet a háziorvosokhoz vagy a szakrendelőkbe eljutni, felértékelődik a beteg és az orvos távkapcsolata. Szerencsére egyre több az olyan megoldás, amely kiválthatja a rutinlátogatásokat.

Ezek egyik összetevőjét az életfunkciókra vonatkozó adatokat gyűjtő okos eszközök jelentik. Az okosórák és fitnesszkarkötők már nemcsak a pulzust mérik,

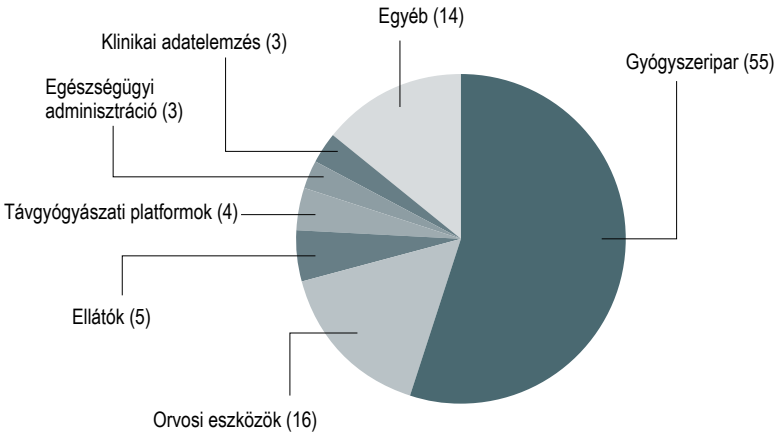
hanem esetenként a vér oxigénszintjét is, és jelzik a szívritmus-zavarokat. A testen elhelyezett vagy a ruhákba beágyazott szenzorok révén akár olyan létfontosságú méréseket is végezhetnek folyamatosan, mint az EKG vagy az EEG. A Medtronic nevű cég például olyan hordható technológiát tesztel, amely érzékeli, ha viselője eszik, és annak megfelelően hozza működésbe az automatikus inzulinpumpát.
Okostelefonnal kiegészítve a lehetőségek tovább bővülnek. Akár Magyarországon is nagy számban elérhetők olyan digitális vérnyomásmérők, amelyek az adatokat át tudják küldeni egy mobilappba, amely azokból hosszú távú elemzéseket készít, akár egyéb körülmények (időjárás, stresszhelyzet, testmozgás) figyelembevételével. Mindebből jelentést lehet összeállítani, amelyet a beteg elektronikusan elküldhet orvosának, akinek így nem a heti egyszeri mérésből kell megállapítania, hogyan is van páciense. A távdiagnosztika következő lépcsőjét jelenthetik azok az eszközök és alkalmazások, amelyek akár folyamatosan küldik a szükséges adatokat az ellátórendszernek, és riasztanak, ha vészhelyzet állt be.
A vírushelyzet amúgy is felhívta a figyelmet az egészségügyi mobilalkalmazásokra. A legtöbb országban készült olyan alkalmazás (Magyarországon a Vírusradar), amely a kontaktok felkutatásában segítette a hatóságokat, de emellett fejlesztettek információs vagy öndiagnosztikai appokat is.

MI a gyógyításban

A digitális egészségügy egy másik, nagy lendületben lévő területe a mesterséges intelligencia alkalmazása. Rendkívül nagy szerepe lehet a diagnosztikában, ahol akár milliónyi korábbi betegadattal és egyéb információval tudja összevetni egy páciens leleteit a kórkép és a legnagyobb sikerrel kecsegtető gyógymód megtalálásának elősegítésére.
A lehetőségek persze ennél sokrétűbbek és napról napra bővülnek. A Philips a kórházakban ápolt betegek távmonitorozására fejlesztett ki szoftvert és hardvert. Az adatok egy központba futnak be, ahol nem csak képzett orvosok figyelik azokat, hanem egy folyamatos gépi tanulást használó, MI alapú rendszer azt is előre tudja jelezni, ha várhatóan romlani fog a páciens állapota, majd ez alapján jó időben riaszthatja az orvosokat, ápolókat.

A digitális egészségügy sztárterületei

Milyen területekre adtak pénz az egészségipar legnagyobb befektetői (A befektetések számának százalékában, 2015-2020 között)



FORRÁS: CBINSIGHTS.COM

Óriási potenciál rejtőzik a gyógyszerkísérletek és hatásvizsgálatok MI-vel való megtámogatásában. Egy magyar startup, a Turbine például a daganatos betegségek gyógymódjának meghatározásánál veti be az MI-t. Egy szimulált sejtben molekuláris szinten modellezik a rák működését, majd ezen a modellen vizsgálják ki a különféle hatóanyagok és kezelések eredményességét. Ezzel nem csak a klinikai tesztek számát és idejét lehet radikálisan csökkenteni, de pontosabban meghatározható az egyes gyógymódok hatásmechanizmusa is.

Már Magyarországon is sok olyan digitális vérnyomásmérő kapható, amelyet össze lehet kötni okostelefonnal; és van olyan mobilapp is, amely trendelemzést készít

COVID: terjedési modellek és vakcinakutatás

Természetesen a COVID-19 járvány kezelésében is hatalmas szerep jut a mesterséges intelligenciának. Az elmúlt fél évben számtalan szervezet és vállalat készített MI alapú modelleket a járvány terjedésének előrejelzésére, a rejtett esetek arányának felderítésére vagy a szükségesnek vélt intézkedések hatásának vizsgálatára. Az eredményeket széles körben elérhetővé is tették – az már más kérdés, hogy a döntéshozók mennyire vették ezeket figyelembe …
A vakcinát és a hatékony gyógymódot kereső orvosok számára érdekes módon a tudományos publikációk feldolgozásában nyújt óriási segítséget az MI. A vírusról és a járványról szóló tudományos publikációk száma hetente ezres számban nő. Ember nincs, aki ezeket el tudná olvasni, a kutatásokhoz viszont fontos lenne ismerni mások eredményét. Az igényt felismerve hozta létre több szervezet a COVID-19 Open Research Dataset-et (CORD-19), amely több tízezer, a koronavírushoz kapcsolódó tanulmányt tartalmaz és amelyet folyamatosan frissítenek az új publikációkkal. Erre alapozva több olyan eszközt is fejlesztettek, amelyek révén a természetes nyelvi feldolgozás eszközeit használva könnyen kinyerhetők a kutatókat érdeklő fontos információk. ■

FORRÁS: ISTOCK

ÚJ TERÜLETEKEN TAROL A DOLGOK INTERNETE

14 ezer milliárd dollárral dobhatja meg a Föld GDP-jét az IoT

Óriási üzleti lehetőség rejlik az IoT-technológiában a megoldásszállítók, szolgáltatók számára, a Transforma Insights előrejelzése szerint a tavalyi 424 milliárd euróról 2030-ra 1300 milliárd eurósra nőhet a piac. Az ipar, a közlekedés vagy éppen az energiaszektor mellett egyéb területeken is egyre többen élnek a dolgok internete kínálta lehetőségekkel, számos projekt indult a kiskereskedelemben, az egészségügyben, illetve a mezőgazdaságban is.

