CSINOS TAMÁS,
CLICO HUNGARY

FORRÁS: ITB

KIRÁLY ISVÁN,
KINGSOL

FORRÁS: ITB

URZICA OLIVER,
PRIANTO MAGYARORSZÁG

FORRÁS: PRIANTO

NEMCSAK A KONTROLL, DE A FELELŐSSÉG IS NÁLUNK VAN

Van beleszólásunk a felhőben tárolt adataink védelmébe?

Tavaly a cégek túlélésének záloga az volt, hogy a komplett IT-infrastruktúrát a megváltozott körülményekhez igazították, a folyamat katalizátora pedig legtöbb esetben a felhő volt. Gyors és széles körű térnyerését követően azonban egyre-másra bukkantak fel a technológia adatbiztonságát firtató, kevésbé pozitív vélemények, a felhőben tárolt adatok védelme pedig az egyik legtöbbet vitatott kérdéssé vált. Az adatbiztonsági anomália kapcsán azt kerestük, hol húzódik a felelősségvállalás határa a szolgáltató és a felhasználó között.

A Prianto Magyarország 2020 végén lefolytatott felmérése arról számolt be, hogy a felhőalapú technológiák adoptációja 26 százalék körüli hazánkban. Noha ez a folyamat már korábban is elindult, azért még közel sem tart azon a szinten, mint a nyugati országokban. A járvány okozta pánik és távmunkatrend a vállalatokat ezen törekvéseik felgyorsításra ösztönözte, ám igazi nagy áttörést az hozhat majd, amikor a kormányzati és közigazgatási intézmények körében is elfogadottabbá és elterjedtebbé válik a felhő használata. Addig is viszont fontos, hogy a felhasználók a felhő biztonsági vetületét is jobban átlássák.

„Nemcsak beleszólásunk van, hanem a mi felelősségünk a szolgáltatóknál tárolt adataink védelme. Az emberi hibák kiküszöbölhetetlenek, például nem szándékos adattörléssel szinte mindenki találkozott már. Azonban egy felhasználó helytelenül beállított vagy maradványjogosultságai is vezethetnek komoly adatvédelmi incidenshez. Többek között ezek a problémák is a szolgáltatás igénybe vevőjének felelősségébe tartoznak. Fontos, hogy a felhasználói, hozzáférési jogosultságokat megfelelően kezeljük, például egy, az identitást vagy a kiemelt jogosultsággal rendelkező felhasználókat kezelő technológia révén”, fogalmazta meg *Urzica Olivér,* a Prianto Magyarország vezetője.

Ugyanis nem minden felelősség a szolgáltatóé, sőt. A felhő alapú szolgáltatás igénybevételével együtt jár a megosztott felelősségi modell vállalása, ugyanakkor felmerülhet a kérdés, hogy a felhasználók mennyire vannak tisztában saját, illetve a szolgáltatók felelősségével.

Minden szolgáltatásnál máshol húzódik a határ

A tapasztalat azt mutatja, hogy például a kis-és középvállalkozások sokszor nem is tudják, hogy attól, hogy fizetnek egy bizonyos felhőszolgáltatásért, az adataik biztonságáért saját maguk felelnek. De ugyanez igaz a nagyvállalati közegre is.

„Sokféle felhő létezik, biztonsági szempontból azonban „as-a-service-eket” kell megkülönböztetni. Dióhéjban összefoglalva megkülönböztetünk Infrastructure as a service (IaaS-), Platform as a Service (PaaS-) és Software as a Service (SaaS-) szolgáltatásokat, ahol minden esetben máshol húzódnak felelősség határai. Az IaaS esetében majdnem minden a felhasználó felelőssége, mert a szolgáltató csak azért kezeskedik, hogy a számítási kapacitást bármikor elérhetővé tegye. PaaS esetén a szolgáltató a hálózatot, a szervereket, operációs rendszert, tárhelyet és az egyéb alapszolgáltatásokat biztosítja, míg a felhasználó felelőssége az alkalmazás telepítése, konfigurációja, védelme. SaaS-nál pedig az ügyfél- és a személyes adatok védelme megint csak a felhasználó felelősségévé válik, hiszen a szolgáltató csak a szoftverfunkcionalitást bocsátja rendelkezésre”, foglalta össze *Csinos Tamás,* a Clico Hungary ügyvezetője.

