Microsoft 365

Beépített biztonság az ügyfelek bizalmának megőrzéséért

A biztonságra értékként tekintő vállalati kultúra kialakítása ágazattól és cégmérettől függetlenül fontos feladat. Ám ha a legtöbb kis- és középvállalathoz hasonlóan cége nem rendelkezik saját IT-biztonsági csapattal, akkor nehézségeket okozhat az egyes technológiák biztonsági szolgáltatásainak és az Önre háruló feladatoknak a megértése, nem beszélve a megfelelő biztonsági megoldás kiválasztásáról.

A biztonság megteremtéséhez kapcsolódó feladatok listája hosszú:

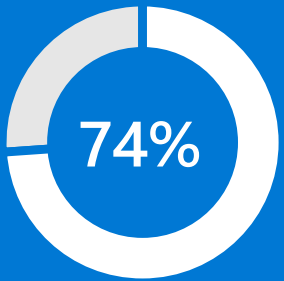
- Át kell gondolni, hogy a már meglévő irányelvek, technológiák és emberek képesek-e a szervezet, illetve az ügyfelek biztonsági igényeinek veszélyeztetése nélkül gondoskodni a zökkenőmentes kommunikációról és együttműködésről.
- Az adatbiztonsági szabályzatnak egyértelműen bizonyítania kell az ügyfelek számára a cég adatbiztonsággal kapcsolatos elkötelezettségét, különösen az alkalmazottak, beszállítók, partnerek, eszközök, adatok és szoftvermegoldások terén bekövetkező változások esetén.
- Meg kell ismerni a cég által a kommunikációhoz és együttműködéshez használt megoldások biztonsági képességeit.
- A biztonság kiemelten fontos a bizalmas dokumentumokkal végzett munka során, de a fájltároló rendszer túlzott összetettsége fokozottan növeli a kockázatot és csökkenti a csapat hatékonyságát.

Miután az összes fenti pontot ellenőrizte, gondoskodnia kell róla, hogy a biztonsági intézkedések a vállalattal és a folyamatokkal együtt fejlődhessenek.

Szerencsére már elérhetőek beépített biztonsági képességeket kínáló együttműködési eszközök, mint például a Microsoft 365.

Számos kisvállalat tulajdonosával beszélgettem, és sokuk azt mondja: »Túl kicsik vagyunk mi egy hackernek.« A valóság azonban az, hogy mérettől függetlenül minden vállalkozás célpont lehet, akár egy ötfős startupról, egy 50 fős kisvállalatról vagy egy 500 munkatársat foglalkoztató globális vállalatról van szó."

William Peteroy
technológiai igazgató
Gigamon



A kkv-tulajdonosok 74%-a úgy gondolja, nem valószínű, hogy biztonsági támadás érné cégüket – ezzel szemben az adatbiztonsági incidensek 43%-a a kisvállalatokat érinti.[1]

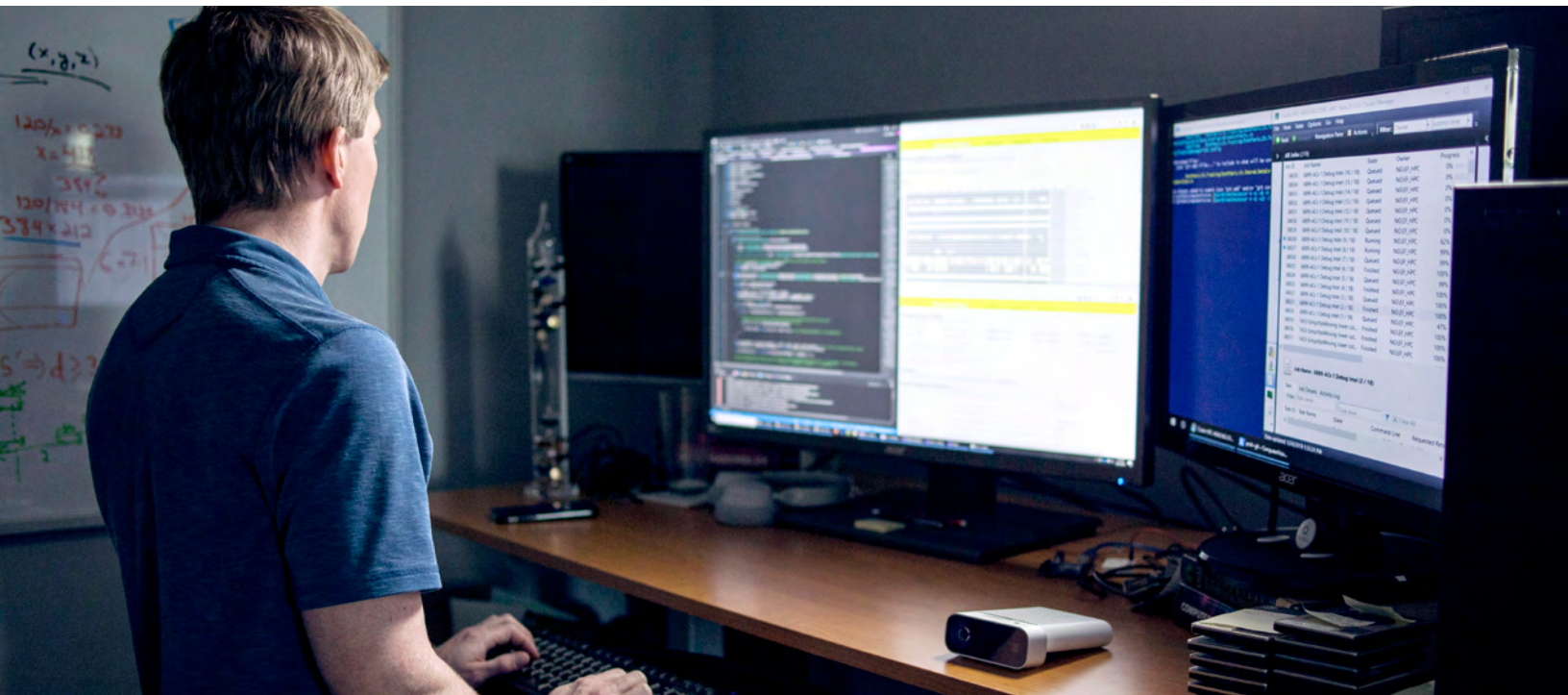
[1] „A biztonság állapota a kis- és középvállalatoknál", Microsoft, 2019.

