

7 ok, amiért foglalkozni kell a Microsoft 365 biztonsági mentésével

Miért fontos, hogy a
szervezetek védjék a
Microsoft 365 adataikat?
Esettanulmány



Bevezető

Ellenőrzés alatt tartja Microsoft 365 adatait? Hozzáfér az összes szükséges elemhez? A reakció jellemzően "Természetesen igen" vagy "A Microsoft gondoskodik mindenről."

De ha tényleg belegondolunk – biztosak lehetünk-e benne?

A Microsoft sok mindenről gondoskodik és magas szintű szolgáltatást nyújt ügyfelei számára, de elsősorban a Microsoft 365 infrastruktúrájának kezelésére és a felhasználók rendelkezésre állási idejének fenntartására helyezi a hangsúlyt.

Gyakori tévhit, hogy a Microsoft biztonsági másolatot készít az adatokról, miközben "csak" felhívja ügyfelei figyelmét, hogy felelősséggel tartoznak saját adataikért. A figyelmeztetés figyelmen kívül hagyása kedvezőtlen és káros következményekkel járhat.

Valójában Önnek kell biztosítania az Exchange Online, a SharePoint Online, a OneDrive for Business és a Microsoft Teams adataihoz való hozzáférést és azok felügyeletét.

Ez az ismertető bemutatja a Microsoft 365 biztonsági mentés hiányának veszélyeit, és a megoldást, amely biztosítja biztonsági mentést, az adatok hosszú távú megőrzését, valamint kitölti az adatvédelem réseit.

„Aggódtunk a Microsoft 365 adatbiztonsági és megőrzési irányelvei miatt. Ezért döntöttünk úgy, hogy gondoskodunk adataink biztonsági másolatáról a Microsoft 365-ben.”

— **Karen St.Clair,**

IT Vezető

Columbia Power & Water Systems



A nagy Microsoft 365 tévhit

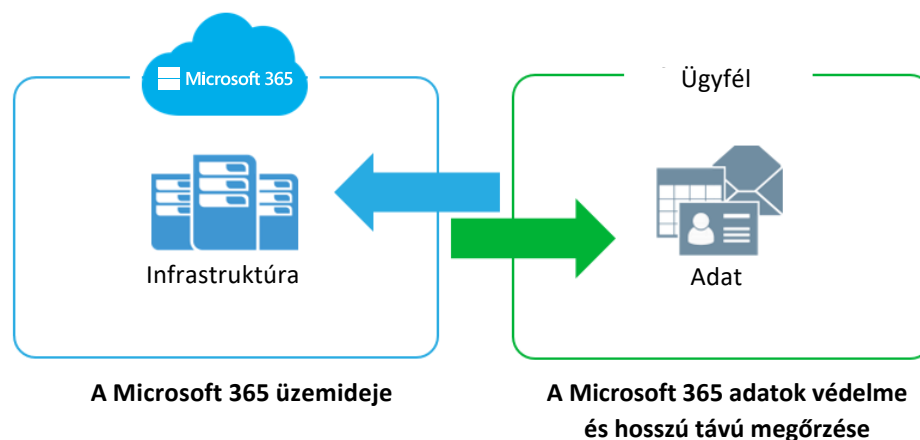
A Microsoft vélt felelőssége és a felhasználó tényleges felelőssége nem mindenki számára egyértelmű, amely problémát okoz a Microsoft 365 adatainak védelme és megőrzése terén.

A Microsoft által biztosított biztonsági mentés és az adatok helyreállíthatósága, valamint a felhasználók feltételezései gyakran eltérnek egymástól.

Ez azt jelenti, hogy a Microsoft 365 szabványos óvintézkedéseinek ellenére előfordulhat, hogy újra meg kell vizsgálnia az adatok ellenőrzésének szintjét, és a hozzájuk való hozzáférést.

A Microsoft 365 georedundanciát kínál, amelyet gyakran összetévesztenek a biztonsági mentéssel. A biztonsági mentésnek azt nevezzük, amikor az adatokról másolatot készítenek, és egy másik helyen tárolják. Azonban még ennél is fontosabb, hogy a biztonsági mentéshez közvetlenül hozzáférhessen és ellenőrzése alatt tarthassa. Ezáltal, ha adatok elvesznek, véletlenül törölődnek vagy rosszindulatú támadás célpontjává válnak – gyorsan helyreállíthatja őket. A georedundancia ezzel szemben csak a webhely- vagy hardverhibák ellen nyújt védelmet, ha infrastruktúra-összeomlás vagy leállás következik be.