Gyártás, közlekedés, okosváros-fejlesztések, energiaellátás – a legtöbben valószínűleg ezeket a területeket említenék, ha arra kérnék őket, hogy mondjanak szegmenseket, ahol aktívan használják az IoT- (internet of things – dolgok internete) megoldásokat. Bár az elmúlt években valóban ezekben az ágazatokból indult hódító útjára az a trend, hogy minél több eszközt, berendezést csatlakoztassunk valamilyen kommunikációs hálózathoz, napjainkra már kevés olyan szektort lehetne találni, ahol nincs jelen a technológia.

A legmodernebb szállodákban már a vendégek egyéni igényeire lehet beállítani például a fényeket, hűtést-fűtést, távolról, a recepcióról menedzselve, abban a pillanatban, amikor a vendég bejelentkezik.

Az előrelátó, a pénztárcájukra és a környezetre egyaránt figyelemmel lévő épületüzemeltetők sem kerülhetik meg a technológiát, hiszen a kihelyezett érzékelők, a peremhálózati, számítási képességgel is rendelkező berendezések, illetve az adatokat összegyűjtő és elemző, felhőalapú rendszerek egészen elképesztő mértékben javíthatják az ingatlanok működési hatékonyságát. Márpedig az épületek létrehozása és fenntartása felelős a globális energiafogyasztás és az üvegházhatást okozó gázok kibocsátásának 30 százalékáért, ugyanakkor a bennük rejlő energiahatékonysági potenciál jelenleg 82 százalékban kihasználatlan a Nemzetközi Energia Ügynökség World Energy Outlook jelentése szerint.

Az IoT-piac elemzésével és kutatásával foglalkozó IoT Analytics július elején hozta nyilvánosságra, hogy több mint 1400 dolgok internete projekt vizsgálata alapján melyek tekinthetők jelenleg a „legforróbb" felhasználási területeknek. A cikk elején már említett ágazatok természetesen megtalálhatók a felsorolásban, de az épületek, az ellátási lánc, az egészségügy és például a mezőgazdaság is helyet kapott a toplistán.

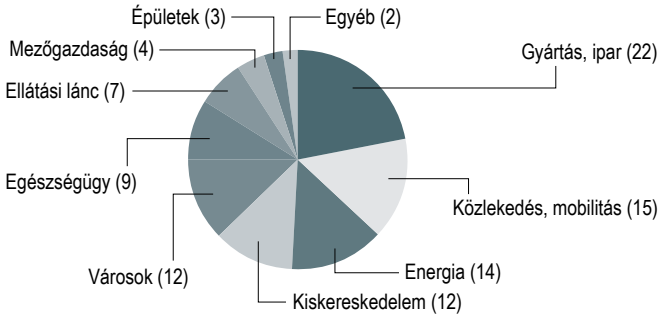
Összekapcsolt világ

Számos elemzés és előrejelzés jelent meg az utóbbi néhány hónapban is, hogy milyen mértékben nő majd az IoT-eszközök száma a következő években és ha egyetlen szóval kellene jellemezni a fejlődés ütemét, akkor talán a brutális lenne a megfelelő. Abban ugyanis az összes prognózis egyetért, hogy többszörösére nő az ilyen készülékek mennyisége mindössze pár év alatt. A Transforma Insights például azzal számolt, hogy a 2019 végi 7,6 milliárdról 2030-ra 24,1 milliárdra nő az IoT-eszközök száma. Ennél jóval gyorsabb fejlődést vázolt prognózisában a Cisco, az IoT-szektor egyik meghatározó szereplőjének számító vállalat várakozásai szerint 2023-ra már 29,3 milliárd, hálózathoz csatlakoztatott készülék lesz világszerte.

Az ugyanakkor nem egyértelmű, hogy ezekben az előrejelzésekben benne vannak-e például a szenzorok, amelyek egyre nagyobb számban jelennek meg a gazdaság szinte minden területén. A Transforma Insights például arra számít, hogy a legnagyobb arányban a különböző, médiatartalmak fogyasztására is alkalmas, az egyéni felhasználóknál lévő csatlakoztatott eszközök lesznek majd (az összes 34 százaléka), jóval kevesebb lesz belőlük az elektromos hálózatokban (14 százalék) és a hálózathoz kapcsolódó járművekben (7 százalék).

Az IoT-t legintenzívebben alkalmazó szektorok

Százalék, részesedés a vizsgált 1414 projektből



FORRÁS: IOT ANALYTICS

Sokmilliárdos plusz

A Transforma Insights arra is vállalkozott, hogy megbecsülje, mekkora potenciális piacot jelent az IoT. Szerintük a múlt évben 424 milliárd eurós volt ez a piac, 2030-ra pedig 1300 milliárd eurósra nőhet. Ennek a legnagyobb részét, 66 százalékát, a szolgáltatások teszik majd ki, amibe a cég szakértői a kommunikációs szolgáltatásokat is beleszámolták, a fennmaradó összeg pedig a hardverre jut.

