Microsoft

Kiberbiztonsági eshetőségek és megoldások egyszerűen

Bevezetés

Az utóbbi években az információbiztonság az egyik legfelkapottabb téma lett az informatikában. A hacker- és vírustámadások növekvő száma, illetve a nagy port kavaró adatvesztési történetek az informatikai ágazat figyelmét is felkeltették.

A vállalkozások vezetői gyakran nincsenek tisztában az információbiztonság kérdéseivel, a kockázatokkal és az aktuális fenyegetésekkel. Sokszor legfeljebb arról a két-három fenyegetésről van tudomásuk, amelyet ők maguk általában véve aggasztónak találnak, és nem is akarnak az IT apró részleteivel bajlódni. A költségvetés-jóváhagyásakor az a fontos számukra, hogy az új szoftverekbe történő befektetések ár-érték aránya optimális legyen, és hogy ezek pozitív hatást gyakoroljanak az üzletmenetre.

Ebből az e-könyvből ötleteket meríthet ahhoz, hogyan szólítsa meg az üzleti döntéshozókat a saját nyelvükön, vagyis az üzlet nyelvén. A kézikönyv bemutatja, hogyan lehet csökkenteni az üzleti fenyegetések kockázatait, és hogyan lehet megelőzni a hacker- és vírustámadások okozta katasztrófákat a Microsoft megoldásai, például a Microsoft 365 és a Microsoft Azure segítségével.

E-könyvünk a 2018-as változat frissített kiadása, amelyben az új technológiák és kihívások is helyet kaptak.

Az e-könyv használata

Ebben az e-könyvben példákat mutatunk be a különféle támadástípusokra és az ellenük alkalmazandó védelmi intézkedésekre. A leírások műszaki nyelven és a döntéshozók által érthető nyelven is megtalálhatók.

Az információbiztonsági témájú beszélgetések megközelítése

Az információbiztonsági döntéshozókkal folytatott beszélgetéseknek van néhány sajátossága. Az emberek általában nem nagyon törődnek a biztonsággal, amíg „minden rendben van". Azok a vállalatok, amelyek már elszenvedtek jelentős adatvesztést valamilyen zsarolóvírus miatt, sokkal nagyobb figyelmet szentelnek a biztonságnak, mint azok, akik még nem szembesültek ilyen problémákkal. Ugyanakkor az is igaz, hogy nem létezik 100%-os biztonság. Amíg egy rendszer működik, addig ki van téve a kockázatoknak. A mi feladatunk, hogy bemutassuk, hogy a kockázatok léteznek, és olyan megoldást kínáljunk, amellyel elfogadható szintre lehet csökkenteni őket. Mivel a kockázatcsökkentés szoftverek vásárlásával jár, olyan egyensúlyi helyzetre kell törekedni, ahol kifizetődőbb fizetni a biztonságért, mint megfizetni annak hiányáért.

A legnagyobb információbiztonsági kihívások a kis- és középvállalkozások számára

01 **Az emberek jelentik a leggyengébb láncszemet.**
Gyakran nincsenek tisztában az általuk kezelt információk értékével, és nem ügyelnek eléggé az adatok védelmére.

A távmunkára való átállással pedig még rosszabb lett a helyzet, több okból is: az otthoni eszközök kevésbé biztonságosak, mint a vállalatiak, a felhasználók korlátlanul hozzáférhetnek az eszközökhöz, és nincs szükség a Wi-Fi-jelszó feltörésére, mert bárki egyszerűen megkérdezheti azt.

02 **Számos eszköz áll rendelkezésre.**
Manapság viszonylag könnyű hackerré válni. Ezernyi eszköz érhető el ingyenesen bármelyik kezdő számára. Ezért van napjainkban olyan sok úgynevezett „hacker". Az efféle „hackerek" ugyan nem tudnak bejutni egy jól védett infrastruktúra falai mögé, de azok a vállalatok, amelyek nem törődnek az információbiztonsággal, a kockázati csoportba tartoznak.
A kezdő hackerek eredményesebbé váltak a távmunka elterjedésével.