Biztonsági tippek és eszközök

A Forrester felmérése alapján ha minden anyagot egy helyen, a felhőben tárol a Microsoft 365 részét képező Microsoft Teamsben, ezzel 14,6%-kal csökkentheti a csapatai állásidejét, és hatékonyabban gondoskodhat a biztonságról és a megfelelőségről.[2]

A Microsoft 365 néhány, adatbiztonsággal és -megosztással kapcsolatos bevált módszer, irányelv és engedély ötvözésével megfelelő támogatást nyújthat a munkatársaknak a hatékony együttműködésben és az ügyfeleknek történő értékteremtésben. Az ügyfelek adatainak védelme kiemelten fontos a bizalmuk elnyerésében és megőrzésében. Ez nemcsak szükségszerű az üzleti vezetők számára, hanem potenciális versenyelőnyt is jelenthet másokkal szemben.

[2] „The Total Economic Impact™ of Microsoft Teams", Forrester, 2019.



A kaliforniai Santa Clarában található, hálózati és biztonsági technológiákkal foglalkozó Gigamon számára az intelligens és átfogó biztonsági megoldások a cég működési céljainak és termékkínálatának szerves részét képezik. William Peteroy, a Gigamon műszaki igazgatója és kiberbiztonsági szakértője az alábbi négy lépést javasolja cége és az ügyfelek adatainak biztonságos kezeléséhez:

A támadások kockázatának csökkentése érdekében többfaktoros hitelesítést kell alkalmazni minden lehetséges felhasználó és fiók esetén.

Minden, a rendszerekhez hozzáféréssel rendelkező felhasználóra és eszközre szabályzatokat és engedélyeket kell alkalmazni, beleértve a szerződéses partnereket is, főleg, ha csak ideiglenes hozzáférést kapnak.

Meg kell vizsgálni az alkalmazni kívánt felhőszolgáltató biztonsági szolgáltatásait, illetve egyeztetni kell a szolgáltató és cége biztonsággal kapcsolatos felelősségeit és teendőit.

Ha engedélyezett a munkatársak számára a saját eszközök (pl. mobiltelefonok) használata, akkor ki kell dolgozni az ilyen eszközök adatokhoz való hozzáférését felügyelő szabályzatot. Nyilván kell tartani minden, a rendszerek eléréséhez használt eszközt, és hozzáférés-szabályozási szoftvert kell telepíteni a biztonsági szabályzatnak való megfelelés érdekében.

A Microsoft Security Assessment segítségével gyorsan felmérheti, hogy cége megfelelő védelemmel rendelkezik-e a kiberbiztonsági fenyegetésekkel szemben, illetve javaslatokat kaphat a biztonsági helyzet javításához.

További útmutatók a sorozatból

Az együttműködés támogatásával cége előreléphet >

Modernizált kommunikáció és folyamatok >

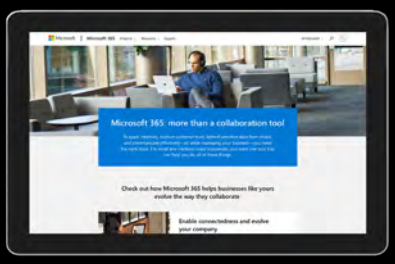
Az innováció ösztönzése a munkatársak összekapcsolásával >

A biztonság fokozása a Microsoft 365 segítségével

Ha a hatékony együttműködési eszközöket szigorú adatbiztonsági gyakorlatokkal ötvözi, az eredmény lenyűgöző lesz. Csökkentheti a kockázatokat, nagyobb értéket teremthet, fokozhatja az ügyfelek bizalmát, és növelheti az esélyét annak, hogy vállalkozása sikertörténetet írjon.

Cége fejlődése során számos kiberbiztonsági fenyegetéssel kell szembenéznie, ám ezeket könnyedén elháríthatja, ha a biztonságot helyezi az együttműködés középpontjába. Tudja meg, hogyan valósíthatja meg mindezt, és hogyan gondoskodhat a vállalati és ügyféladatok nagyobb biztonságáról.

Kapcsolatfelvétel



További információ a Microsoft 365 együttműködési megoldásairól ›