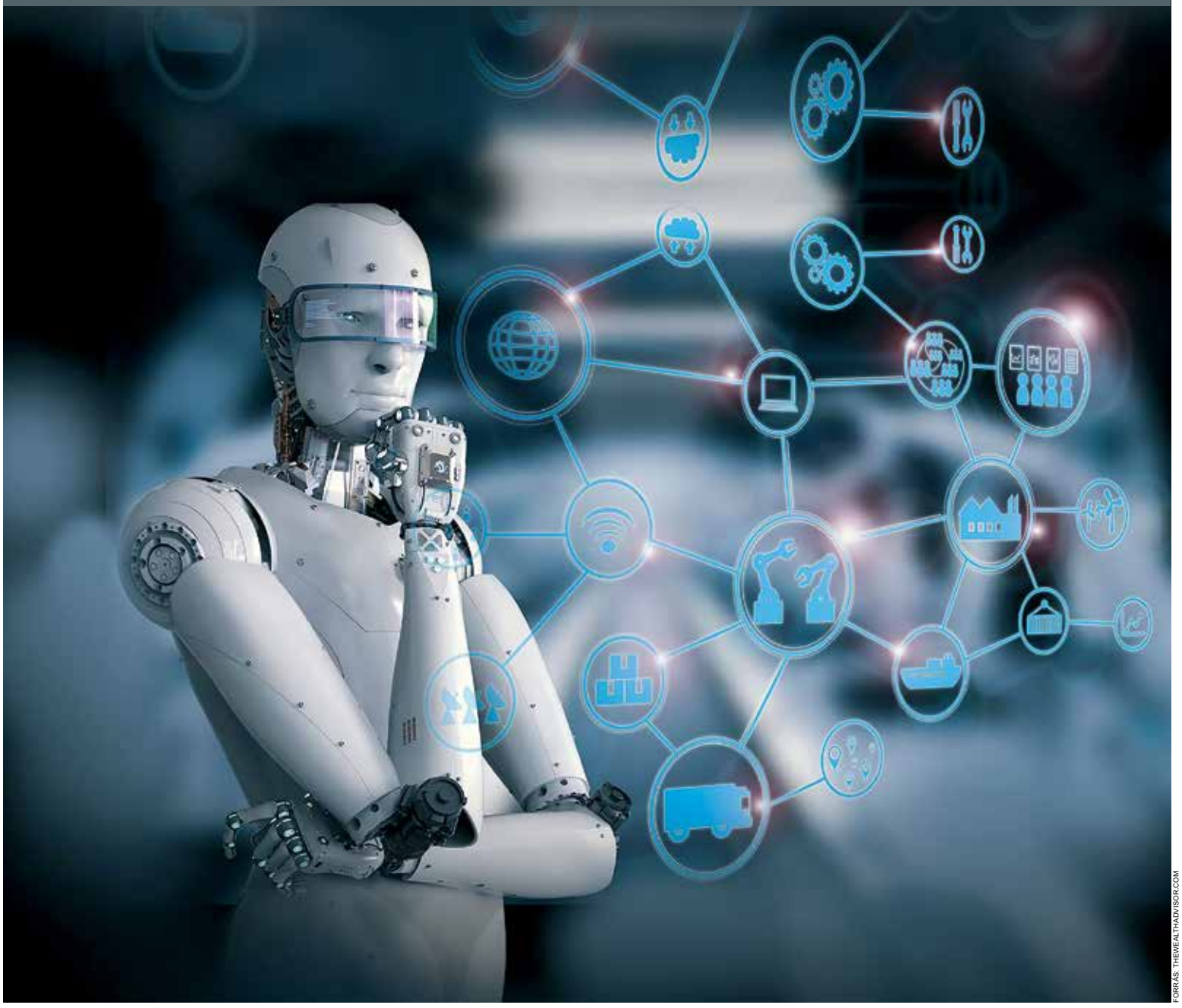
> Az ipari IoT-alkalmazások 2030-ra 14200 milliárd dolláros pluszt jelenthetnek a Föld GDP-jében

A Fortune Business Insights tanulmánya pedig azt mutatja be meglehetősen érzékletesen, hogy még olyan területeken is hatalmas felfutás várható a dolgok internete kapcsán, amelyekre kevesen gondolnának a technológia kapcsán. A banki, pénzügyi szolgáltatási és biztosítási szektorban az adataik szerint 2018-ban 17,85 milliárd dollárt költöttek IoT megoldásokra, 2026-ra azonban az ilyen jellegű kiadások ebben az ágazatban elérhetik a 116,27 milliárd dollárt.

Az Accenture prognózisa pedig arra mutat rá, hogy milyen hatással van a dolgok internete a teljes gazdaságra. A társaság azt vizsgálta, hogy az ipari IoT alkalmazások hogyan befolyásolhatják a globális gazdaságot, és becslésük szerint 2030-ra egészen elképesztő, 14200 milliárd dolláros pluszt jelenthetnek a Föld GDP-jében, persze csak akkor, ha valóra válnak azok az előrejelzések, amelyek gyors elterjedésükkel számolnak. ■

3OO MILLIÁRD DOLLÁROS PIACI LEHETŐSÉGET KÍNÁL AZ MI NÉHÁNY ÉVEN BELÜL

Mindenhol tarol a mesterséges intelligencia



FORRÁS: THEWEALTHADVISOR.COM

Egészségügy, pénzügy, kiskereskedelem, ügyfélszolgálatok – már most is számtalan területen támogatja a vállalkozásokat és a fogyasztók kiszolgálását a mesterséges intelligencia, és a következő években további dinamikus bővülésre lehet számítani az alkalmazásában. Az IDC prognózisa szerint 2024-re már 300 milliárd dollárt költenek világszerte erre a technológiára.

Január végén bejárta a világot a hír, hogy egy kanadai startup „Bluedot" nevű algoritmusa az Egészségügyi Világszervezetet, illetve az amerikai járványügyet napokkal megelőzve, már 2019. december 31-én arra figyelmeztetett, hogy a kínai Vuhanban megjelent koronavírus globális fenyegetéssé nőhet. Ez az eset meglehetősen pontosan mutatta meg, hogy mi a mesterséges intelligencia (MI) egyik legnagyobb előnye: elképesztő mennyiségű információt képes feldolgozni rövid idő alatt, és az eredményekből, a felismert mintázatokból még következtetésekre is futja.

Segítség a gyógyításban

A torontói startup a Bluedotot kifejezetten fertőző betegségek előrejelzésére hozta létre, azonban az MI az egészségügy egyéb területein is jelen van már évek óta. Az IBM Watson for Oncology például egy olyan mesterséges intelligencia alapú, klinikai döntéstámogató rendszer, amely abban segíti a szakorvosokat, hogy a legmegfelelőbb terápiás javaslatot állítsák fel a daganatos betegeik számára, a megoldást pedig már az Európai Unióban is engedélyezték orvosi eszközként.
A COVID-19 járvány kapcsán persze nemcsak a korai felismerésnél, de a krízis kezelésében is számos lehetőség kínálkozott és adódik még ma is az MI bevetésére. A Gartner még tavasszal készített egy tanulmányt annak kapcsán, hogy a mesterséges intelligencia hogyan tudja támogatni a hatóságok és az egészségügyi dolgozók munkáját. A beérkező adatok elemzésével és a mintázatok feltárásával hatékony eszköz lehet a vírus terjedési útjának feltárásában. Elég csak arra gondolni, hogy a mobiltelefon cellainformációk és a térfigyelő kamerák adatainak összevetése mekkora emberi erőforrást igényelne, miközben ezek a feladatok MI-vel is megoldhatók. De jó szolgálatot tehet a mesterséges intelligencia a diagnózis felállítása során, illetve a kórházakban a beérkező betegek kapcsán a kezelési sorrend megállapításában.

