



iSolutions

Biztonság a felhőben

Hogyan véd meg a cégedet
a modern kiberkockázatokkal szemben





Sok vállalat ma már használ felhőalapú rendszereket – e-mailt, fájlmegosztást, üzleti alkalmazásokat. Gyakran halljuk azt is: „a felhő biztonságos”.

Ez részben igaz. A nagy szolgáltatók, mint a Microsoft vagy a Google valóban nagyon komoly biztonsági rendszereket építettek ki. De a valóság ennél árnyaltabb.

A modern vállalati IT-biztonság nem egyetlen megoldás, hanem több egymást erősítő terület együttese. Ha ezek közül bármelyik hiányzik, a teljes rendszer sebezhetővé válhat.

Ebben az e-könyben bemutatjuk a felhőbiztonság négy alappillérét, és azt is, milyen megoldások segítenek a gyakorlatban.





A vállalati biztonság négy alappillére



A modern IT-biztonság négy fő területre épül:

Külső támadások elleni védelem (kibervédelem)

Belső visszaélések elleni védelem

Adatbiztonság

Működési biztonság (üzletmenet folytonosság)

Mind a négy pillér egyformán fontos.





1. Külső támadások elleni védelem

A legtöbb cégvezető fejében a kiberbiztonság még mindig elsősorban a hackerek elleni védekezést jelenti.



Valóban fontos terület, hiszen ma már:

- automatizált, AI-vezérelt támadások futnak a világ minden pontjáról
- zsarolóvírusok (ransomware) cégek ezreit bénítják meg
- célzott támadások indulnak akár KKV-k ellen is

Régen sok vállalat ezt „túlzásnak” gondolta.
Ma viszont már látható, hogy **a támadások mennyisége**

Tipikus külső támadások

- adathalászat (phishing)
- zsarolóvírus
- jelszófeltörési kísérletek
- fertőzött weboldalak
- rosszindulatú programok



Alapvető védelmi eszközök



Vírus- és zsarolóvírus védelem

A hagyományos vírusirtók ma már nem elegendők.

A modern védelemnek tartalmaznia kell:

- ransomware felismerést
- viselkedésalapú elemzést
- automatizált karantént



DNS védelem

Ez a védelem még a fertőzés előtt megállítja a támadást.

A rendszer figyeli a hálózati forgalmat, és ha a felhasználó egy ismert káros oldalhoz próbál csatlakozni:

- blokkolja a kapcsolatot
- megakadályozza a letöltést

Így a támadás sokszor már azelőtt megáll, hogy a számítógépre kerülne.



Naplózás és biztonsági monitorozás

A modern IT-rendszerek minden eseményt naplóznak:

- belépések
- fájlműveletek
- adminisztrátori műveletek
- hálózati események

A biztonság három szintből áll:

1. naplózás
2. naplóelemzés
3. riasztások kezelése

Ez már a NIS2 szabályozásban is kötelező elvárás.





2. Belső visszaélések elleni védelem



Magyarországon sokszor nem a hackerek jelentik a legnagyobb kockázatot, hanem a belső visszaélések.

Például:

- egy kolléga adatokat visz magával
- érzékeny információk kerülnek ki
- üzleti adatok szivárognak ki

Sok cégvezető erről nem is tud, mert nincs megfelelő kontroll. A felhőalapú rendszerek viszont számos eszközt kínálnak ennek kivédésére.



Mit lehet ellenőrizni a felhőben?

- ki nyitott meg egy dokumentumot
- ki töltött le adatokat
- ki osztott meg fájlokat
- mikor történt módosítás

Akár évekre visszamenőleg is visszakereshető, hogy ki mit csinált.
Ez nem bizalmatlanság – hanem vállalati kockázatkezelés.



3. Adatbiztonság

Az egyik legnehezebben érthető kockázat az adatvesztés.

Egy autó nem tűnik el egyik pillanatról a másikra – ha ellopják, annak nyoma van a térfigyelő kamerán, lehetnek tanúk, és a rendőrségnek is vannak eszközei az előkerítésére.

De egy adatbázis vagy dokumentumgyűjtemény el tud tűnni pillanatok alatt.

Adatvesztés történhet például:

- zsarolóvírus miatt
- emberi hiba miatt
- rendszerhiba miatt
- törlés vagy felülírás miatt

A legfontosabb védelem: mentések

A modern mentési stratégia három alapelvre épül:

1. Több példányban legyen meg az adat

- felhőben
- helyben

2. Cégen kívül is legyen mentés

Ha minden egy rendszerben van, egy támadás mindent elérhet.

