FORRÁS: 123RF.COM

„A HÁLÓZAT MAGA A SZÁMÍTÓGÉP” – *JOHN GAGE*, SUN MICROSYSTEMS, 1984.

A felhő jött, látott és győzött

A hibrid munkavégzés népszerűsége, a szigorú helyi vagy régiós szabályozások, de az ambiciózus fenntarthatósági célok is a felhőtechnológia malmára hajtják a vizet. A mesterséges intelligencia is ezt a technológiát választja otthonául, néha csak az emberi fantázia határa szab gátat a szolgáltatások terjedésének.

Ha még maradt is pár szkeptikus, aki pár évvel ezelőtt az ördögtől valónak tartotta a cloudot, ahol az adatok elvesznek, rossz kezekbe kerülnek, netán nincs semmi jogszabály, amely alapján felelősségre lehetne vonni a szolgáltatókat, a Covid-járvány minden ellenállást legyőzött. Sok vállalat- vagy IT-vezetőtől hallhattuk egy évvel ezelőtt, hogy a járvány volt a szervezetük digitális transzformációjának legnagyobb katalizátora.

A kényszerhelyzet elmúltával a digitális projektek továbbra is a cégek prioritási listáinak az élén maradtak, és ha a következőkben felvázolt trendek beválnak, akkor nem is fogunk lassulást tapasztalni ezen a téren. A felhőtechnológia már nem egy opció több közül, hanem olyan lehetőség, amelynek előnyei szilárd kapaszkodót jelentenek az előttünk álló bizonytalan gazdasági helyzetben.

A vállalatok egyszerűen nem engedhetik meg maguknak, hogy a digitális átalakulást fékezzék, de a felhőnek köszönhetően nem is kell. A technológia rugalmassága és méretezhetősége csökkenti az innováció pénzügyi kockázatát, miközben megteremti az oly vágyott agilitást. A Gartner adatai szerint 2025-re a vállalatok világszerte többet költenek majd a nyilvánosfelhő-szolgáltatásokra, mint a hagyományos IT-megoldásokra.

Nincs hibrid munkavégzés felhő nélkül

Annak ellenére, hogy az irodák újranyitottak és hívogatóbbak, mint valaha, a munkatársak nem töltik ki a tereket. A távoli munkavégzés, de leginkább a hibrid munka megszokottá vált. Az emberek megkedvelték ezt a munkavégzési lehetőséget, hiszen sokkal jobban tudják például a munka-magánélet egyensúlyát megvalósítani.

Ez az a terület, ahol a felhőmegoldások térnyerése nem áll meg. A Gartner becslése szerint 2023-ban a desktop mint szolgáltatás (DaaS) terület volumene 3,2 milliárd dollárra nő, hiszen egyre több vállalat előfizetés alapú, virtuális desktop szolgáltatásokat vesz igénybe.

Népszerűek maradnak tehát az olyan megoldások, mint a kommunikációt elősegítő eszközök, a projektmenedzsment, videókonferencia, fájlmegosztás, tudásmenedzsment stb. alkalmazások, hiszen ezek a szükségesek a kollégák együttműködéséhez, a produktivitás és hatékonyság növeléséhez – helyszíntől függetlenül.

A fenntarthatósági célok a felhőtechnológiától függnek

Az előttünk álló évben egyre több szervezet nemcsak a hatékony növekedésre, hanem a fenntartható működés kialakítására is összpontosít. Az IDC felmérése szerint a válaszadók 83 százaléka az IT-beruházási döntések meghozatalakor a fenntartható, környezetkímélő működésre is figyel. Az IDC becslése szerint a vállalatok 85 százalékánál a szoftveres és felhő alapú megoldások segítségével 35 százalékkal növelik a fenntartható működés arányát.

Sokan bírálják ezt a látásmódot, mondván, a felhőszolgáltatók is rengeteg nem megújuló erőforrást kénytelenek felhasználni. Védelmükre legyen mondva, ők hatékonyabban és jobban teszik, mint az a sok kis szervezet, amelyeknek nem a felhőszolgáltatás jelenti tevékenységük középpontját.