Idén világszerte 156,5 milliárd dollárt költhetnek MI megoldásokra

Jelentős előny

Bár az elmúlt években e sorok írója is több alkalommal szembesült azzal konferenciák kerekasztal-beszélgetései során, hogy még az infokommunikációs szakmán belül is megoszlanak a vélemények arról, hogy létezik-e már igazi MI, a köznyelvben, a sajtóban és az informatikai cégek reklámjaiban, ajánlataiban is működő és jól használható technológiaként utalnak rá. A nagy technológiai cégek előszeretettel hangoztatják, hogy az általuk fejlesztett digitális asszisztensek mögött is mesterséges intelligencia dolgozik, az okostelefonok gyártói pedig ott tartanak, hogy a mobilos fotózás élményét is MI-vel emelik új szintre. Ha pedig valaki egy online ügyfélszolgálaton a chat megoldást választja, nagy valószínűséggel nem élő emberrel, hanem egy robottal kezd „beszélgetni", amit szintén valamilyen mesterséges intelligencia támogat, szerencsés esetben gépi tanulásra és természetes nyelv feldolgozására is képes algoritmussal.
A PwC elemzése szerint a bankok 34 százaléka fektet be MI-fejlesztésekbe, mivel abban bíznak, hogy ezzel a rendkívül munkaerő-igényes back-office feladatok egy része alól mentesíthetik munkatársaikat, ráadásul az ügyfelekről és a tranzakciókról rendelkezésre álló nagy mennyiségű adat valós idejű elemzése révén az MI hatalmas segítséget nyújthat számukra a csalások kiszűrésében. Érdekes lehetőségre mutatott rá a McKinsey az MI kiskereskedelemben történő alkalmazása kapcsán. A cég tanulmánya szerint a szektor azon szereplői, amelyek élenjárnak a mesterséges intelligencia bevetésében, akár 5 százalékkal is növelhetik a haszonkulcsukat – ennyi pedig ebben az ágazatban már komoly eredménynek számít. A kiskereskedelemben az egyik leginkább magától értetődő alkalmazási terület a készletgazdálkodás: egyrészt a korábbi évek adatainak elemzésével az MI meglehetősen pontos becslést tud adni egyes kiemelt időszakokra vonatkozóan – mint például az iskolakezdés, vagy a karácsonyi szezon –, hogy miből, mennyit érdemes rendelni, másrészt az aktuális forgalom valós idejű követésével az eddiginél sokkal gyorsabb reagálási lehetőséget biztosít a kereskedők számára. ■

Töretlen fejlődés

Az egyes üzleti szektorokat eltérő ütemben hódítja meg az MI, de a következő években hatalmas üzleti lehetőséget kínál a fejlesztőcégeknek. Az IDC előrejelzése szerint idén világszerte 156,5 milliárd dollárt költhetnek az MI-hez kapcsolódó szoftverre, hardverre és szolgáltatásokra, ami 12,3 százalékos bővülést jelent a múlt évhez képest. Ebben az évben a -19 járvány miatt a korábbihoz viszonyítva valamivel lassabban fejlődik ez a szegmens, de a következő években gyors visszarendeződés várható. 2024-ben pedig már 300 milliárd dolláros lesz a mesterségesintelligencia-megoldások piaca, ami évente átlagosan 17,1 százalékos növekedést jelent.

FORRÁS: MOBILETRANSACTION.ORG

JÖNNEK AZ AZONNALI UTALÁSON ALAPULÓ FIZETÉSI MEGOLDÁSOK

Megmentheti a kereskedőket a QR-kód

Egyelőre csak az átutalások gyors megvalósulásában látjuk az azonnali utalási rendszer előnyeit, a szabályozó segítségével azonban ez biztosítja az alapot a jövő év január elejétől mindenki számára kötelező elektronikus fizetési megoldások biztosításához. Világviszonylatban is a gyors fizetés terjedése határozza meg a fintech világát. A blockchain is ígéretes a fintechben, de egyelőre még nem érezteti hatását.

Amikor a tavaszi járvány miatti karanténban készpénzhiány alakult ki a házban, az online tartott fitnesszlecke árát utalással fizettem ki, és az ételfutár mobilterminálján fizettem érintős (valójában érintés nélküli…) kártyámmal. Az azonnali fizetési rendszernek köszönhetően az utalások azonnal megérkeztek, mintha kézbe adtam volna a pénzt. Fogyasztóként egyelőre csak ezt látom az idén március elején debütált, azonnali fizetési rendszer egyedüli előnyének, a bankok, pénzintézetek és pénzügyi szolgáltatók – ahogy a tech cégek is – még mindig a nem túl látványos háttérfejlesztéseken dolgoznak.

Kötelező lesz az elektronikus

Mert van min dolgozni, ugyanis a kormány áprilisi döntése szerint a 2021. január elejétől az online kasszát használó kereskedők kötelesek elektronikus fizetési lehetőséget biztosítani ügyfeleiknek. Ettől ugye a gazdaság további fehéredését várják el a szakértők. Az Európai Bizottság kutatása szerint 2014-2016 között 530 milliárd forinttal több bevétel folyt be a magyar költségvetésbe az online kassza bevezetésének köszönhetően, most azért valószínűleg kisebb lesz a plusz bevétel.
De az is látható, hogy a lakosoknál lévő készpénzállomány folyamatosan nő: az MNB adatai szerint 2020 júniusának végére elérte a rekordot jelentő 6965,3 milliárd forintot. Egyetlen hónap alatt 74,1 milliárd forintos volt a növekedés.

QR-kódos megoldások

A 213 ezer online kassza mellett 147 ezer bankkártya-elfogadó terminál volt kihelyezve 2019 végén az MNB adatai szerint, ami azt jelenti, hogy a kötelező átállás 66 ezer kisebb-nagyobb vállalkozást érint. Ehhez nem feltétlenül szükséges POS terminált beszerezni, hanem a március óta kiválóan működő azonnali fizetési rendszert is igénybe lehet venni – ha lennének erre megoldások. A piac azonban már készül például a mobilszám vagy a QR kódon alapuló fizetési lehetőségek bevezetésére. Őszre várható a bankok saját megoldása, vagy egy olyan központi alkalmazás, mellyel mindenki, banktól függetlenül tud pénzt küldeni azonnal. A Giro Zrt például már dolgozik egy QR-kód alapú, központi, azonnali fizetésen alapuló mobilfizetési megoldáson a bankokkal közösen, a Simple Pay felületeken pedig már van egy működő megoldás. A QR-kód kihelyezése a legolcsóbb, a leginkább költséghatékony megoldás lenne ugyanis azoknak a kereskedőknek, akik eddig valamiért nem biztosítottak elektronikus fizetési lehetőséget ügyfeleiknek.