A Microsoft gondoskodik az infrastruktúráról, de az adatokért továbbra is az ügyfél felel



„Minden felhőalapú telepítési típus esetében Ön birtokolja adatait és identitását.”

— Microsoft dokumentáció

7 érv, amiért foglalkozni kell a Microsoft365 biztonsági mentésével

A Microsoft 365 robosztus és nagy teljesítményű szoftver szolgáltatásplatformként (SaaS) tökéletesen igazodik számos szervezet igényeihez. Biztosítja az alkalmazás elérhetőségét és a folyamatos üzemidőt, de biztonsági mentése számos más fenyegetés ellen is védelmet nyújthat. Lehet, hogy azt gondolja:

„Valószínűleg elég jól működik a Tároló”, de ebben sokan tévednek. Az adatok kompromittálódásától annak a felfedezésig átlagosan több mint 1401 nap telik el.

Döbbenetesen nagy ez a rés, és nagy valószínűséggel észre sem veszi, hogy valami hiányzik vagy eltűnt, csak amikor már késő.

Világszerte több száz Microsoft 365-re áttért informatikai szakemberrel történt egyeztetés alapján elmondható, hogy az adatvédelmi sérülékenységi típusai közül az alábbi 7 a listavezető:



Véletlen
törlés



Adatmegőrzési
házirend
hiányosságai és
rendezetlenség



Belső
biztonsági
fenyegetések



Külső
biztonsági
fenyegetések



Jogi és
megfelelési
követelmények



A hibrid e-mail-
telepítése és
migrációja
Microsoft 365-be



Teams
adatszerkezet

¹ – <http://info.microsoft.com/rs/157-GQE-382/images/EN-GB-CNTNT-eBook-Security-HolisticVision.pdf>





#1 Véletlen törlés

Ha töröl egy felhasználót (akár szándékosan, akár nem) a törlés a hálózaton is átfut a OneDrive vállalati postafiók törlésével együtt.

A Microsoft 365-ben lévő natív tárolók és verzióelőzmények, csak korlátozottan képesek megvédeni Önt az adatvesztéstől, ami a megfelelő biztonsági mentésből történő egyszerű helyreállítást komoly problémává változtatja, miután a Microsoft 365 georedundás módon örökre törölte az adatokat vagy a megőrzési időszak lejárt.

A Microsoft 365 platformon kétféle törlés létezik: helyreállítható törlés és végleges törlés.

A helyreállítható törlés példája a 'Törölt elemek' mappa ürítése. „Véglegesen törölt”-nek is nevezik. Ebben az esetben a végleges azonban nem jelent teljesen végleges állapotot, mivel továbbra is megtalálható a "Viszaállítható elemek" mappában.

Végleges törlés esetén az elem teljesen törlődik az adatbázisból. Ha ez megtörténik, az helyrehozhatatlan.



#2 Adatmegőrzési házirend hiányosságai és rendezetlenség

Digitális korunk felgyorsult üzleti élete folyamatosan fejlődő szabályzatokat igényel, beleértve az adatmegőrzési házirendet is, amellyel nehéz lépést tartani és kezelni.

A Microsoft 365 korlátozott biztonsági mentési és megőrzési házirenddel rendelkezik, amely csak bizonyos szituációkban képes védelmet nyújtani, nem célja, hogy mindenre kiterjedő mentési megoldásként funkcionáljon.

Az adathelyreállítás egy másik típusa, az időpont-hoz kötött Point-in-time visszaállítás nem tartozik a Microsoft hatáskörébe. Probléma esetén egy biztonsági mentési megoldás lehetővé teheti a probléma előtti időponthoz való visszatérést.

A Microsoft 365 biztonsági mentési megoldással nincs adatmegőrzési házirend hiányosság vagy rugalmatlan helyreállítás. Legyen szó rövid távú biztonsági mentésről vagy hosszú távú archiválásról, felhasználói csoportonkénti vagy időponthoz kötött visszaállításról. Minden kéznél van, így az adatok helyreállítása gyors, egyszerű és megbízható.