03 **A mi cégünk olyan kicsi – ki foglalkozna velünk?**
Ez a gondolkodásmód igen gyakori a vállalkozások körében. A kisvállalatokat is érheti célzott támadás, de ami még nagyobb probléma, hogy a hackerek nem válogatnak a célpontok között. Automatizált módon hajtják végre a támadásokat, és bármit célba vesznek, ami támadható. Ha a támadás sikerrel jár, akkor megnézik, mit lehet kezdeni a megszerzett információkkal. Ismerünk olyan eseteket, amikor a hackerek feltört vállalati szerverekről próbáltak meg hozzáférni a kormányhivatalok szervereihez. A vállalatok csak akkor tudták meg, hogy hackertámadás áldozatai lettek, amikor megjelentek a titkosszolgálat emberei, hogy kihallgassák őket, és lefoglalják az eszközeiket.

04 **Elavult technológiák.**
Az elavult technológiákkal az a legnagyobb baj, hogy olyan fenyegetések elleni védekezésre tervezték őket, amelyek a szoftver készítése idején voltak aktuálisak. Minél régebb óta érhető el egy adott szoftver az eredeti formájában, annál több olyan támadás jelenik meg, amely ellen nem nyújt védelmet. Nem minden támadás előzhető meg az elavult technológiák „foltozgatásával".

05 **Kevés információbiztonsági szakember van, az IT-szakértők pedig nem fordítanak kellő figyelmet az információbiztonságra.**
A kis- és középvállalatok nem mindig rendelkeznek információbiztonsági szakemberekkel. Ilyenkor az informatikai munkatársak látják el az információbiztonsági feladatokat. A probléma az, hogy az informatikusok feladata az informatikai szolgáltatások működésének biztosítása, amit a biztonsági kérdések megnehezíthetnek. Például egy körültekintően beállított tűzfal a megbízható alkalmazások működését is akadályozhatja. Ebben az esetben az IT-szakembernek döntenie kell: figyelemmel kíséri az alkalmazás által használt portokat, vagy kikapcsolja a tűzfalat. Az utóbbi egyszerűbb, ezért előfordul, hogy azt választják.

Eshetőségek és megoldások

Veszélyforrás

Az e-mail-jelszavak kitalálhatók, elkérhetők, vagy kinyerhetők a böngésző memóriájából

Megoldás

Microsoft 365: Többfaktoros azonosítás

Az Microsoft 365 beállítása kétfaktos azonosításhoz

Informatikai nyelven

Valószínűleg Ön is tudja, hogy sok felhasználó nem úgy tekint a jelszavakra, mint az illetéktelen hozzáférés elleni védekezés eszközére, hanem mint a rendszergazda „mesterkedésére". Könnyelműen bánnak a jelszavakkal, miközben számonkérik az információbiztonságot az informatikai részlegtől.

A többfaktoros azonosításhoz nem elég a jelszót tudni, a felhasználónak felelősséget is kell vállalnia a személyes eszközeiért. Egyszerűen beállítható az online szolgáltatásokhoz, és megoldást nyújt számos biztonsági problémára.

Használható hozzá telefonhívás, SMS, mobilalkalmazáson keresztüli megerősítés vagy egy mobilalkalmazásban kapott kód beírása, és rugalmas kivételeket is be lehet állítani. Beállítható például, hogy mellőzze a második faktort, ha a felhasználók vállalati IP-címről jelentkeznek be, de az otthonról dolgozóktól követelje meg.

Ha mégis bekövetkezik egy biztonsági incidens, a felelősség teljes mértékben a felhasználókat terheli, mert nem vigyáztak kellőképpen a jelszavaikra és a személyes eszközeikre.

Ügyeljen arra, hogy elnyerje a vezetőség támogatását, ellenkező esetben a többfaktoros azonosítást is csak a rendszergazdák mesterkedésének fogják tartani.