A megosztott felelősségi modell tehát nemcsak az informatikára nézve, hanem jogi és üzleti szempontból is fontos, ezért átfogó modellként kell működnie. Ezáltal bizonyos, főként az üzemeltetéssel kapcsolatos terhek lekerülnek az előfizetők válláról, így több erőforrást tudnak allokálni az adatvédelmi folyamatok megerősítésére. Az informatikai infrastruktúra szervezettebbé, a rendszerek áttekinthetősége és menedzsmentje könnyebbé válik a megfelelő eszközök kiválasztásával.

Beépített javaslatokkal a megfelelésért

Ahogy a fentiekből is körvonalazódik, maga a felhasználó sokat tehet azért, hogy az adatai biztonságban legyenek. Ennek kapcsán *Király István,* a King-Sol vezérigazgatója megfogalmazta azokat az ajánlásokat, amelyek általánosságban, cégfüggetlenül segítenek a felhőt biztonságosabbá tenni.

„A felhőbeli erőforrások hozzáférésének kezelése kritikus, így a beállítást a hozzáférés-vezérléssel kell kezdeni. Szintén stabil védelmi pont a többfaktoros hitelesítés, a lemeztitkosítás. Adatszivárogtatás ellen pedig Data Loss Prevention (DLP-) megoldásokkal lehet védekezni. Mindezeken túl vannak úgynevezett biztonsági pontszámok, amelyeket a felhasználó kap, miután elvégezte a beállításokat. A rendszer százalékosan értékeli ezeket, és a kapott pontszám függvényében javaslatokat tesz, hogyan lehetne elérni a maximális védelmet. Ha több cég vagy több rendszergazda fér hozzá a felhős környezethez, akkor létezik egy olyan beépített megoldás is, az Azure Policy, amely segít a szervezeti szabványok betartatásában és a megfelelőségi követelmények kiértékelésében”, összegezte Király István.

A Microsoft egyébként ad egy biztonsági javaslatlistát, amellyel ellenőrizhető, hogy milyen beállításokat kell még elvégezni ahhoz, hogy az adott minősítésnek megfelelhessen a cég.

A felhőszolgáltatásokat nyújtó cégek ragaszkodnak a megosztott felelősségi modellhez, hiszen az általuk nem befolyásolható eseményekért nem vállalhatnak felelősséget

A munkafolyamatok megóvása is kulcsfontosságú

Ami a felhőben tárolt adatok és munkafolyamatok megfelelő biztosítását illeti, „kritikus, hogy céges oldalról olyan megoldásokat és folyamatokat alkalmazzanak, amelyek biztosítják a megfelelő hozzáférési jogosultságokat az identitások teljes életciklusa alatt. Ilyen a One Identity Manager, a Privileged Account Management; az adatok védelmét és azonnali elérését, illetve mentését, amilyen például a Unitrends „hardened” Linux rendszerre épített megoldása, a tevékenységek és alkalmazások felhasználásának monitoringját, illetve nyomon követhetőségének metódusát. Így nem csak a szankciókat, botrányokat, potenciális üzleti károkat, pereket és az IT összeomlását lehet elkerülni, hanem hatékony, optimális működést is biztosíthatunk a cégek és munkavállalóik számára”, mondta Urzica Olivér.

Szintén kritikus, hogy miként azonosítják a cégek a felhasználókat, ugyanis ez a felhős rendszereknél más megközelítést igényel. „A saját infrastruktúra esetében vannak olyan fizikai ellenőrzési pontok, amelyek alapján azonosítani lehet a felhasználót. Távolról ellenben nehezen lehet meggyőződni arról, hogy adott esetben tényleg a marketingmenedzser lépett-e be a levelezésébe vagy valaki más, aki annak adja ki magát. Nem lehet elégszer hangsúlyozni, hogy a felhasználó az új végpont, így elsősorban őt kell megvédeni”, zárta a gondolatait Csinos Tamás.

Kiss Franciska

Stúdióminőségben rögzített beszélgetések

Letölthetők, streamelhetők:

Portrék, interjúk

Stúdióbeszélgetések
- Cégbemutatók
- Aktuális ICT-piaci esemény megvitatása
- Tematikus ICT-magazinok

Élő podcast felvételek
- ITB-rendezvényeken
- Nyilvános eseményeken

ITB PODCAST