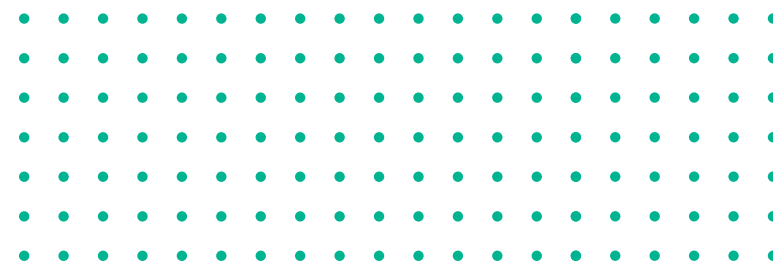
#3 Belső biztonsági fenyegetés

A biztonsági fenyegetés gondolata a hackereket és a vírusokat juttatja eszünkbe. A vállalkozások azonban belülről tapasztalják leggyakrabban ezt, hiszen legtöbbször saját alkalmazottaik szándékos és nem szándékos tevékenységének esnek áldozatául. A fájlokhoz és a kapcsolati adatokhoz való hozzáférés gyorsan változhat, néha problémát okozhat szemmel tartani azokat, akikben megbízunk. A Microsoft nem tud különbséget tenni normál felhasználó és felmondott alkalmazott között, aki távozása előtt megpróbálja törölni a kritikus vállalati adatokat. Ezenkívül egyes felhasználók tudtukon kívül is komoly fenyegetést jelenthetnek fertőzött fájlok letöltésével vagy felhasználóneveik és jelszavaik véletlen kiszivárogtatásával, melyeket olyan webhelyen használnak, amelyeket megbízhatónak gondolnak. Egy másik példa a bizonyítékok manipulálása. Például amikor egy alkalmazott törli a terhelő e-maileket, fájlokat, eltitkolja a jogi, minőségbiztosítási vagy HR részleg elől.



#4 Külső biztonsági fenyegetés

A rosszindulatú programok és a vírusok - például a zsarolóprogramok - világszerte komoly károkat okoznak a szervezetek számára. Ilyenkor azonban nem csak a vállalat hírneve van veszélyben, hanem a belső és az ügyfél adatok védelme és biztonsága is. A külső fenyegetések általában e-mailbe csatolt mellékleteken keresztül jutnak a rendszerbe és nem mindig elegendő felvilágosítani a felhasználókat arról, hogy mire kell figyelniük – különösen, ha a fertőzött üzenetek nagyon meggyőzőek. Az Exchange Online korlátozott biztonsági mentési/helyreállítási funkciói nem megfelelőek a súlyos támadások kezelésére. A rendszeres biztonsági mentések segítenek az adatok fertőzés mentes másolatának tárolásában és az adatok gyors helyreállításában.





#5 Jogi és megfelelőségi követelmények

Néha hirtelen hozzá kell férnie az e-mailekhez, fájlokhoz vagy más típusú adatokhoz jogi eljárások során. Olyan dolgok történhetnek meg velünk, amire korábban sosem gondoltunk volna. A Microsoft számos biztonsági "hálót" épített be a várható vitás ügyekkel/perekkel kapcsolatos dokumentumok megsemmisítésének elhalasztására vonatkozóan. De ezek nem kellően erős mentési megoldások, amelyek meggátolnák, hogy azt, hogy jogi problémáink megoldódjanak. Például egy biztonsági mentési megoldással, ha véletlenül törli az e-maileket vagy dokumentumokat, mielőtt törvényes visszatartást alkalmazna, továbbra is visszakaphatja azokat, így biztosítva a jogi kötelezettségek teljesítését. A jogi és megfelelőségi követelmények, valamint hozzáférési előírások iparáganként és országokként eltérőek, ugyanakkor de a pénzbírság, büntetés és jogi viták három olyan dolog, amit jobb elkerülni.

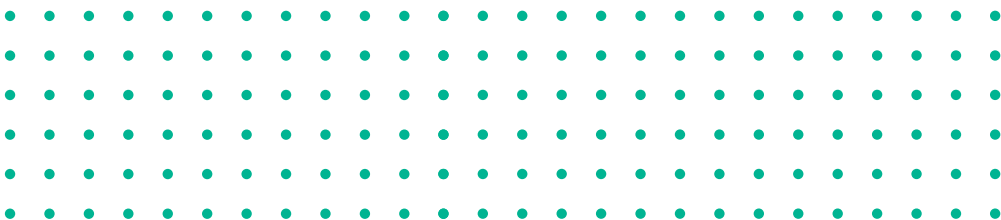


#6 A hibrid e-mail- telepítése és migrációja Microsoft 365-be

A Microsoft 365-öt alkalmazó szervezeteknek időre van szükségük ahhoz, hogy átmenetet biztosítsanak a helyszíni Exchange és a Microsoft 365 Exchange Online között. Néhányan a régi rendszer egy kis részét is fenntartják a nagyobb rugalmasság és további felügyelet biztosításának érdekében. Ezen hibrid e-mail telepítések gyakoriak, de további felügyeleti kihívásokat jelentenek.

