



Hogyan védj a felhő alapú infrastruktúrát?

Ez a gyakorlati útmutató a biztonságról és az adatkezelésről új felhőfelhasználók számára jó kiindulópont az adatbiztonsággal és az adatkezeléssel kapcsolatos kockázatok és aggályok csökkentéséhez.

Amikor a felhőalapú számítástechnika először népszerűvé vált, a biztonság volt a CIO-k legnagyobb aggodalma, amikor azt fontolgatták, hogy bevezessék-e ezt az új IT-támogatási alternatívát. A félelmek az egyszerűtől, például a hozzáférés ellenőrzésétől, a jelentősig terjedtek, például hogy ezek az új, hyperscale platformok és alkalmazások mézesmadzagként szolgálhatnak a bűnözők számára, akár hozzáférések megszerzésére, akár rosszabb célokra. Ma azonban a legrosszabb biztonsági félelmeink nagyrészt eloszlottak. A kockázatok többségét sikerült mérsékelni, és most már évtizedek tapasztalatából profitálhatunk.

Valójában a biztonsági helyzet fordulatot vett: míg korábban gyakran ez volt a vállalati bevezetés legnagyobb akadálya, ma már sok IT-vezető részben azért választja a felhőt, mert annak biztonsága jobb, mint amit a legtöbb szervezet saját adatközpontjaiban elérhetne.

A felhőszolgáltatók rendelkeznek a szükséges készségekkel, infrastruktúrával, folyamatokkal és technológiával az adatok védelméhez. Azonban az ügyfeleknek is kulcsszerepet kell játszaniuk abban, hogy biztosítsák saját eszközeik épségét.

Íme néhány kulcsfontosságú szempont a felhővel újonnan ismerkedő vagy a biztonsági alapokat újragondoló informatikai vezetők számára:

Dolgozz együtt a felhőszolgáltatóddal, hogy megértsd a biztonsági intézkedéseiket.

Nem elég egyszerűen átruházni az adatok és alkalmazások védelmének felelősségét. A hozzáállásnak a megosztott felelősségen kell alapulnia. Kritikus fontosságú, hogy szorosan együttműködj a partnerekkel, és tisztán értsd, ki milyen szerepet és feladatot vállal a felhőben tárolt eszközeid védelmében. Ne becsüld túl a felhő megosztott felelősségi modelljét: ez továbbra is a te környezeted, a te operációs rendszered és a te adataid.

Vezess be erős hozzáférés-ellenőrzési intézkedéseket.

Nem mindenkinek kell ugyanazokhoz az alkalmazásokhoz, adatokhoz és szolgáltatásokhoz hozzáférnie. Sőt, előfordulhat, hogy csak bizonyos szintű engedélyekre van szükségük, nem teljes irányításra, és ezekre az engedélyekre sem 24/7-ben van szükségük. A személyi hozzáférés-kezelés, valamint a többtényezős hitelesítés okos megoldás lehet annak korlátozására, hogy mikor és ki jogosult az adataid megtekintésére vagy módosítására.

Használd ki a titkosítás erejét.

Titkosítsd az adatokat nyugalmi állapotban, továbbítás közben és feldolgozás során, hogy ha az adatok rossz kezekbe kerülnek, ne legyenek értékesek a támadók számára. Az adatok algoritmus segítségével olvashatatlan karakterekké alakítása mára az egzotikusból megszokottá vált, mivel egyértelművé váltak az előnyei és hasznossága. Győződj meg róla, hogy te is kihasználod ezt a lehetőséget.

Készíts rendszeresen biztonsági mentéseket.

Az adatok másolása egyszerű, de alapvető üzletmenet-folytonossági képességet biztosít incidensek esetére. Ugyanígy, a rendszerek rendszeres javítása és frissítése (ami a felhőben sokkal egyszerűbb, mint helyszíni IT használatakor) alapvető higiéniai tényező. Felhőszolgáltatód segíthet a legjobb megközelítés kidolgozásában az adott bevezetés és az igényeid szerint.