A mesterséges intelligencia is a felhőbe költözik

Az MI lassan, de biztosan belekúszik életünk minden apró részletébe, hiszen hatékonyan végzi el a rábízott feladatokat, sok esetben innovatív megoldások kiépítésére vetik be. A felhő abban tudja segíteni a mesterséges intelligenciához forduló szervezeteteket, hogy költséghatékonyan indítsák el ezeket a projekteket.

A McKinsey & Company 2021-es MI-vel kapcsolatos kutatása arra a következtetésre jutott, hogy az MI területén magas teljesítményt nyújtó vállalatok 64 százaléka az MI-munkafolyamatokat nyilvános vagy privát felhő infrastruktúrán működteti. Ezek a magas teljesítményt nyújtó szervezetek a nyilvános felhőből olyan MI-képességeket vásárolnak, mint az arcfelismerés és gépi beszéd. Előre jelzi a kutatás azt is, hogy a vállalatok kétharmada 2023-ban az előző éveknél többet tervez MI-re fordítani.

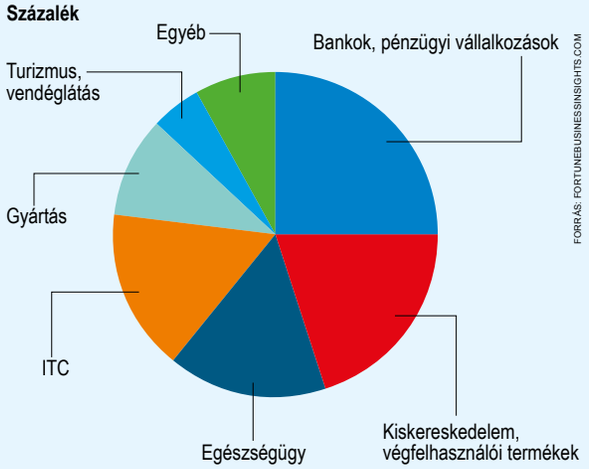
A vállalatok a független, iparág-specifikus felhőhöz fordulnak

Az EU példájára rengeteg állam és kontinens fogalmazta meg saját adatvédelmi és/vagy IT-biztonsági elvárásait, arról nem is beszélve, hogy szinte követhetetlen, milyen elvárásai vannak egy-egy piacnak egy adott iparág szereplőjével szemben. Ez arra kényszerítette a vállalatokat, hogy a független, iparág-specifikus felhőszolgáltatásokat vegyék igénybe.

A független felhőszolgáltató mint elgondolás nem új, de a geopolitikai változások egyre népszerűbbé teszi. A független szolgáltatást úgy találták ki, hogy egy adott országban vagy régióban működjön, ahol egységesen megfelel az adott hatóságok szigorú adatvédelmi, IT-biztonsági vagy egyéb előírásainak.

A Capgemini tanulmánya szerint a szervezetek 71 százaléka a megfelelőségi elvárások miatt független felhőszolgáltatást vesz igénybe. Ez egyszerre új piaci lehetőség a szolgáltatók számára, de ugyanakkor a szigorú előírások által szabályozott vállalatok, kormányzati szervezetek számára is előnyös, hogy hatékonyan, a felhőtechnológia segítségével végezzék munkájukat. A Forrester meglátása szerint a felhőbe való költözés éllovasai 2023-ban a német és egyéb európai pénzügyi szervezetek lehetnek.

XaaS-piac szegmenseinek eloszlása 2021-ben



Előtérbe kerülnek a natív felhőmegoldások

A Forrester „2022 Infastructure Cloud Survey” szerint a vállalatok 40 százaléka a natív felhőstratégiát választja 2023-ban, hiszen szeretnénk növelni agilitásukat és hatékonyságukat, miközben csökkentik költségeiket. A natív felhőmegoldások a szoftverfejlesztés újszerű megközelítését jelentik mikroszolgáltatások, konténerek, API-k és szolgáltatási hálózatok igénybevételével.

A különböző iparági szabályozások is a törvényeknek megfelelő működést lehetővé tevő felhőszolgáltatások felé fordítják a vállalatok figyelmét, legyen az az egészségügy, pénzügy, távközlés területén tevékenykedő cég. A Gartner számai szerint 2027-re a vállalatok több mint fele fog iparágra szakosodott felhő szolgáltatást igénybe venni.