Üzleti nyelven

A jelszó önmagában már nem elég. Az emberek öntapadós cetlikre vagy fájlokba jegyzik fel a jelszavakat, elmondják egymásnak vagy a böngészőben mentik őket. Gyakran nagyon egyszerű jelszót választanak, hogy könnyen meg tudják jegyezni. Ráadásul sokan ugyanazokkal a bejelentkezési adatokkal és jelszavakkal regisztrálnak több webhelyen és fórumon is, amelyek alkalmasint megkérdőjelezhető biztonsági beállításokkal rendelkeznek.

Amikor belép egy internetbankba, a jelszó mellett meg kell adnia egy SMS-ben kapott kódot is. Miért ne kellene ugyanilyen szintű védelem a vállalati dokumentumok esetében?

Magyarázza el a munkatársaknak, hogy az a plusz 15 másodperc, amely ahhoz kell, hogy beírjanak néhány karaktert, igazán elfogadható ár a fontos információk hozzáférésének védelméért cserébe.

Veszélyforrás

Elfelejtett jelszó

Megoldás

Microsoft 365: Felhasználók általi jelszóátállítás

Informatikai nyelven

Minden informatikai csoportnál ugyanúgy kezdődik a nap: sorban jelentkeznek a felhasználók, hogy valaki állítsa át az elfelejtett jelszavukat. Ha a felhasználók maguk is átállíthatják a saját jelszavukat egy alternatív bejelentkezési módszer segítségével, akkor sokkal kevesebb efféle hívás érkezik.

Ön határozhatja meg, hogy milyen módszereket használhatnak a felhasználók a jelszó átállításához. Például: SMS-ben kapott kódot, mobilalkalmazást, biztonsági kérdéseket vagy a személyes e-mail-címüket. Eldöntheti, hogy elég egy opció, vagy kettő kombinációjára legyen szükség.

Ez a szolgáltatás integrálható a helyi Active Directoryval. A rendszer egy percen belül szinkronizálja a felhőben átállított jelszót a helyi Active Directoryval.

Mint minden új megoldásnál, ennél is időt kell hagyni arra, hogy a felhasználók megszokják. Az Ön feladata nemcsak az, hogy bevezesse a jelszóátállítási funkciót, hanem az is, hogy tájékoztassa és megfelelő utasításokkal lássa el a felhasználókat.

Üzleti nyelven

Előfordult már Önnel, hogy elfelejtette a vállalati e-mail-címéhez vagy számítógépéhez tartozó jelszót? Ez az alkalmazottakkal is gyakran megesik.

Ez a kellemetlenségen és az informatikai csoport hívásával elvesztegetett időn kívül biztonsági kockázatokat is jelenthet. Távmunka esetén nehéz ellenőrizni, hogy a hívó valóban az-e, akinek mondja magát.

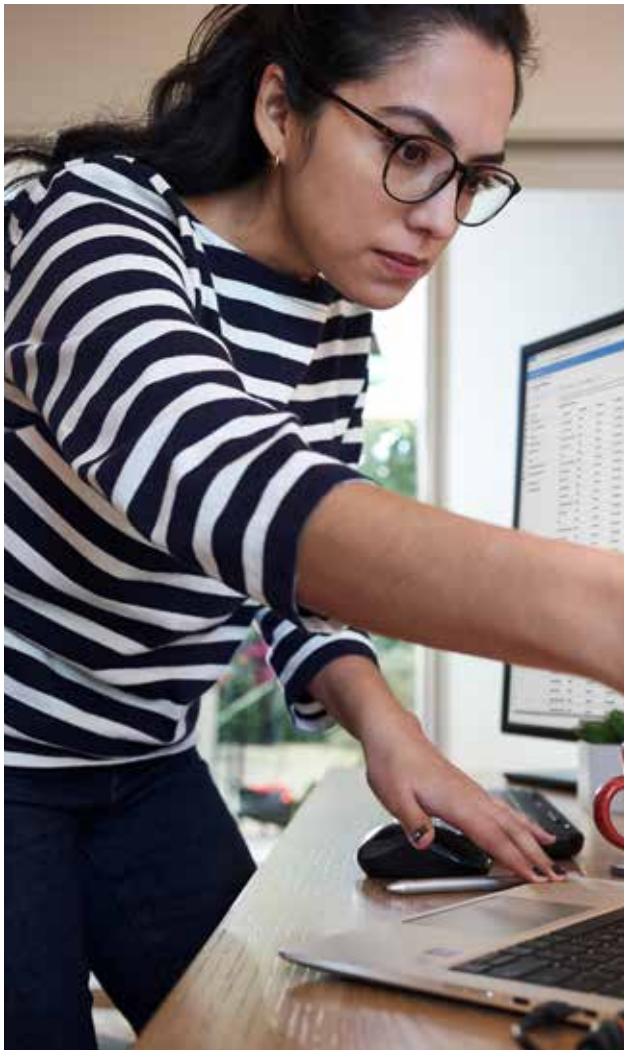
Egyszerű és hatékony megoldást jelentene, ha a felhasználók maguk is átállíthatnák a saját jelszavukat egy SMS-ben vagy mobilalkalmazásban kapott kód, illetve biztonsági kérdések segítségével.