3. Verziók tárolása

Így visszaállítható egy korábbi állapot.

Ez különösen fontos **zsarolóvírus (ransomware) támadások** esetén, amikor az adat megvan, de nem lehet hozzáférni.

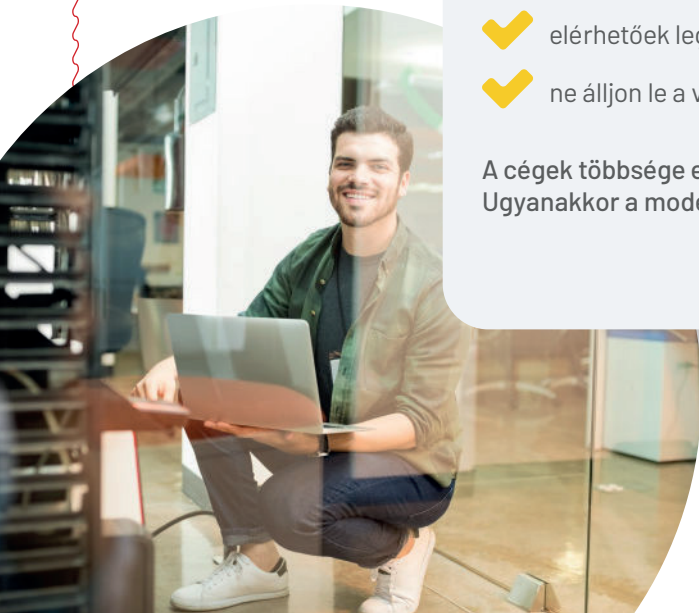




4. Működési biztonság

A negyedik pillér a legkézzelfoghatóbb.

Ez az úgynevezett üzembiztonság vagy üzletmenet-folytonosság.



A cél egyszerű:

- ✓ a kollégák tudjanak dolgozni
- ✓ működjön az internet, a nyomtató, és minden egyéb eszköz
- ✓ elérhetőek legyenek a rendszerek
- ✓ ne álljon le a vállalat

A cégek többsége ezt már jól érti, ezért gyakran erre vesznek fel IT-szakembert. Ugyanakkor a modern vállalatoknál **a másik három pillér legalább ennyire fontos.**



Miért lett most ennyire fontos a kiberbiztonság?

Az elmúlt években négy jelentős változás történt.

1. Robbanásszerűen nőtt a kibertámadások száma

Ma már nem csak véletlen támadások vannak.

Egyre több automatizált, célzott, és iparág-specifikus támadás történik.

A támadók ma már **KKV-kat is célba vesznek**, mert sokszor gyengébb a védelem.



2. Megjelent a NIS2 szabályozás

Az Európai Unió felismerte, hogy a kibertámadások **nemcsak cégeket, hanem országokat is veszélyeztetnek**.

Ma már a kiemelt stratégiai ágazatok, mint:

- a bankrendszerek,
- az energiaellátás,
- az élelmiszeripar,
- és az egészségügy

is mind digitális infrastruktúrával működik.

Egy sikeres támadás akár **teljes rendszereket és országokat béníthat meg**.

A NIS2 célja ezért:

- a kiberbiztonság szintjének emelése,
- a vállalatok tudatosságának növelése,
- és a kötelező biztonsági intézkedések bevezetése.



Mi kell a NIS2 megfeleléshez?

A NIS2 megfelelés alapja néhány jól meghatározható működési terület. Fontos, hogy a vállalat **garanciális, támogatott hardver- és szoftverkönyezetet használjon**, a rendszerek folyamatosan frissítve legyenek, és az IT működés **dokumentált formában is létezzen** (hálózati architektúra, eszközlétár, jogosultságok, katasztrófhelyzeti terv). Emellett elvárás a **magas szintű adatmentés**, amely biztosítja, hogy egy támadás vagy rendszerhiba esetén az adatok visszaállíthatók legyenek.

A NIS2 hangsúlyt fektet a **szabályozott működésre és a biztonsági kontrollokra** is. Ide tartozik az **IT biztonsági szabályzat, a naplózás és annak folyamatos figyelése**, valamint a **szigorú felhasználó- és jogosultságkezelés** (például kétfélsős azonosítás, szerepkör alapú hozzáférések). Bár ezek a követelmények elsöre túlzásnak tűnhetnek, valójában mind a cégek stabilabb, biztonságosabb működését szolgálják.



Miért lett most ennyire fontos a kiberbiztonság?

Az elmúlt években négy jelentős változás történt.