Felnőnek a „mindent szolgáltatásként” megoldások

Az XaaS, vagyis „mindent szolgáltatásként” megoldások 2023-ban már megérnek, kiforrottak lesznek, ez is növeli a felhőmegoldások népszerűségét. Csak a képzelet szab határt, hogy mi mindent lehet a felhőben igénybe venni – adattárolást, biztonságot, hálózatot – azonban csakis úgy, hogy a technológia mellé a szakemberek tudását és támogatását is csatolják a szolgáltatók. És mint a legtöbb felhő szolgáltatás esetében is, itt is csak az igénybe vett erőforrásokért fizet a vállalat.

Az IMARC csoport becslése szerint a 2021-ben 198,6 milliárd dolláros XaaS-iparág 2027-re 624,1 milliárd dollárosra nő. Ebben a szolgáltatási szeletben még bőven vannak kihívások, egy új megoldást kitalálni és felhő alapokon szolgáltatni nem egyszerű, de a kínálat 2023-ban ezen a piacon is egyre szélesebb és színesebb lesz. ■

A LŐPOR MARADJON SZÁRAZ

Több felhő, több veszély

Az összetett infrastruktúrák összetett védekezési módszereket kívánnak meg. A mind gyakoribbá váló többfelhős környezetek egészen új kihívások elé állíthatják a vállalatokat – de sok régi alapelv itt is működik.

FORRÁS: 123RF.COM

A biztonsági szabályok kidolgozása és betartatása egyfelhős környezetben is idő- és munkaigényes feladat – a nehézségek egy többfelhős infrastruktúrában csak hatványozódnak. Egyrészt többfelé kell figyelni, másrészt minden platform kicsit más is. Az általános megközelítés nagyjából hasonló, de az egyes konkrét biztonsági intézkedések és azok megvalósítása nagymértékben különbözhet.

Hibák itt és hibák ott

Sok esetben ugyanarról a tőről fakadnak a felhőkörnyezeteket fenyegető veszélyek, mint amelyek a saját adatközpontban működő rendszerekre leselkednek. Gyakori hiba a rossz vagy hiányos konfiguráció, esetleg az elégtelen biztonsági beállítások. Jellemzően csak arról van szó, hogy nem megfelelően állítják be a hozzáférési jogosultságokat az egyes felhőszolgáltatásokhoz. Sűrűn előforduló probléma, hogy az AWS Simple Storage Service (S3) tárhelyeit (bucket-jeit) helytelenül konfigurálják, így azokból adatok szivároghatnak ki.

Számos veszélyt rejtenek a nem kellően biztonságos programozási interfészek (API-k). Az ügyfelek ilyen API-kon keresztül menedzselhetik a felhőben lévő adataikat. A gond csak az, hogy az API-kat sok esetben külső cégek fejlesztik, amelyeknél nem mindig lehet megállapítani, hogy mekkora gondot fordítottak a biztonságra. Az ilyen API-kat előszeretettel támadják a hackerek, hogy illetéktelen hozzáférést szerezzenek a rendszerekhez és adatokhoz.

Veszélyes munkaerő

Nem szabad megfeledkezni a belső fenyegetettségekről sem. Mint minden informatikai környezetre, a felhőben futó rendszerekre is komoly veszélyt jelentenek a hanyag, nemtörődöm vagy éppen nem kellően biztonságtudatos felhasználók. A túlzott vagy nem jól kezelt, időben vissza nem vont jogosultságok igen komoly károkat tudnak okozni. Ha ráadásul a belső felhasználó nem egyszerűen hanyag, hanem szándékosan akar rosszat tenni, a kockázat megsokszorozódik.

Az elrontott hálózati konfigurációból is számos probléma származhat. A felhő egyik előnye, hogy az üzleti felhasználók is könnyedén, néhány kattintással újabb erőforrásokat tudnak bevonni. Ennek azonban megvannak a hátulütői is, hiszen ezek az emberek nem jártasak a hálózati infrastruktúra rejtelmeiben. Az eredmény: SSH nélküli szerverek, feleslegesen nyitva maradt portok, félrekonfigurált hálózati hozzáférési listák (NACL-ok).

Magas kockázat a hanyag, gondatlan vagy kevéssé képzett felhasználó.