Veszélyforrás

Gyenge jelszavak használata

Megoldás

Microsoft 365: Jelszó nélküli hitelesítés



Informatikai nyelven

Az Azure AD, amely a Microsoft 365-beli hitelesítést is végzi, lehetőséget ad a jelszavak elhagyására. Többféle választási lehetőséget kínál:

01 Regisztrálni lehet egy mobileszközt felhasználói eszközként. A hitelesítés úgy történik, hogy megjelenik egy szám a képernyőn, a Microsoft Authenticator alkalmazás pedig felkínál egy csomó számot, amelyek közül a felhasználó kiválasztja a megfelelőt, és ami még fontosabb, az ujjlenyomatával azonosítja magát a mobileszközön.

02 Hardverkulcs. Ennél a módszernél egy megfelelő hardverkulcsra és néhány adatra van szükség.

03 Biometrikus adatok.

04 Az Azure AD által nem támogatott attribútumok. A helyi AD és az Azure AD összevonásának beállításával még több hitelesítési módszer vehető igénybe. Például intelligens kártya is használható hitelesítésre.

Mindegyik módszernek megvannak a saját jellemzői, követelményei és hatóköre. Tekintse meg a lehetőségeket a következő címen:
https://docs.microsoft.com/hu-hu/azure/active-directory/authentication/concept-authentication-passwordless

A legtöbb vállalatnál még csak kezdeti fázisban van a jelszó nélküli hitelesítésre való áttérés, ezért ez a megoldás még elég szokatlan. A jelszó nélküli hitelesítésre való áttérést fokozatosan célszerű megvalósítani, és amíg be nem fejeződik, nem szabad elhanyagolni a jelszavas védelmet.

Üzleti nyelven

Képzelje el a következő helyzetek valamelyikét:

01 Egy vagy több munkatársa kap egy Word- vagy PDF-formátumú e-mailt az egyik partnercégtől. A dokumentum megnyitásakor megjelenik egy halom titkosított szöveg és a következő üzenet: „Ez a dokumentum személyes adatokat tartalmaz, ezért a jogszabályi megfelelőség érdekében titkosítva van. A titkosítás feloldásához adja meg az e-mail-címét és a jelszavát."

02 A könyvelési osztály egyik munkatársa üzenetet kap az adóhatóságtól egy adókötelezettséggel kapcsolatban. Az üzenet egy hivatkozást is tartalmaz, amelyen keresztül megtekintheti a részleteket. Amikor rákattint a hivatkozásra, a megjelenő üzenet arra kéri, hogy adja meg az e-mail-címét és a jelszavát.

Mindkét példában egy-egy adathalász kísérlet szerepel, amelynek célja, hogy megszerezzék a munkatársak jelszavait.

A jelszó az egyik leggyengébb láncszem, amit egy napon muszáj lesz kiiktatni.

Hogyan oldja fel a mobileszközét? Talán ujjlenyomat-azonosítással. Ez az egyik jelszó nélküli hitelesítési módszer, ami mára már megszokottá vált a mobileszközök révén. Biztonságosabb, mivel nagyon nehezen használható a tulajdonos fizikai jelenléte nélkül, és kényelmesebb, mert nem kell rendszeresen megváltoztatni.