Frissítsd rendszeresen az üzletmenet-folytonossági tervedet.

A gyakori biztonsági incidensekre való felkészüléssel a szervezet felkészültségi kultúráját alakít ki. Kérd meg felhőpartneredet, hogy segítsen biztonsági auditot végezni, és ezt időről időre ismételjétek meg – évente kétszer egy jó gyakoriság.

Kommunikálj és oktass.

A biztonság mindenki feladata. Oktasd a szervezet minden tagját az adatok kezeléséről, a gyanús tartalmakra való kattintás kockázatairól, a nem jóváhagyott szoftverek letöltéséről és a szociális manipuláció veszélyeiről.

Kövesd nyomon a szélesebb környezet változásait.

Bizonyos szabályok és törvények változásai befolyásolják, hogy, hogyan kell kezelned az adatokat. Gondoskodj róla, hogy szervezeted megbízható hírforrásokból figyelemmel kísérje a nemzetközi adatkezelési szabványok, például a GDPR, NIST és más vonatkozó kódexek frissítéseit. A felhőhöz tartozó modern monitorozási és menedzsmenteszközök segítenek betartani ezeket a szabványokat. Ezek nemcsak téged érintenek közvetlenül, hanem befolyásolják az aktuális adatbiztonsági gondolkodást is. Emellett gondoskodj arról is, hogy valaki a csapatból nyomon kövesse a biztonsági problémákról szóló híreket, például az új fenyegetési mintákat, hogy a csapat naprakész legyen.

Figyeld az anomáliákat.

A szokatlan minták észlelése további vizsgálatot igényelhet, és segíthet a problémák kezelésében, mielőtt azok komolyabbá válnának. Például egy adott webhelyre irányuló szokatlanul nagy forgalom vagy furcsa hálózati mintázatok esetén azonnal lépj kapcsolatba a partnereiddel. Együtt meghatározhatjátok a kockázatokat, és szükség esetén lezárhatjátok a problémás területeket.

Dolgozz együtt szakértői partnereddel.

A felhőbevezetésért felelős partnereid széles körű tapasztalattal rendelkeznek – használd ki ezt. Egy jó partner nem csupán tranzakciós kapcsolatot kínál és nem mérhető pusztán egy szolgáltatási KPI-vel. Olyan partnerre van szükséged, aki a legjobb érdekeidet tartja szem előtt, és folyamatos tanácsadási forrást jelent.

Használd ki az AI lehetőségeit a biztonság érdekében.

Bár jó dolog, ha több biztonsági eszközből érkezik rengeteg jelzés, ezek csak akkor hasznosak, ha rendelkezésedre állnak olyan eszközök, amelyek képesek ezekkel dolgozni. Az AI képes feldolgozni az adatokat, és biztonsági szakértők tudásával átalakítja a jelzéseket hasznos betekintéssé. Az AI-alapú biztonsági ügynökök elérhetők a felhőből, minimális konfigurációval és képzési igény nélkül.

Mítosz, hogy a felhő alapértelmezés szerint biztonságos. Tartsd be azt a szabályt, hogy ami elromolhat, az el is fog, és maradj éber. Bár a felhőalapú számítástechnika mára elérte azt a szintet, hogy gyakran biztonságosabb, mint a helyszíni megoldások kezelése, a biztonsági helyzet folyamatosan változik. Dolgozz együtt a felhőszolgáltatóddal, hogy megértsd és figyeld a kockázatokat, így mindig védett maradhatsz.



© depositstockphotos

Készen állsz arra, hogy felfedezd a felhőmegoldásokat?

Lépj kapcsolatba velünk a cloudsolutions@telekom.hu e-mail címen.

[Tudj meg többet](#)



[Kapcsolat](#)

[Impresszum](#)



© 2025 Magyar Telekom Nyrt