Amikor rejtekhely a felhő

Mindezeken túl a felhős környezetekre is leselkednek a kártevők, a rosszindulatú kódok. Ezeknek két alapvető fajtáját különböztethetjük meg: amelyek terjedésre/terjesztésre és kommunikációra használják a felhőt; és amelyek kifejezetten a felhős rendszereket és erőforrásokat támadják.

Ami az elsőt illeti, a felhős tárhelyeken – legyenek azok dedikált szolgáltatások, mint a Dropbox vagy a Box, esetleg IaaS vagy PaaS megoldások tárolórendszerei – számtalan különféle kártevő bújhat meg. A zsarolóvírusok különösen előszeretettel használják a felhő infrastruktúrát. Számos malware telepíti vezérlőrendszereit (command & control servers) a felhőbe, mert a nagy szervezetek, vállalatok általában nem tiltják a nagy felhőszolgáltatók (AWS, Microsoft Azure, Google Cloud) felé irányuló forgalmat.

Végül, bizonyos kártevőket szolgáltatásmegtagadásos (DDoS-) kampányokban is használhatnak. A felhőbe telepített, a hackerek irányítása alatt álló rendszer kiválóan alkalmas lehet nagy mennyiségű adatforgalom generálására, amellyel megbéníthető a kiszemelt áldozat weboldala, szolgáltatása.

Amikor célpont a felhő

És ha ez nem lenne elég, egyre több olyan malware is létezik, amelyeket kifejezetten a felhős környezetekre és szolgáltatásokra hoztak létre. Az ismertebbek között vannak a kriptobányász kártevők, amelyek a felhős virtuális gépeket és konténerekben futó alkalmazásokat célozzák. Ezek a vírusok keresik a nem védett API-kat, és megpróbálják kihasználni őket arra, hogy saját workloadot telepítsenek és futtassanak. Ha sikerül, az áldozat erőforrásait használják arra, hogy kriptopénzeket bányásszanak.

Az is előfordul, hogy virtuális gépek sablonjaiba rejtik el a károkozó fájlokat. Ennek révén minden újonnan létrehozott VM fertőzött lesz, elősegítve a vírus állandó terjedését. Számtalan formája van annak a támadásnak is, amely során a felhőszolgáltatók piacterein elérhető pluginokat és modulokat fertőzik meg. Ilyen módon adatok lophatóak a SaaS-szolgáltatásokat igénybe vevőktől vagy bejuttatható a kártevő a PaaS és IaaS rendszerekbe. ■

Három lépés a felhő biztonságáért

Gondossággal és odafigyeléssel a felhős infrastruktúrára leselkedő veszélyek egy jó része elkerülhető, vagy legalábbis a kockázatok jelentősen csökkenthetőek.

1. Titkosítsuk a felhőben tárolt adatokat! Ha így teszünk, akkor sem járunk rosszul, ha a felhős rendszereinket feltörnék és kikerülnek az adataink.

2. Rendszeresen készítsünk biztonsági mentést a felhős adatokról és workloadokról! Számos szervezet a saját infrastruktúráján tárolt adatokat menti a felhőbe. Ugyanakkor, ha a felhő az adatok elsődleges helye, azokat érdemes máshol is letárolni – lehetőség szerint egy külön előfizetéssel vagy fiókkal, mert így számos támadási formából eredő kárt megelőzhetünk. (Természetesen csak megfelelő ellenőrzés és szükség esetén tisztítás után célszerű elvégezni a workloadok mentését.)

3. Alaposan szabályozzuk a hozzáférést! Hívjuk akár zero trustnak, akár least privilege accessnek, a lényeg az, hogy mindenki csak ahhoz az erőforrásokhoz és csak annyi időre kapjon hozzáférést, amire és ameddig feltétlenül szükség van. A jogosultságokat rendszeresen és tervezetten felül kell vizsgálni, a hozzáféréshez pedig erős jelszavakat és kétfaktoros azonosítást kell megkövetelni. Tovább csökkenthetjük a kitettséget és erősíthetjük a biztonságot, ha szegmentáljuk felhős erőforrásainkat.

+1 Oktassuk a felhasználókat! Még ha kellően biztonságtudatosak is a dolgozók (általában nem azok), a felhőmigrációs stratégia részévé kell tenni, hogy felhívjuk a figyelmüket az új kockázatokra és azok elkerülésére.