Ma már a vállalati rendszerekben is kezdik bevezetni ezt a módszert, hogy biztosítsák azt a biztonságot és kényelmet, ami a mobileszközökön már megszokottá vált. Ha egy munkatársnak megjelenik egy ablak, amelyben a jelszavát kérik, azonnal gyanút fog majd, hiszen a vállalat egyáltalán nem használ jelszavakat.

Veszélyforrás

Nem biztonságos jelszavak használata

Megoldás

Microsoft 365: Jelszavas védelem

Informatikai nyelven

Ki lehet zárni azokat a szavakat, amelyeket nem célszerű jelszónak használni, például a vállalat nevét. Ezzel nemcsak az adott szót tiltja le, hanem az abból képzett kifejezéseket is.

További információ:
https://docs.microsoft.com/hu-hu/Azure/active-directory/authentication/concept-password-ban-bad

Ez a funkció a felhőbeli fiókok esetén használható, és integrálható a helyi Active Directoryval.

Üzleti nyelven

Milyen szavakkal próbálkozik egy hacker, amikor megpróbálja kitalálni a jelszót? Jó eséllyel olyanokkal, amelyek valahogyan kapcsolódnak az illető vezeték- és keresztnevéhez, illetve a vállalat nevéhez.

A munkatársak nem használhatnak könnyen kitalálható szavakat jelszóként. Az ilyen szavak listáját a vállalata informatikai részlegének kell összeállítania.

Veszélyforrás

Jogosulatlan hozzáférés nem megbízható helyekről

Megoldás

Microsoft 365: A hozzáférés korlátozása helymeghatározás segítségével

Informatikai nyelven

Az Azure AD egyik legfontosabb szolgáltatása a Feltételes hozzáférés. Ennek segítségével engedélyezheti a többfaktoros azonosítást, kötelezheti a felhasználókat a jelszavuk módosítására, megakadályozhatja, hogy bejelentkezzenek a személyes eszközeikről stb.

Az egyik kulcsfontosságú beállítás a nem megbízható helyekről történő bejelentkezések korlátozása.

Összeállíthat különböző helylistákat nyilvános IP-címekből vagy az azoknak megfelelő földrajzi helyekből. Ezek engedélyezési vagy tiltólisták lehetnek.

Üzleti nyelven

Talán hallott már arról, hogy a hackerek elrejtik a földrajzi helyüket, hogy ismeretlenek maradjanak. Előfordulhat, hogy az illető a szomszédban van, de látszólag egy idegen országból próbál csatlakozni.

Több mint 200 ország van a világon. Miért engedné, hogy minden létező országból hozzáférjenek az Ön adataihoz?

Ezt megoldhatja úgy, hogy csak bizonyos országokból engedélyezi a hozzáférést, amelyek listáját a vállalata informatikai részlege állítja össze.

Veszélyforrás

Szabályozási követelményeknek való megfelelés

Megoldás

Microsoft 365: Tárolási házirendek

Informatikai nyelven

A hatóságok évről évre szigorúbb követelményeket írnak elő az adatok tárolására vonatkozóan. Szaporodnak az olyan nemzetközi előírások is, mint az európai uniós adatvédelmi rendelet, a GDPR. Az ezeknek való megfelelés biztosításához bürokratikus és technikai intézkedésekre egyaránt szükség van.

A megfelelőség egy összetett folyamat eredményeként érhető el, amely meghaladja a jelen útmutató kereteit, illetve az informatikai részleg kompetenciáját.

Mindazonáltal van egy fontos követelmény, amely szinte minden vállalatra érvényes, mégpedig az információk védelme a véletlen vagy éppen szándékos törléssel szemben.

A tárolási házirendek segítségével:

01 Garantálható a dokumentumok megőrzése a megadott ideig.

02 Automatikusan törölhetők a dokumentumok egy bizonyos idő elteltével.

03 Az előírt idő elteltével a rendszer értesíthető az a személy, akinek döntenie kell a dokumentum törléséről vagy további tárolásáról.