3. A felhőszolgáltatók biztonsági modellje is változott

Régen sokszor azt kommunikálták:

„Menj a felhőbe, és rögtön biztonságban leszel.”

Ma már a helyzet árnyaltabb.

A szolgáltatók többféle csomagot kínálnak:

- az alapcsomagok csak alapszintű védelmet adnak
- a komolyabb biztonsági funkciók csak a magasabb szintű csomagokban érhetőek el

Ez olyan, mintha egy ház védelme esetében az alapcsomag a zár az ajtón, de amennyiben komoly védelmet szeretnél, a prémium csomag tartalmazná a kamerát és a riasztóberendezést.

4. A cégek egyre tudatosabbak

Egy sikeres kibertámadás következményei súlyosak lehetnek:

- üzleti leállás
- reputációs kár
- pénzügyi veszteség
- partneri bizalom elvesztése

Ezért egyre több cégvezető érti meg,
hogy a biztonság befektetés, nem költség.





Gyakorlati lépések és tippek a vállalati IT-biztonság növelésére

A modern felhőbiztonság több alapvető intézkedésből áll.



Eszközmenedzsment

Csak ellenőrzött eszközökről lehessen hozzáférni a céges rendszerekhez.

Például:

- csak céges laptopról lehet belépni
- ismeretlen eszközről tiltott a hozzáférés
- adminisztrátori jóváhagyás szükséges

Felhasználói hitelesítés

A hozzáférések védelme kritikus.

Fontos elemek:

- kétlépcsős azonosítás (2FA)
- erős jelszabályok
- autentikátor alkalmazások
- hozzáférési korlátozások – a céges rendszerekbe csak meghatározott helyekről (pl. irodai vagy otthoni hálózatról, illetve csak adott országon belülről) lehessen belépni

Ez ma már **alapkövetelmény**.



Központi címtár

Egy szerver használata esetében a rendszergazda veszi fel a felhasználókat, akik így tudnak bejutni a céges számítógépekre.

A felhőben alapvető esetben ez csak az alkalmazásokat védi, például az e-mail rendszert, a dokumentumokat, és a chat-et. Ugyanakkor a modern felhőszolgáltatások (Microsoft, Google) most már lehetővé teszik, hogy a felhasználók:

- egyetlen központi rendszerben legyenek kezelve
- egységes jogosultságokkal
- központi biztonsági szabályokkal

Tehát ma már akár **a számítógépes belépést is lehet a felhővel védeni**, és ezt ajánlott mindenhol bekapcsolni.

Felhasználói aktivitás naplózása

A rendszerek képesek rögzíteni:

- ki, mikor, honnan lépett be
- milyen adatot módosított
- mit töltött le

Ez segít a:

- belső visszaélések megelőzésében
- incidensek kivizsgálásában
- audit megfelelésben



Megéri a magasabb biztonsági szint?



Sok cégvezető számára a licenrdíj növekedése elsőre soknak tűnik.

Például egy magasabb Microsoft 365 csomag **felhasználónként havi néhány ezer forinttal drágább.**

Ez azonban, ha jobban belegondolunk, egy nagyon kicsi összeg.

Összehasonlításképpen:

- az irodai kávé ára havonta
- 50-100 km üzemanyag
- vagy egy gyorséttermi ebéd.

Egy prémium csomagnak további előnyei is vannak. A biztonság mellett a termékek tudása is nagyobb, például mesterséges intelligenciát is tartalmaznak, amelybe a legtöbb vállalat egyébként is befektet.

A biztonság hiánya viszont hatalmas kockázatot jelenthet.



Egy támadás következményei lehetnek:

- adatvesztés
- üzleti leállás
- partneri bizalom elvesztése
- pénzügyi kár

Ezért a megfelelő biztonság mindig megtérülő befektetés.



Esettanulmány

Egy közelmúltbeli kibertámadás jól mutatja, milyen súlyos következményei lehetnek egy sikeres behatolásnak.

2021-ben az UNIX Autót súlyos zsarolóvírus-támadás érte: egy banki levélnek álcázott e-mailek keresztül jutottak be a támadók, majd hetekig észrevétlenül feltérképezték a teljes hálózatot, megszerezték a jogosultságokat, végül néhány perc alatt megbénították a vállalat működését.

A teljes cégcsoport leállt három országban, bezártak az üzletek, megállt a logisztika, és a támadók 2,7 millió dollár váltságdíjat követeltek. A közvetlen veszteség végül jóval több mint 1 milliárd forint lett, de akár a 2 milliárdot is elérhette.