A megfelelő Microsoft 365 biztonsági mentési megoldásnak kezelnie kell a hibrid e-mail-telepítéseket és az Exchange adatokat, úgy, hogy a forrás helye irreleváns.

Ezenkívül bárhol képesnek kell lennie az adatok tárolására Ön választásának megfelelően, akár a helyszínen, akár felhőobjektum-tárolásban, mint pl. AWS S3 vagy Azure Blob formájában, vagy külső szolgáltatóval.





#7 Teams adatszerkezet

A Microsoft Teams gyorsan elterjedt és a távmunka térnyerésével egyre nagyobb szerepet tölt be. Jelenleg ez a termelékenységi univerzumunk középpontja. A Microsoft a Teamst felhasználói felületként azonosítja, amely olyan Microsoft 365 szolgáltatásokat egyesíti, mint a SharePoint Online és a OneDrive Vállalati verzió. Ez a megközelítés gyors, valós idejű kommunikációt és együttműködést tesz lehetővé a csoportok számára.

Meg kell védenie adatait ezeken a helyeken, de ez nem minden. A Teams konfigurációs beállításokkal és felhasználókkal rendelkezik, amelyeket védeni kell és szükség esetén visszaállíthatónak kell lenniük. Egy erre a célra kialakított biztonsági mentési megoldás nemcsak az adatokat, hanem a beállításokat és a kapcsolódó alkalmazások közötti kapcsolatokat is megvédheti.

Napjainkban egyre többször jönnek létre Teams csoportok projektekhez és egyéb alkalmakra. A projekt befejezése után megesik, hogy hosszútávon is meg kell őrizni a projektmunka másolatát, például jogi és megfelelőségi szempontok miatt. Azonban gyakran előfordul, hogy ezeket a csoportokat tévedésből törlik, vagy helytelenül alkalmazzák az adatmegőrzést, melyből adódóan a fájlok vagy alapvető dokumentumok nem érhetők el.

A biztonsági mentések egyszeri alkalmak esetén is hasznosak. Például, ha egy alkalmazott valami nem helyénvalót közöl egy Teams-beszélgetés során, de törli az üzenetet, a biztonsági mentéssel a beszélgetés helyreállítható és elérhetővé válik egy esetleges HR felülvizsgálat számára. A külső szállítóktól származó biztonsági mentések nem csak védelmet nyújtanak az ismeretlennel szemben, hanem számos módot kínálnak a hiányzó vagy véletlenül törölt csoportok vagy csatornák visszaállítására.

Milyen gyakran találkozunk velük?

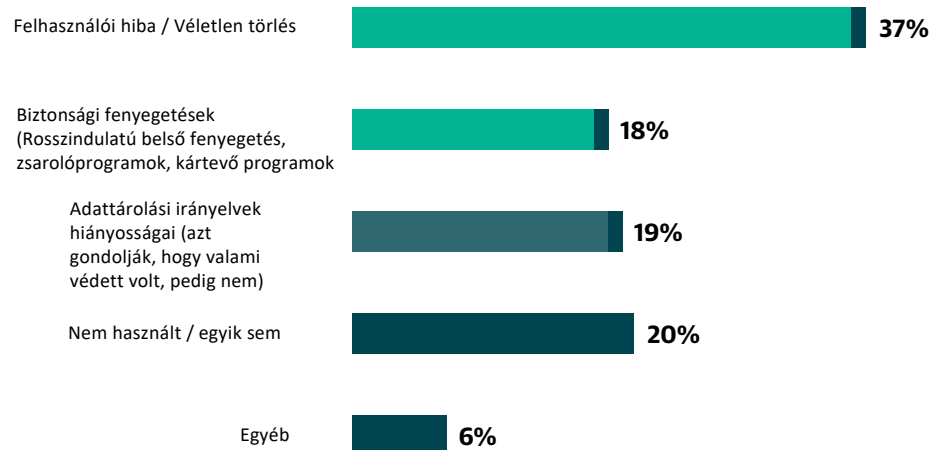
Mostanra már biztosan érti, hogy miért rendkívül fontos biztonsági másolatot készíteni Microsoft 365 adatairól, de valószínűleg kíváncsi, hogy ez a 7 adatvédelmi sérülékenységi tényező valójában milyen gyakran történik meg. A válasz sajnos az, hogy túl gyakran. Több mint 1000 informatikai szakembert kérdeztek meg arról, hogy milyen formában tapasztaltak adatvesztést a felhőben. A felhasználói hibák / véletlen törlés, a biztonsági fenyegetések és adatmegőrzési hiányosságok mind felkerültek a listára.¹ Az ijesztő valóság az, hogy bár bizalmas felhőadatokat tárolnak Office- dokumentumokban, becslések szerint azok 76%-áról nem készül biztonsági másolat². Az IDC szerint 10 vállalkozásból 6 nem rendelkezik adatvédelmi tervvel a Microsoft 365 adatait illetően. Ön is ezen védtelen szervezetek valamelyikében dolgozik?