FORRÁS: 123RF.COM

NEMCSAK A SÁVSZÉLESSÉG FONTOS

Adat-energia egyenérték

Sokan és sokat beszélnek az adatvagyonról, annak összegyűjtéséről, tárolásáról és hasznosításáról. Az adat azonban önmagában nem létezik, nem létezhet: komoly infrastruktúra kell ahhoz, hogy valóban „digitális aranybányaként” tudjuk használni.

2021 második felétől igen jelentős energiaár-változásokat tapasztalhatott meg mindenki. Ez nem csupán a lakosságot, hanem a gazdaságot is keményen érintette, és természetesen a költségnövelő hatásokat nem kerülhette el az informatika sem. Ami egy kis szektorban a kriptovaluta-bányászat vesztét okozta, az nagyban még jobban fájt: az elektromos energia árának egyes időszakokban radikálisnak is nevezhető emelkedése az adatközpontok üzemeltetőinek is erős fejfájást okozott.

A költségek mellett nagy hangsúlyt kapott 2022-ben a reziliencia is: az orosz–ukrán háború igen látványosan mutatott rá arra, hogy már Európában sem tekinthető magától értetődőnek, hogy egy adatközpont mindig rendelkezni fog a zavartalan működéséhez szükséges kapcsolatokkal, legyen szó a kommunikációs vagy az energiahálózatról. Itt ma már beszélni kell a fizikai fenyegetettségről (mint amilyen a háború maga) illetve a kibernetikai műveletekről is. Az ukrajnai hadszíntéren zajló fegyveres küzdelem mellett már Nyugat-Európában és az Amerikai Egyesült Államokban is megszaporodtak az alapvető közművek, így az elektromos hálózat elleni kibertámadások.

Kiserőmű

A kérdés komolyságát jól jelzi az is, hogy szakértői becslések szerint a világ elektromos energiájának 3-4 százalékát már ma is az adatközpontok fogyasztják el. Mindezt úgy, hogy az 5G és az IoT jelentette „adatrobbanás” még be sem következett igazán, márpedig ez még több szervert, még több épületet – és még több, oda vezető tápvezetéket jelent. Vagy éppen mikroméretű nukleáris reaktorokat? Mert bizony ez az elképzelés is egyre inkább teret nyer, igaz, megvalósítására a közeljövőben azért nem sok esélyt látnak a szakemberek. Pedig maga az elképzelés – energetikai szempontból legalábbis – kifejezetten hatékonynak tűnik.

A kis méretű, moduláris reaktorok (SMR-ek) teljesítménye a „rendes” atomerőműveknek töredéke. Paks négy blokkja összesen közel 2000 MW leadására alkalmas, ehhez képest az SMR-ek esetében néhányszor tíz, legfeljebb néhány száz megawattról beszélünk. Azt sem szabd elfelejteni, hogy ilyen, kis méretű és teljesítményű reaktorok már évtizedek óta több ország haditengerészeténél megtalálhatók hadihajókba és tengeralattjárókba beépítve. Azt is el kell mondani, hogy bizony számos „esemény” fűződik ezekhez. Igaz, ezek többsége még a hidegháború idején, szovjet hadihajókon történt, de a nukleáris energiához fűződő, vélt vagy valós veszélyek a mai napig élénk visszhangot váltanak ki. Így annak, aki elsőként kíván egy mikroméretű reaktort telepíteni egy adatközpont betáplálására, erős társadalmi ellenállással is kell számolnia.

Kis fogyasztás

De mi történik akkor, ha megfordítjuk a gondolatmenetet, és azt tűzzük ki célul: fogyasszunk kevesebbet? Mi lenne, ha a tárolt és feldolgozott adatmennyiség rohamos növekedését nem követné vagy legalábbis nem ekkora iramban az energiaigény? A pesszimista meglátás szerint kisebbfajta csoda: számos tényező nehezíti ugyanis a maximálisan takarékos adatközpontok kialakítását. Csak gondoljunk bele abba, hogy az esetek többségében nem az adott központ tulajdonát képezik az ott üzemeltetett szerverek, hálózati eszközök. Így ezek fogyasztására, ennek visszaszorítására meglehetősen kevés eszköze van. Még nehezebb területnek minősül a régebbi, vagy nem eleve ilyen célra kialakított épületek, helyiségek hatékonyabbá tétele. Nem ritka eset, ha a fizikai védelem számít prioritásnak: itt a méretes vasbeton falak vonzzák a vevőket, nem az alacsony szintre szorított áramszámla.