Gyorsabban fizethetünk világszerte

Az Európai Unióban kialakított Single European Payment Area és a PSD2, plusz az egységes banki üzenetek kidolgozására létrehozott ISO 20022 szabvány hatására Európában az azonnali fizetési rendszerek elterjedése megállíthatatlan. A trendet erősíti az amerikaiak elköteleződése is, igaz, jegybank szerepét betöltő US Federal Reserve csupán 2021-ben tervezi elindítani az azonnali fizetéseket lehetővé tevő FedNow rendszert. Ezután a gyors, azonnali fizetések elterjedését már nemzetközi viszonylatban sem gátolja semmi.

A Libra projekt

2019 nyarán jelentette be a Facebook a Libra projektet, amely teljesen átalakította volna a pénzátutalást, és a közösségi oldalt a blockchain alapú digitális iparág megkerülhetetlen szereplőjévé tett volna. A projekt két részből állt: a Libra token egy stabil alapokra helyezett kriptovaluta lett volna, de létrejött volna egy blockchain-hálózat is a tranzakciók ellenőrzésére.

A közösségi oldal jól gondolta, hogy a hatóságok nem nézik majd jó szemmel ezt a kezdeményezést, ezért a Libra Egyesület esernyője alatt mutatták be a projektet, támogatónak megnyert olyan neveket, mint MasterCard, Visa, PayPal, Stripe és Visa. Azonban ezek a támogatók is sorban kihátráltak az elképzelés mögül.

A blockchain megjelent a nemzetközi átutalásokban

A blockchain pénzügyi hasznosításán a Facebook már 2019 óta dolgozik, amikor bejelentette a Libra nevű kriptovaluta megalkotási terveit. Az ambiciózus elképzelések azonban meghiúsultak: az amerikai központi szabályozói ellenállás hatására nem ez lesz az első hivatalos kriptovaluta, hanem inkább egy digitális pénztárcává alakul, melyben a meglévő, kormányzatok által támogatott hivatalos valuták is megjelenhetnek – és ha elkészül a Facebook a saját Libra kriptovalutával, akkor kiegészítheti a meglévőket.
A blockchain megoldások a lassú és költséges nemzetközi átutalások területén próbálnak terjedni, ott már nagyobb sikerrel, bár jelentős és látványos változtatásokat még itt sem hozott. 2019-ben több nemzetközi szolgáltató is piacra dobta blockchain alapú átutalási megoldását, a Visa (B2B Connect), IBM (Blockchain World Wire) és a Ripple (RippleNet), megkötötték a technológia elterjedéséhez elengedhetetlen partneri szerződéseket is, ezzel kialakítva a szükséges infrastruktúrát. Úgy tűnik, a blockchain ezen a területen praktikus technológiai megoldásként tud (majd) érvényesülni. ■

FOLYAMATROBOTIZÁLÁS

A mézeshetek vége

A folyamatrobotizálás lassan belép az érett technológiák közé, ami együtt jár a felfokozott várakozások (és csalódások) csillapodásával, és a technológia valódi helyének megtalálásával a vállalati infrastruktúrában.

FORRÁS: ISTOCK

A következő évek egyik meghatározó technológiája lesz a folyamatrobotizálás (robotic process automation, RPA). A Gartner szerint idén 1 milliárd dollárt költenek erre a világ vállalatai, az éves növekedési szint pedig meghaladja a 40 százalékot. A Forrester merészebb számokat jósol, szerintük 2021-re már 2,9 milliárd dollár lesz a piac forgalma. Bármelyik szám is jön be, felmérések szerint az üzleti döntéshozók 70 százaléka növelni kívánja az RPA-megoldások bevezetésére és fejlesztésére szolgáló beruházásokat.

Mit tudnak ezek az eszközök, hogy most mindenki róluk beszél?

Alapvetően olyan folyamatokat hajtanak végre irodai környezetben, amelyeket eddig emberek végeztek el. Minden munkahelyen vannak olyan feladatok, amikor egyik programból a másikba kell adatokat másolni, több helyről, több képernyőről kell összeszedni az adatokat, és átmozgatni egy újabb rendszerbe. Ismétlődő, kevés hozzáadott értéket tartalmazó, unalmas és ezért sok hibára lehetőséget adó munkák ezek.

Egy RPA-rendszer betanítható arra, hogy milyen alkalmazásokat, képernyőket nyisson meg, ott milyen mezőket keressen meg, azokból hova másolja az adatokat, milyen transzformációnak vesse alá őket és hova továbbítsa a végeredményt. Gyors, nem fárad, nem hibázik, a felszabaduló munkaerő pedig értelmesebb, hasznosabb munkákkal tud foglalkozni.

Éppen ezért beleesett a feljövőben lévő technológiák szokásos csapdájába: általános csodaszert kezdtek látni benne, ami minden bajra gyógyírt kínál. Erre az RPA ugyanúgy nem képes, mint ahogy nem volt képes egyetlen korábbi, túlhype-olt megoldás sem, ami néhány felhasználóban keserű szájízt hagyott. Kiderült, hogy a folyamatrobotok kidolgozása sok esetben komoly kódolást igényel, képesek meghibásodni, ha az általuk figyelt képernyőkön megváltozik a kezelőfelület.

Nem kell megijedni: a folyamatrobotizálás nem bukott és még kevésbé nem halott technológia. Nagyon is fejlődésben van, éppen ezért a felhasználók csak most kezdenek rájönni, hogy hol, mire és miként kellene alkalmazni a technológiát.

Folyamatrobotizálás a gyakorlatban

Az American Express emberi munkaerő helyett már RPA-t használ a repülőjegyek lemondásához és a visszatérítések kifizetéséhez. A robotizált folyamat képes online interakciót folytatni az ügyféllel és feldolgozni a tranzakciót. Eközben az ügyfél valószínűleg észre sem veszi, hogy ember helyett egy intelligens szoftverrobot segíti a folyamatban.

Az eddigiektől eltérően kell mérni a folyamatrobotizálási (RPA-) eszközök, projektek hasznosulását: lehetnek új szolgáltatások? Javult a dolgozók hangulata?

Mire figyeljen hát a vállalati informatika?

Mindenképpen számítani lehet a piac konszolidációjára. Manapság legalább 150 RPA-eszköz kapható a piacon. A kisebb gyártók egy részét felvásárolják, akár a nagyobb RPA-szállítók, akár azok az informatikai vállalkozások, amelyek fantáziát látnak a piacban. Jobban láthatóvá válik a gyártók és termékek közötti különbség is: bizonyos RPA-eszközök inkább gyors, taktikai előnyöket kínálnak az asztali alkalmazások közötti folyamatok automatizálásával, mások pedig stratégiai transzformációra is lehetőséget nyújtanak nagyvállalatoknak.