Üzleti nyelven

Előfordulhat, hogy törlik vagy módosítják a fontos dokumentumokat.

Ilyenkor nemcsak fontos információk veszhetnek el, de az is megtörténhet, hogy a szabályozó hatóságok megbírságolják a vállalatot.

Az informatikai részleg egy ideig tárolja a dokumentumok másolatait a gyors helyreállíthatóság érdekében, de mi van akkor, ha a kérdéses dokumentum 3 éve keletkezett? Vannak olyan dokumentumok, amelyeket a jogszabályok szerint több évig meg kell őrizni.

A tárolási házirendek védik a fontos dokumentumokat, e-maileket vagy akár a csevegéseket is a véletlen vagy szándékos törléstől a megadott ideig.

Veszélyforrás

Rosszindulatú e-mail-mellékletek

Megoldás

Microsoft 365: Biztonságos mellékletek

Az Office 365 ATP Biztonságos mellékletek szolgáltatáshoz használt profil és konfiguráció

Informatikai nyelven

A rendszer minden mellékletet lefuttat a Microsoft-adatközpont saját hardveres tesztkörnyezetében, és amíg nem ellenőrzi, hogy a melléklet biztonságos, addig nem kézbesíti a felhasználónak. A rendszer elemzi a melléklet viselkedését.

A rendszergazda igény szerint megkaphatja a melléklettel rendelkező eredeti e-mailek egy példányát.

Üzleti nyelven

Képzeljen el két helyzetet, amelyekben megnyit egy e-mail-mellékletben kapott dokumentumot, és az:

01 Egyszerűen megnyílik.

02 Lefuttat egy makrót, amely adatokat továbbít a laptopjáról, vagy titkosít más dokumentumokat.

Kívülről egyformának tűnhet a két dokumentum, azonban másképp viselkednek.

A Microsoft e-mail szolgáltatása ellenőrzi a dokumentum viselkedését, mielőtt az e-mail eljutna a felhasználó postaládájába. Ha a dokumentum a fenti második esethez hasonlóan viselkedik, akkor a rendszer a melléklet nélkül kézbesíti az e-mailt.

A zsarolóvírusok nem hatolhatnak be a vállalat levelezőrendszerén keresztül. Az emberekkel ellentétben a rendszert nem tévesztik meg a tetszetős e-mailek, és azonnal törli őket.

Veszélyforrás

E-mailben kapott rosszindulatú hivatkozások

Megoldás

Microsoft 365: Biztonságos hivatkozások

Az Office 365 ATP Biztonságos hivatkozások szolgáltatás bemutatása és konfigurációja

Informatikai nyelven

Minden alkalommal, amikor a felhasználó rákattint egy hivatkozásra egy e-mailben vagy egy Office-dokumentumban, a rendszer ellenőrzést végez. Ha a hivatkozás rosszindulatú webhelyre mutat, a rendszer blokkolja.

A rendszergazda manuálisan is felvehet webhelyeket a rosszindulatú webhelyek listájára.

Üzleti nyelven

A mai hackerek jól értenek a marketinghez.

Tetszetős e-maileket küldenek, valósághű másolatokat készítenek a bankok webhelyeiről, és az emberek érzelmeire játszanak.

Ha a felhasználó rákattint egy e-mailben kapott hivatkozásra, könnyen elszabadíthat egy vírust, elveszítheti a hozzáférését egy internetbankhoz vagy egy piactérhez stb.

A Microsoft perceken belül értesül az ilyen hivatkozásokról. A vírusos webhelyek vagy hamis banki weboldalak megnyitására tett minden kísérletet letiltunk.

Veszélyforrás

Zsarolóvírus-támadások

Megoldás

Windows 10: Szabályozott mappahozzáférés

A Szabályozott mappahozzáférés beállítása

Informatikai nyelven

A „Szabályozott mappahozzáférés" funkcióval megakadályozhatja, hogy nem megbízható folyamatok írjanak az Ön által meghatározott mappákba. A Fájlkezelőt, a Microsoft Wordöt és a hasonló folyamatokat ez nem érinti, de az ismeretlen folyamatok általi módosításokat a rendszer blokkolja.