A változás azonban ma már elkerülhetetlen. Ezt nem csupán az anyagiak indokolják és vezérlik, de a közvélemény kényszerítő erejét és a szabályozói oldal lassú, de biztos változását sem lehet figyelmen kívül hagyni. Néhány évvel ezelőtt még sokan elnéző mosollyal bólintottak a „fenntarthatóság”, a „zöld energia” vagy a „környezetbarát informatika” kifejezések olvasásakor. Ma már ott tartunk, hogy a Microsoft számít a klímaváltozás elleni harc egyik legnevesebb résztvevőjének. A redmondi cég óriási összegeket fektet zöld energiával foglalkozó cégekbe, és természetesen saját karbonlábnyomát is igyekszik csökkenteni. Nem is akárhogyan: 2030-ra karbonnegatív lesz a működésük.

Nagy változás

Az ilyen jellegű, radikális fordulathoz azonban nagyon sok mindenre szükség van. majdnem olyan sokra, mint amennyi „hagyományos” energiát ma elfogyaszt egy-egy méretesebb adatközpont. Szükség van például a megújuló energiák minél nagyobb arányú kiaknázására. Azonban nem mindenhol van annyi vízierőmű, mint Norvégiában, ahol az ország elektromos energiatermelésének mintegy 90 százalékát oldják meg a folyók segítségével, nem fúj folyamatosan a szél, vagy nincs annyi geotermikus erőmű, mint a távoli Izlandon, ahol külön reklámkampányt húztak fel erre a szerencsés helyzetre.

Ennek megfelelően egy-egy új adatközpont helyszínének kiválasztásakor ma már egyre nagyobb hangsúlyt kap a zöld energiához való hozzáférés. A szerencsés lokáció azonban csak az egyik eleme ennek az összetett kérdésnek: nincs takarékos üzemeltetés hatékony és kis fogyasztású, megfelelően méretezett, megtervezett és kivitelezett hűtőrendszer vagy éppen kis fogyasztású szerverek, hálózati elemek alkalmazása nélkül.

Mint az informatika minden területén, itt is a rendszerben gondolkodás, a megfelelő jövőkép kialakítása, a gondos tervezés hozhat csak szemmel látható, és ami még fontosabb: zsebet kímélő megoldást. Márpedig helyzet van: csak gondoljunk arra, hogy az elektromos gépjárművek elterjedése mekkora pluszterhet jelent majd az alapos infrastrukturális lemaradásokkal és kapacitáshiánnyal küszködő európai energiahálózatra. ■

Adatközpontok energiafogyasztása (terawattóra)

Figyeljük meg, hogy a 2020-as „járványévben” a hyperscale adatközpontok fogyasztásának emelkedése ellenére sem változott számottevően az összesített fogyasztás.

Év	Hagyományos adatközpontok	Felhős adatközpontok	Hyperscale adatközpontok	Összesen
2015	97,62	61,98	31,11	190,71
2016	83,72	70,33	75,17	229,22
2017	70,11	75,14	49,78	195,03
2018	60,55	76,27	60,87	197,69
2019	50,42	71,70	69,72	191,84
2020	41,00	72,90	76,23	190,13
2021	32,61	71,62	86,58	190,81

FORRÁS: TECHTARGET

EGYETLEN ILYEN SZINTŰ AWS-PARTNER VAN MAGYARORSZÁGON

Felhőben profik

Tudatosan tervezett szervezetépítés, szilárd jövőkép, jól felkészült kollégák, folyamatos továbbképzés: a TC2 2016 január elseje óta járja azt az utat, melynek fontos állomása volt az, hogy ma már – Magyarországon elsőként – Amazon Web Services Migration Competency partnerként dolgozik együtt ügyfeleivel.