A történet legfontosabb tanulsága, hogy a korábban elegendőnek hitt védelem – tűzfalak, vírusirtók, mentések – ma már önmagában nem elég: a problémát többek között szigorú jelszópolitikával, jogosultságkezeléssel, kétlépcsős hitelesítéssel, rendszeres frissítésekkel, hálózati szegmentálással, külső biztonsági felügyelettel és valóban elkülönített, hálózatról leválasztott mentésekkel lehetett volna nagy eséllyel megelőzni vagy legalább enyhíteni.

A megoldás végül nem a váltságdíj kifizetése lett, hanem a teljes rendszer újrakepítés: külső szakértőkkel és egy 50–60 fős csapattal gyakorlatilag nulláról állították helyre az infrastruktúrát, miközben az egész hálózatot újragondolták és sokkal biztonságosabb alapokra helyezték.

Bár a helyreállítás rendkívül fájdalmas és költséges volt, a cég végül modernebb, megbízhatóbb és jobban védett IT-környezettel állt talpra. Ez az eset jól mutatja, hogy a kibervédelem nem pusztán IT-kérdés, hanem közvetlen üzleti kockázat: ha nincs megfelelő megelőzés, a veszteség nemcsak technikai, hanem pénzügyi, működési és reputációs szinten is óriási lehet.





Miért fontos a szakértői támogatás?

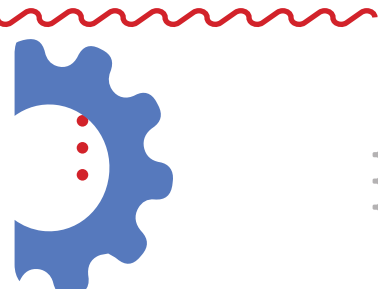


A modern biztonsági rendszerek rendkívül összetettek.

Sok cégnél látjuk például, hogy ugyan beszerezték a drágább csomagot, de a funkciók nincsenek megfelelően beállítva.

Vagy éppen fordítva: olyan drága licencet fizetnek, amelyre valójában nincsen szükség.

Ezért fontos a cégre szabott szakértői tervezés és beállítás.





A jó IT szolgáltató most fontosabb, mint valaha!

A vállalati adatbiztonság megteremtésében az IT szolgáltatónak kulcsfontosságú szerepe van. És hogy milyen egy jó rendszergazda? Nos, hadd mutassuk be a legfontosabb szempontokat!



✓ **Értse az üzleti folyamatokat!** – Nagyon fontos, hogy a rendszergazda értse és átlássa azt, mi a vállalkozás célja, és ennek megfelelően javasoljon hatékony informatikai megoldásokat.

✓ **Legyen transzparens!** – Fontos, hogy a vállalkozás számára világos legyen, hogy a rendszergazda hogyan dolgozik, mi alapján hoz döntést és tesz javaslatokat. Ha egy szolgáltató nem enged betekintést a munkafolyamataiba és nem tudja alátámasztani döntéseit, abból arra következtethetünk, hogy ő maga sem látja át, hogy mit miért csinál.

✓ **Fókuszáljon a hatékonyságra!** – Az üzleti informatikai megoldások szempontjából fontos, hogy a hangsúly a hatékonyságon és ne az áron legyen! A legdrágább megoldás természetesen nem mindig a legjobb, de a legolcsóbbat érdemes fenn tartásokkal kezelni.

✓ **Legyen mindig készenlétben!** – A rendelkezésre állás kérdése nagyon fontos szempont, hiszen egy nem elérhető rendszergazda hatalmas károkat tud okozni a vállalkozás számára. Gondoljunk csak bele, milyen sokba kerülhet a cégnek, ha két-három napot áll amiatt, mert nem éri el a rendszergazdát.

A jó IT szolgáltató mindig kincset ér egy vállalkozásnak, de a jelenlegi gazdasági helyzetben különösen fontos, hogy megfelelő partneri viszony jöjjön létre a két fél között!

+++++

Bízd ráink az informatikát és növekedj biztonságosan a felhőben!

Tapasztald meg Te is, hogy a felhőben történő munka mennyivel
hatékonyabbá teszi céged működését!

Vedd fel velünk a kapcsolatot az űrlap kitöltésével!



<https://www.isolutions.hu/kapcsolat/>

Elérhetőségeink

2040 Budaörs, Baross utca 89.

Új érdeklődés, konzultációs igény: + 36 20 457 7703

Ügyfélszolgálat, support: +36 1 506 0900

gondolategbreszto@isolutions.hu



iSolutions



Google Cloud
Partner



Microsoft 365
Partner