Ez a funkció nem működik, ha telepítve van egy más gyártótól származó víruskereső.

Üzleti nyelven

A zsarolóvírusok komoly veszélyt jelentenek, és gyakran megkerülik a víruskeresők által biztosított védelmet. A védett mappákban lévő fájlok akkor is érintetlenek maradnak, ha a rendszert titkosítja a vírus.

Még ha a víruskereső szoftver nem is tudja kezelni a zsarolóvírust, a dokumentumok akkor is tökéletes biztonságban maradnak.

Veszélyforrás

Zsarolóvírus-támadások

Megoldás

Microsoft 365: OneDrive Vállalati verzió

A OneDrive Vállalati verzió beállítása Windows 10 rendszeren

Informatikai nyelven

Ha egy zsarolóvírus bejut a rendszerbe, nemcsak a dokumentumokat, hanem az archívumokat is titkosítja, és az árnyékmásolatokat is törli.

Ha beállítja a Windows 10 rendszerben a dokumentumok szinkronizálását a OneDrive Vállalati verzió felhőtárhelyével, minden adatot helyre fog tudni állítani. A rendszer azonnal szinkronizálja a fájlokat, amint mentésre kerülnek a megadott könyvtárban.

A szinkronizáló klienst a Windows 10 beépítve tartalmazza, a Windows 7-re pedig telepíthető.

A legkisebb rendelkezésre álló tárhely felhasználónként 1 TB.

A beépített verziókövetéssel nemcsak az aktuális, hanem a korábbi fájlverziók is visszaállíthatók.

Üzleti nyelven

Előfordult már, hogy a haját tépte mérgében, mert véletlenül töröltek egy dokumentumot, vagy zsarolóvírus áldozatává vált? Vagy mert törölte egy dokumentum egy részét, és nem volt lehetőség a visszaállításra?

A zsarolóvírusok mellett a felhasználók is törölhetnek fontos adatokat, akár szándékosan, akár véletlenül.

Automatikusan a felhőbe mentheti a fájlok másolatát. A dokumentumok összes korábbi változata is mentésre kerül.

Visszaállíthatja a titkosított, törölt vagy módosított fájlokat, akárhány módosítást végeztek is rajtuk.

Veszélyforrás

Adatok letöltése jelszóvédelem nélküli adathordozóról

Megoldás

Windows 10: BitLocker-titkosítás

A BitLocker dokumentációja

Informatikai nyelven

Ön is tudja, hogy a merevlemez kivehető a számítógépből, és áthelyezhető egy másikba.

A rendszer pedig elindítható DVD-ről is, hozzáférést biztosítva a teljes fáljrendszerhez. Ráadásul egyik esetben sincs szükség a bejelentkezési jelszó megadására.

A cserélhető adathordozók is könnyen elveszhetnek, az ezeken tárolt információk értéke pedig sokszorosan meghaladja az adathordozóét.

Célszerű titkosítani az adathordozókat. Mint minden biztonsági intézkedés, ez is némi kellemetlenséggel és kockázattal jár.

A BitLocker megfelelő beállításával minimalizálni lehet a kockázatokat.

A helyreállítási kulcsok a helyi Active Directoryba vagy az Azure Active Directoryba is menthetők, így az adatok a lemez fizikai sérülése esetén is helyreállíthatók.

A még nagyobb biztonság érdekében érdemes archiválni is az adatokat.

Üzleti nyelven

Az adatvesztés egyik leghétköznapibb módja az, amikor az eszközzel együtt vesznek el az adatok.

Például egy reptéri ellenőrzőponton felejti a laptopját, vagy kiesik a táskájából egy pendrive. Ezek az esetek pedig nemcsak azzal járnak együtt, hogy új eszközöket kell vásárolni, de az adatokhoz való illetéktelen hozzáférés nagyfokú kockázatát is magukban rejtik.