A TC2 növekedési lehetőségeit alapvetően és szerencsére pozitívan befolyásolja, hogy a nagyvállalati szegmens mind Magyarországon, mind Európában az elmúlt 2-3 esztendő során arra a felismerésre jutott, hogy részben vagy egészben „felhőbe kell menni". Az IDC 2022 nyarán közzé tett felmérése ezzel kapcsolatban arra válaszolt, hogyan érhető el termelékenységnövekedés; mennyire lesznek biztonságosak az érzékeny és kritikus alkalmazások, adatok a felhőben; hogyan fejleszti a felhőinformatikára áttérés az egyre kritikusabbá váló agilitást, kiemelten például a piacra jutási időt.

A migráció komoly szakmai felkészültséget igényel: tervezést, amelyben az informatikai platform, adatbázis(ok) és alkalmazás(ok) migrációját hajtjuk végre az ehhez optimálisra tervezett AWS architektúrában.

Az AWS konkrét elvárásokat támaszt a migráció szakmai keretrendszerére, és a dokumentációs rendre vonatkozóan is ezekkel a projektekkel kapcsolatban. Az az AWS partner, amely ezen elvárásokon túl a meghatározott számú, szakmai szintű hivatalos AWS vizsgákat is teljesíteni tudja, továbbá megfelelő méretű, darabszámú referenciamunkát tud felmutatni, az belevághat a Migration Competency Partner programba.

Ennek során egy igen alapos, az AWS által megbízott, külső cég által elvégzett auditra és négy, az auditálás során a lehető legalaposabban megvizsgált referencia projektre volt szükség. A TC2-nek az audit folyamatban azt kellett dokumentációkkal alátámasztva bizonyítania, hogy a migráció lépései és eszközei sablonozott folyamatokban (természetesen az egyes ügyfelek sajátosságait figyelembe véve!) és nem ad hoc módon történtek meg. „Az auditálási folyamat komoly, de nem teljesíthetetlen kihívást állított a TC2 elé", szögezte le *Ákos György*. „Szerencsére a megfelelő tudás és tapasztalat mellé kollégáink a partneri viszonyhoz szükséges, magas szintű szakmai vizsgákkal is rendelkeztek – ehhez jelentett megfelelő alapot a már említett, folyamatos fejlődés és a szakmai

FORRÁS: TC2

RÉVÉSZ RÓBERT ÉS ÁKOS GYÖRGY, A TC2 TÁRS-ALAPÍTÓI ÉS VEZETŐI

továbbképzések sorozata. Természetesen szükség volt olyan, az auditálási folyamatba bevonható, sikeres migrációval zárult esettanulmányokra is, amelyek mérete, komplexitása megfelelt az AWS elvárásainak." A migrációs program támasztotta kihívást a TC2 2022-ben teljesítette, így 2023 január elejétől hivatalosan – Magyarországon elsőként – elérte a Migration Competency partneri szintet.

Megjegyzendő, a térségben is nagyon kevés cég rendelkezik ilyen kompetenciával és tanúsítással. Ezzel a ranggal a CEE- és EMEA-régiókban is azon kiemelt partnerek ligájába tartozik a TC2, amelyben jogosult az AWS által biztosított kereskedelemtámogató eszközök használatára, így csökkenteni tudja ügyfelei számára a migrációs projektek bekerülési költségét, valamint az éles üzemű működés folyó költségét is.

„Maga az auditálás nem csupán a Migration Competency Partner cím elnyerése miatt hasznos számunkra", tette hozzá Ákos György. A migrációk végrehajtása közben kialakultak azok a gyakorlatban finomított eljárások, ellenőrző listák, amelyeket alkalmazva szabványosított folyamatokon alapulóvá válik egy-egy nagyvállalat részleges vagy teljes felhőbe költöztetése. Márpedig a TC2 feltett célja, hogy az Alpac Capital EWVC alapjának 2022-es, 2 millió eurós befektetését okosan felhasználva, létszámot növelve új szolgáltatásokkal bővítse portfólióját, a növekedésben immár a regionális és európai piacra támaszkodva. ■

FORRÁS: DREAMSTIME

Akkor jó az adat, ha két helyen is megvan

A zsarolóvírusok és egyéb kiberbiztonsági veszélyek árnyékában rendkívül sokat kockáztat az a vállalat, amelyik nem készít rendszeresen biztonsági másolatot adatairól.