Mondanunk sem kell, hogy a megfelelő eszköz kiválasztása nagymértékben befolyásolja a kívánt eredmények elérését, ezért változni fognak a fontosnak tartott kiválasztási kritériumok is. Olyan gyakorlatias és üzleti szempontok kerülnek előtérbe, mint az átfogó biztonság és compliance (auditálhatóság), a méretezhetőségi és integrálhatósági potenciál, a bevezetéshez szükséges kódolás mennyisége vagy éppen az (ön)tanulási képességek.

Másképp lehet és kell mérni a folyamatrobotizálási eszközök, projektek hasznosulását is. Tudunk-e új szolgáltatásokat kínálni? Mennyivel nő a folyamatok hatékonysága? Hogyan javult a szolgáltatások, folyamatok minősége, sebessége, csökkentek-e a kockázatok? Sikerül-e a folyamatautomatizálásból kinyert adatok alapján optimalizálni vagy újraalkotni az üzleti folyamatokat? Jobb lett-e a dolgozók hangulata?

Digitális munkaerő a láthatáron

A folyamatrobotizálás egyik legjelentősebb hatása mégis az lehet, hogy elfogadottá, megszokottá teszi a mesterséges intelligencia használatát. Az RPA-eszközökbe számos MI-technológia építhető be, a természetes nyelvi feldolgozástól az intelligens optikai karakterfelismerésig, ezek még öntanuló képességekkel is kiegészíthetők. Ezek révén pedig, állítják a szakértők, az RPA továbbfejlődik úgynevezett hiperautomatizációvá, és lehetővé teszi a digitális munkások (digital workers) megjelenését.

A digitális munkások abban különböznek a hagyományos, egyszerű szoftverrobotoktól, hogy nem csupán előre rögzített folyamatokon tudnak végigmenni gyorsan és fáradhatatlanul, hanem képesek alkalmazkodni az előre nem látott változásokhoz. Ezek már többféle feladatra is kiválóan használható, önszerveződő eszközök, amelyek ugyanazokat az informatikai rendszereket használják, mint az emberek.

A jövő egyik nagy változása pontosan az lesz, hogy a szoftverrobotok egyre több helyen és egyre nagyobb mértékben dolgoznak együtt az emberi munkaerővel – és erre mind a két felet fel kell készíteni. ■

ROBOTIZÁLT FOLYAMAT-AUTOMATIZÁCIÓ

Egyszerűbb, mint hinnénk

FORRÁS: GRAPESOLUTIONS

Robotokat a szoftveriparban is alkalmaznak, és ugyanarra a célra, mint a fizikai gyártásban: megszabadítani az embereket az ismétlődő, monoton feladatoktól, miáltal nemcsak a hatékonyság nő, de a hibalehetőségek száma is csökken.

A versenyképességüket megőrizni, illetve növelni akaró vállalkozások folyamatosan a feladataikhoz igazítják üzleti folyamataikat. Amikor a folyamatok egyes lépései már jórészt számítógépes alkalmazásokban zajlanak, az applikációk és a folyamatok elválaszthatatlan kölcsönhatásba kerülnek.
Komplex rendszereknél ez a kölcsönhatás gondokat is okozhat. Egy összetett vállalati számítógépes rendszer kialakítása időigényes feladat, az implementáció során az üzleti folyamatokat sok esetben át kell alakítani – és ez is nem is mindig a üzleti igényeknek, hanem a bevezetendő rendszer elvárásainak megfelelően történik. A hosszú idő alatt és drágán bevezetett rendszer megtérülésére fókuszálva nem egyszer inkább „befagyasztják" a kapcsolódó üzleti folyamatokat, aminek következtében a valós üzleti elvárások lassan túlnőnek a lemerevedett üzleti rendszeren.
Ezt a helyzetet a vállalkozások kreatív dolgozói újabb és újabb alkalmazások belső fejlesztésével próbálták javítani, tovább növelve ezzel az üzleti rendszerek komplexitását és személyfüggőségét. Az eredmény? A tisztán digitalizált működés irányába tartó szervezet olyan hibrid rendszer birtokába került, amely nem működött hatékonyan, csak részben volt rugalmas, üzemeltetése drágának bizonyult, és biztosan nem volt alkalmazható az üzleti folyamatok gyors és hatékony automatizálására.

Csak egyszerűen!

Pedig közben a folyamatok automatizálása alapkövetelménnyé vált. A munkaerőnek a nagyobb hozzáadott értéket termelő folyamatokkal kell foglalkoznia, miközben a nagyszámú tranzakciót monotonon végrehajtó szervezetek háttérbe szorulnak. A helyzet kezeléséhez olyan folyamatrobotizációs (RPA) megoldásokra lesz szükség, melyek képesek könnyen kapcsolódni a meglévő rendszerekhez, alacsony az erőforrás igényük, egyszerű az üzemeltetésük és rövid fejlesztési idővel is bevezethetőek.
A Grape Solutions RPA-üzletágának a UiPath rendszerekre épülő megoldásai mindezen elvárásoknak megfelelnek. A meglévő rendszereket a megszokott képernyőkön keresztül is képesek kezelni, az üzleti feladatokat automatikusan elvégzik, stabilan a nap 24 órában, a hét minden egyes napján. A folyamatautomatizáló robot erőforrásigényét tökéletesen kielégíti egy átlagos dolgozói asztali számítógép, de igény szerint akár virtuális gépeken, szervezet háttérrendszerein is üzemeltethető.
A megoldás bevezetése is egyszerűbb, mint a legtöbb vállalati szoftveré. Az automatizált folyamat fejlesztése minden esetben a meglévő üzleti folyamatok megismerésével kezdődik. Általában elegendő csak a

grape SOLUTIONS

meglévő rendszerek képernyőin végigkövetni a folyamatot, hiszen jó eséllyel az automatizálás is a képernyők használatán keresztül fog megvalósulni. Így nincs szükség bonyolult technikai rendszerleírásokra, a felhasználó maga is be tudja mutatni az adott üzleti folyamatot, nem kell informatikus segítségét igénybe venni.