Ha igen, akkor remélhetően ezen tájékoztató anyag révén már rendelkezésére állnak azon információk, melyek arra ösztönzik vállalkozását, hogy megvédje Microsoft 365 adatait.

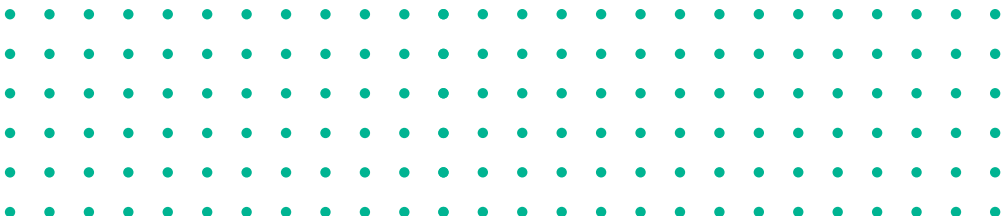
² – Veeam customer survey, September 2019

³ – [IDC: Why a Backup Strategy for Microsoft Microsoft 365 is Essential, 2019](#)

Q14. Milyen adatvesztési formákat tapasztalt a felhőben?



Válaszadók = 1579



Összefoglaló

Vizsgálja meg közelebbről. Lehetnek biztonsági részek, melyekről korábban talán nem is tudott?

Ön már hozott egy okos üzleti döntést a Microsoft 365 üzembe helyezésével, most találjon olyan biztonsági mentési megoldást, amely teljes hozzáférést és teljes ellenőrzést kínál Microsoft 365 adatai számára, és elkerülheti az adatvesztés szükségtelen kockázatát.

Ha hasznosnak találta ezt az anyagot, akkor küldje el kollégáinak e-mailben. [Forward this report](#)

Veeam Backup *for Microsoft 365*

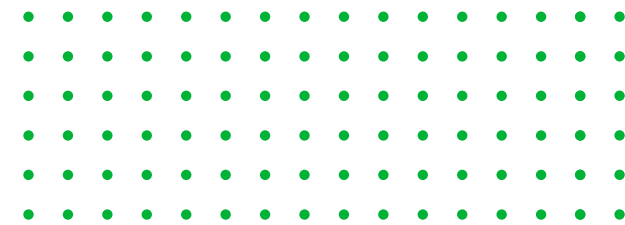


Ingyenes próbeverzió letöltése

<https://go.veeam.com/backup-office-365>

The Veeam logo consists of the word "veeam" in white lowercase letters on a green square background.

Gold
Microsoft Partner



#1 Microsoft 365 Backup

Több irányítás. Könnyed helyreállítás.

Az új Veeam® Backup for Microsoft 365 v6 Self-Service Restore Portal funkciója lehetővé teszi a rendszergazdák számára a biztonságos adatvisszaállítást, továbbá biztonsági másolatot is tartalmaz az **Amazon S3 Glacier**hez, a **Glacier Deep Archive**-hoz és az **Azure Archívum**hoz.

A Veeam Backup for Microsoft365 verziója

- **Automatizálást és méretezhetőséget** nyújt vállalatok számára
- **Időmegtakarítást** biztosít a visszaállítások kezelésével
- **Fokozott biztonságot** kínál a több szintű felhasználói azonosítással (MFA)
- **Biztonságot** szolgáltat az alacsony költségű objektum tárolással

Kezdje egy 30-napos INGYEN verzióval!



Az Ön Veeam Gold Partnere:



Nádor Rendszerház Kft.
1152 Budapest, Telek u. 7-9.
Telefon: +36 1 470-5000
E-mail: info@nador.hu
Web: www.nador.hu

