UGYANAZOK AZ ALAPELVEK

Nem ördöngösség a felhőbiztonság

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

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

A több nem feltétlenül jobb

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

NAGY ZOLTÁN, A MAGYAR TELEKOM CSOPORT BIZTONSÁGI IGAZGATÓJA

FORRÁS: T-SYSTEMS

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

Ellenőrzött hozzáférés

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

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

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

Feladatok és felelősségek

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

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

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

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

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

Előny a hibrid felhőnél

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

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

Üzemeltetni is egyszerűbb

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