Együttműködésben ember és gép

Az felmérés után a Grape Solutions szakemberei optimalizálják az adott folyamatot az automatizáláshoz, majd az ügyfél jóváhagyása után a folyamat tényleges fejlesztését is megkezdik. A fejlesztés alatt és után egyaránt szükség lehet a felhasználók bevonására a tesztelésbe, hiszen ők ismerik behatóan a folyamatot, a robot pedig csak azt és úgy tudja végrehajtani, ahogy azt számára leprogramozták. A rendszer tesztelését és élesítését követően a Grape Solutions vállalja a folyamatos üzemeltetést is.
A UiPath technológiájának köszönhetően a meglévő folyamatokat napokon belül a megváltozott igényekhez lehet igazítani, néhány héten belül pedig teljes folyamatok automatizálására is mód van.
A folyamatrobotok többféle módon is működhetnek. Az úgynevezett unattended (felügyelet nélkül működő) robot önállóan, valamilyen logika alapján tervezett módon, központilag futtatható, nem terhelve a felhasználó napi munkavégzéséhez szükséges erőforrásokat. Így komplex folyamatok teljes automatizálása is egyszerűen megoldható a háttérben.
Elfordulhatnak olyan esetek is, amikor a felhasználó a részfolyamatok automatizálásával párhuzamosítani tudja feladatainak megoldását. Ebben az esetben ő maga indítja el az adott folyamatot, és amíg a robot azt végrehajtja, addig a felhasználó a kifejezetten személyes munkavégzést igénylő feladatain dolgozik. Amikor mind a két részfeladat elkészül, egy másik automatizmus vagy a felhasználó saját maga is összegyúrhatja azokat egy végleges megoldássá.

FORRÁS: GRAPESOLUTIONS

Közös munka gyümölcse

A fentiekből is látszik, hogy a sikeres megvalósításhoz elengedhetetlen a felhasználó folyamatos közreműködése. Ezért sosem egyedi folyamatok automatizálásában érdemes gondolkodni, hanem szélesebb körű partnerségben. Ennek keretében a Grape Solutions szakemberei már az üzleti folyamatok átszervezése során is együttműködnek a felhasználó szakembereivel, tehát a BPR (Business Process Reengineering) folyamat során tudatosan felmérik, milyen folyamato(ka)t fognak részben vagy egészben automatizálni.
A UiPath alapú rendszerek kellően felhasználóbarátak ahhoz, hogy az ügyfél munkatársai rövid továbbképzést követően képesek legyenek egyszerűbb folyamatautomatizálások végrehajtására. A munkavállalók így a korszerű technológia használatával hatékonyabban, gyorsabban és pontosabban tudják elvégezni feladataikat. *(X)*

Az eredmények magukért beszélnek

A Grape Solutions RPA megoldását használva az egyik, ügyfélkapcsolati rendszereket üzemeltető partner komoly optimalizációs sikert ért el. A szerződés-nyilvántartó rendszert automatizálva a robotok több tízezer szerződést rögzítettek automatikusan, korábban sosem látott naprakészséget teremtve. Nem csak a szerződések feldolgozása lett naprakész, de egyúttal átlagosan havi 5 FTE (teljes munkaidős munkavállaló) megtakarítására is lehetőség adódott. Elbocsátani nem kellett senkit, a felszabadult munkaerőt más, személyes munkavégzést igénylő területekre irányították át. A rögzített szerződésekhez kapcsolódó hibák száma a nulla közelébe csökkent, miáltal a korábban megszokott manuális utómunka is a minimálisra csökkent.

A Grape Solutions automatikus rendszerével a vállalat egy napon belül képes reagálni ügyfelei papír alapú formanyomtatvány küldési kérésére. A robotizált folyamat nem csak az ügyviteli rendszerben végzi el a szükséges adminisztrációt, hanem gondoskodik az igényelt formanyomtatvány postai úton történő kiküldéséről is. Ezzel a hibás teljesítés lehetősége megszűnt és a korábban több napig tartó igényfeldolgozási idő egy napra csökkent.

A Grape-ről röviden, elismerések

– Széleskörű technológiai fejlesztések, digitalizáció, üzleti intelligencia és tesztelési szolgáltatások
– **140+** szakértő munkatárs
– **100+** egyedi üzleti alkalmazás fejlesztve
– Kiemelkedő ügyfélelégedettségi ráta: 91%-os visszatérő ügyfél

KÖZELEBB KERÜL EGYMÁSHOZ AZ ÜZLET ÉS AZ IT

Proaktív együttműködésben a jövő

A megnövekedett feladatokra a vállalatok gyorsan, viszont időt és energiát spórolva szeretnének reagálni. Ehhez biztosít eszközkészletet a Flowmon forgalomanalitikai megoldása, mely az IT-szolgáltatók és ügyfeleik között képes proaktív partnerséget kialakítani – mondja Ványa László, a Flowmon Networks magyarországi üzletfejlesztési vezetője.

FORRÁS: ITB

VÁNYA LÁSZLÓ, FLOWMON

– Milyen trendeket tapasztal a Network Traffic Analysis (NTA) vagyis a hálózati forgalomanalitikai megoldások területén?

– Azt látjuk, hogy olyan eszközkészletet keresnek a vállalatok és az IT szolgáltatók a piacon, mely a reaktív IT-ból a proaktív IT-ba vezeti át őket. A forgalomanalitika más és más okokból fontos a vállalatoknak: nagyban függ nyilván a core tevékenységtől, van, aki az üzemeltetés támogatásra összpontosít, mások a biztonságra, vagy a pénzt termelő alkalmazásaiknak a minőségét igyekeznek meg megoldásunkkal javítani. Azonban mindenhonnan az az egységes visszajelzés érkezik, hogy eszközkészletünk segítségével sokkal proaktívabbak tudnak lenni, időt, energiát megtakarítva képesek reagálni a megnövekedett feladatokra. A hálózati vizibilitás hozadéka, hogy nem azon kell gondolkodniuk, hol lehet a probléma, hanem azon, hogyan lehet a gondokat orvosolni. Így a vállalat a drága erőforrásait, a megbecsült munkaerőt tudásához mérten tudja arra használni, amire eredetileg tervezte és alkalmazza.

Mindenhonnan az az egységes visszajelzés érkezik, hogy eszközkészletünk segítségével a vállalatok sokkal proaktívabbak tudnak lenni

– Bízzanak jobban a vállalatok az automatizáció bölcsességében?

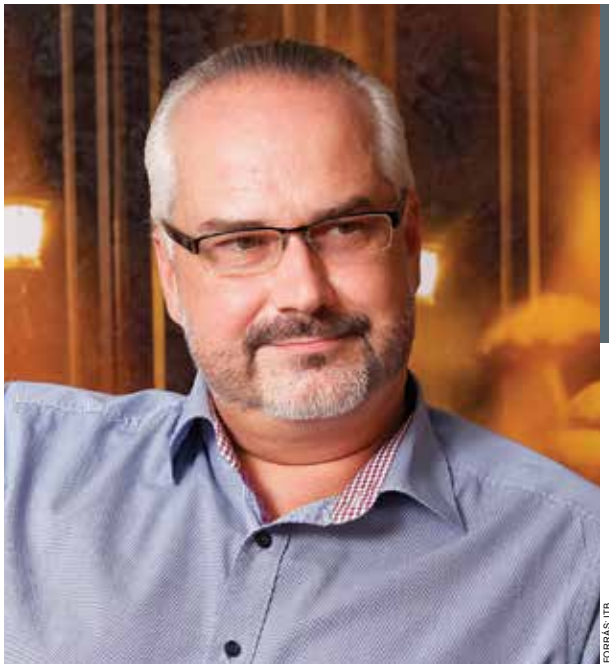
– Igen, meg kell tanulniuk, hogy hagyatkozzanak az okos eszközökre. Tegyük fel, akár valami egyszerű probléma adódik, például a kollégák tömegesen nem tudnak használni egy szolgáltatást, akkor hagyományos eszközökkel egy napot is elveszíthetünk a probléma feltárásával. Automata rendszereinktől csak meg kell kérdezni, mi lehet a probléma, és máris annak elhárításával foglalkozhatunk. Így hosszú kiesés helyett nagyon rövid szünet után folytatható a munka. Merjük az okos rendszerekre, az automatizációra bízni a hibakeresést, a szakemberek tudását használjuk olyan területen, ahol arra valóban szükség van.