A modern tárolórendszerek már kész megoldásokat kínálnak ezekre a feladatokra. A NetApp kínálatában például a SnapMirror látja el ezeket a funkciókat. Feladata, hogy az elsődleges tárolóról egy – földrajzilag távol lévő – másodlagos tárolóra töltse át az adatokat, és onnan biztosítsa azok elérhetőségét, ha az elsődleges helyen katasztrófa történik.

Segítségével biztosítható az adatok magas rendelkezésre állása és a kritikus alkalmazások gyors adatreplikációja. A SnapMirror adatvédelmi funkcióval gyorsan és hatékonyan mozgathatjuk az adatokat a szervezeten belül, valamint rendszerfrissítéseket telepíthetünk a teljesítményre gyakorolt minimális hatással. Ha az adatokat egy vagy több NetApp tárolórendszerre replikáljuk, és folyamatosan frissítjük a másodlagos adattárolót, az adatok naprakészek maradnak, és bármikor rendelkezésre állnak, amikor csak szükség van rájuk.

A NetApp rendszerei háromféle, katasztrófa utáni helyreállítási (disaster recovery, DR-) megoldást kínálnak.

Másolás, amikor akarjuk

Az első az aszinkron SnapMirror. Ez az iSCSI vagy Fiber Channel kapcsolat távolságától függetlenül több módszert is kínál az adatok védelmére. Időszakosan snapshot-másolatokat készíthetünk az adatokról egy köteten (volume-on); átmásolhatjuk őket egy célkötetre; vagy megtarthatjuk őket. A célkötet lehet az adott virtuális gépen (VM-en) belül; egy másik VM-ben a klaszteren belül, vagy másik VM-ben egy másik klaszterben.

Az aszinkron tükrözés során be kell állítani az ütemezést is, vagyis, hogy mikor történjen az adatok replikációja. A célkötetre csak az aktuális és másolt adatok közötti különbségek fognak kerülni.

A SnapMirror-kapcsolatban lévő célkötetek egészen addig csak olvashatóak, amíg a katasztrófa miatt át nem kell venniük a feladatokat. Ha adatszivárgás, véletlen adattörlés, vagy offline állapot következik be, a célkötet írható lesz. Ez alatt az idő alatt azonban a SnapMirror kapcsolat megszakad. Amikor a forráskötet ismét elérhetővé válik, az adatokat újra kell szinkronizálnunk a célhelyről, a módosításokat frissíteni kell, valamint a forrásköteteket is újra kell aktiválnunk.

Replikáció virtuális gépek között

A második módszer az úgynevezett Storage Virtual Machine Disaster Recovery (SVM DR). Ez olyan megoldás, amely egy adott virtuális géphez tartozó köteteken replikálja a konfigurációkat és az adatokat. Az újonnan hozzáadott kötetek automatikusan védelmet kapnak.

A NetApp SVM DR a katasztrófatűrő képességet a virtuális gépen (SVM-en) belül teszi lehetővé. Itt egyaránt lehetőség van külön az SVM-volume adatok helyreállítására vagy a teljes SVM-konfiguráció helyreállítására. Miután az SVM–DR kapcsolat létrejött, csak a művelet meghibásodása esetén szükséges manuálisan beavatkozni. Minden egyéb esetben a rendszer önállóan működik az előre beállított folyamatok alapján. Ha a forrás SVM elérhetetlenné válik, a cél SVM automatikusan aktiválódik.

Folyamatos adatáramlás

Végül a harmadik megoldás a SnapMirror Synchronous (SM-S) technológia. Ez kötetszintű, folyamatos és automatikus adatreplikációt biztosít, amelyre a vállalatoknak biztonsági mentés, katasztrófa utáni helyreállítás, adatmobilitás, vagy folyamatos rendelkezésre állás miatt lehet szükségük, nulla adatvesztéssel. Az aszinkron megoldással ellentétben itt minden adat átmásolódik a célkötetre. A szinkron működés Fibre Channel kapcsolaton, maximum 10 km távolságig lehetséges, miközben a célklaszteren a forrásklaszterével megegyező, vagy magasabb verziójú ONTAP szoftvernek kell futnia.

Természetesen a való életben minden DR egyedi kihívásokat jelent, ezért mindig fontos, hogy a saját igényeinknek megfelelő megoldást alkalmazzunk. *(X)*

ALEF

NetApp