– A Flowmon forgalomanalitikai megoldást sok IT-szolgáltató használja saját ügyfeleik kiszolgálására. Náluk is változott a hozzáállás?

– Az IT-szolgáltatóknak óriási idő és energia lenne minden ügyféllel ugyanolyan mélységben és minőségben foglalkozni egy megbízható eszközkészlet híján. Segítségünkkel sokkal gyorsabban jutnak információkhoz saját ügyfeleikről, a problémákat mélyebben képesek megérteni, hatásukat átlátni. Ez azt jelenti, hogy marad idő a problémák elemzésére, azok kezelésére. Sőt, arra is jut idő, hogy a szolgáltató az ügyféllel közösen együtt gondolkodjon a jövőről, proaktív módon javasoljon megoldásokat, azokra a gondokra, amelyeket a hálózati vizibilitást biztosító termékünk feltárt. A service providerek élete már nem arról szól, hogy 0-24-ben csak hibákat hárítanak el, hanem együtt tervezik az ügyféllel az üzletet kiszolgáló beruházásokat.

– Akkor már nem is ügyfelekről, hanem partnerekről beszélünk.

– Valóban, az IT-szolgáltató olyan proaktív partnere lehet a kiszolgált cégeknek, aki érti, hogyan működik a partner és célzott ötleteikkel segítik azok fejlődését. Vagy ha problémát tapasztalnak, akkor az IT-szolgáltató hatékonyan, gyorsan, érdemben tud javaslatot tenni a fejlesztendő területről, hogy ez többet ne forduljon elő. Az üzletet és az IT-t valóban közelebb hozzuk egymáshoz, és ebben van az óriási érték. A Flowmon ehhez tud egy hatékony eszközkészletet és platformot adni, ami valóban segít ezt az első látásra távol lévő két világot egy csapattá rázni. ■



FORRÁS: ITB

PATAKI TAMÁS, CANON HUNGÁRIA

NEM ELÉGSZÜNK MEG A SZTENDERD MEGOLDÁSOKKAL

A digitális dokumentumkezelés, mint hozzáadott érték, maga a hatékony jövő

Már évek óta tapasztalható a piaci elmozdulás a digitális dokumentumkezelés irányába, a koronavírus pedig végérvényesen biztosította a cégeket arról, hogy a papír alapú iratkezelés napjai leáldoztak. A digitális dokumentumkezelés felé vezető út azonban igényes eszközmegoldásokkal és hatékony szoftvermegoldásokkal van kikövezve, amelyekben a Canon Hungária évtizedes gyakorlattal támogatja az elektronikus munkafolyamatra váltó cégeket, a krízishelyzet pedig a céget is új tapasztalattal gazdagította.

Számtalan ágazat esetében bizonyult katalizátornak a koronavírus, nem volt ez másként az iratkezelés területén sem, sőt. A pandémia miatt tömegével kényszerültek home office-ba a munkavállalók, de az első napok megkönnyebbülését azonban az a felismerés követte, hogy ami eddig papíralapon volt jelen, és papíralapon tartalmazta a szükséges információkat a szervezetben, az bizony az otthon falai mögül nem érhető el. Ilyenkor szembesül sok cégvezető azzal, hogy a számlakezelési folyamat nincs kiépítve, és az e-aláírást sem vezették még be. „Erre vannak professzionális rendszerek, amelyek a dokumentumkezelés, adatkinyerés, validálás mellett a szerződés- és számlakezelő munkafolyamatokat is megkönnyítik. Természetesen mi is rendelkezünk megoldásokkal. Megdöbbentő volt, hogy a szükséghelyzet bevezetése után gyakorlatilag nap mint nap azonnali bevezetésre volt szükség, de sok cég keresett meg minket azzal, hogy helyezzünk el nagysebességű dokumentumszkennert, amivel emailen vagy egy gyorsan telepíthető DMS-workflow szoftveren másodpercek alatt szét lehet küldeni minden érintettnek az abból származó szükséges információt”, mondta *Pataki Tamás,* a Canon Hungária Business Development Managere.

> A szükséghelyzet bejelentése után gyakorlatilag nap mint nap azonnali bevezetésre volt szükség

Elkötelezetten a digitális dokumentumkezelés mellett

Jól mutatja a hirtelen megnövekedett igényt a cég szolgáltatásai iránt az is, hogy a dokumentumkezeléssel kapcsolatos üzletág, Pataki Tamás koordinálásával, az első féléves terv négy és félszeresét hozta.

A digitális dokumentumkezelés olyan hozzáadott értéket képvisel és közvetít a piac felé, mint az e-adatforgalom, a big data és a mesterséges intelligencia gyakorlati alkalmazása, ami nem csak megkönnyíti a munkát, de a repetitív feladatoktól is tehermentesíti a dolgozókat, hiszen a belső összefüggésektől kezdve a karakterfelismerésen át az adatkinyerésig mindenre alkalmas. „Ezekkel a szoftverekkel, eszközökkel és több évtizedes szaktudással tudjuk támogatni a cégek automatikus átállását”, fűzte hozzá Pataki Tamás.

„Vezetőként és magánemberként is elkötelezett vagyok a digitális átalakulás mellett. Nem véletlen, hogy elsőként valósítottuk meg az első, nagy tömegű, e-aláírási folyamatokat a köz- és versenyszférában egyaránt. Komoly a penetrációnk, a pénzintézetek, iparvállalatok, kkv-k körében. Kis túlzással, nincs olyan terület, ahol ne lennének referenciáink, tapasztalataink. Szinte mindenben tudunk biztos megoldást nyújtani. A sztenderd megoldásokon túl gondolkozom és gondolkozunk, ha kell, magunk találjuk ki és rakjuk össze azt az egyedi megoldást, amelyre az ügyfélnek szüksége van”, zárta gondolatait. ■