Még ha van is jelszóvédelem a laptopon, az sem fog megakadályozni egy informatikai szakértőt abban, hogy hozzáférjen az adatokhoz. Márpedig gyakran előfordul, hogy a felhasználók a laptopjukon tárolnak egy jelszavakat tartalmazó dokumentumot, vagy a böngészőjükben mentik a jelszavakat.

Titkosítsa a fontos információkat tartalmazó lemezeket és adathordozókat! Az eszköz esetleges elvesztése vagy ellopása ugyan így is bosszúsággal jár, de legalább senki nem férhet hozzá az adatokhoz.

Még ha elvész is egy fontos adatokat tartalmazó számítógép vagy pendrive, akkor sem kell katasztrofális adatszivárgástól tartania. Az adatok biztonságosan titkosítva lesznek, gondosan elzárva a kíváncsi tekintetek elől.

Veszélyforrás

Támadások mobileszközökön

Megoldás

Microsoft Endpoint Manager
(korábbi nevén Microsoft Intune)

A Microsoft Intune dokumentációja

Informatikai nyelven

A Microsoft Intune a felhőből felügyeli az eszközöket, így a felhasználó aktuális tartózkodási helyétől függetlenül elvégezhetők a felügyeleti feladatok.

Az eszközöket kényszerített módon konfigurálni lehet a biztonsági szabályzatok betartására, illetve törölni lehet bizonyos adatokat vagy akár az összes adatot, ha az illető munkaviszonya megszűnik.

Üzleti nyelven

A Symantec végzett egy kísérletet: mobiltelefonokat hagytak nyilvános helyeken az Egyesült Államokban és Kanadában, mintha véletlenül ottfelejtették volna őket. Előzőleg olyan szoftvert telepítettek a telefonokra, amellyel megfigyelhették az eszközökön végzett tevékenységeket.

A megtalálók 60%-a meg sem próbálta visszajuttatni a telefont a tulajdonosának. Néhány órán belül elkezdték böngészni a dokumentumokat és a fényképeket, és megnyitották az alkalmazásokat.

A mobileszközökkel kapcsolatos legnagyobb veszély az, hogy maguk az eszközök személyes tárgyak, ugyanakkor vállalati információkat tartalmazhatnak. A személyes eszközök felügyeleti lehetőségei pedig eléggé korlátozottak.

A felhasználók meglehetősen gondatlanul bánnak az eszközeikkel: nem használnak titkosítást, gyakran még PIN-kódot sem, kétes biztonságú alkalmazásokat telepítenek rájuk, és könnyen elvesztik őket. Előfordulhat az is, hogy a korábbi munkatársak megőriznek archivált üzeneteket vagy ügyfelek elérhetőségeit az okostelefonjukon.

Ha a munkatársak vállalati e-maileket vagy dokumentumokat kezelnek a mobiltelefonjaikon, Önnek meg kell tudnia védeni a vállalati adatokat.

Ha a mobiltelefonokat összekapcsolják a MEM szolgáltatással, biztonságosabb módon lehet konfigurálni őket, és a munkaviszony megszűnésekor a vállalati adatok (vagy akár az összes adat) törölhető róluk.

Az okostelefonra mentett vállalati e-mailek és üzleti dokumentumok nem „távoznak” a volt munkatárssal. Ha pedig az eszköz elvész, vagy ellopják, távolról is törölhetők róla az adatok.

Veszélyforrás

Vírusok

Megoldás

Windows 10: Microsoft Defender AV

Informatikai nyelven

A Windows 10 platform beépített vírusvédelemmel rendelkezik. A korábbi verziókban használt Microsoft Security Essentials víruskereső program meglehetősen egyszerű volt. A Security Essentials utódja, a Microsoft Defender AV valóban radikálisan különbözik az elődjétől.

Elsődleges előnyei a Windows 10-integráció és a Windows 10 új buildjeihez készült folyamatfejlesztések.

Még a független tesztelők is elcsodálkoztak a víruskereső fejlődésének iramán. Meglepetés! A Windows Defender egész jól teljesít a víruskeresők legutóbbi tesztjein https://www.tomsguide.com/us/windows-defender-av-test,news-25524.html

Ez a csoportházirend segítségével szabályozható víruskereső teljes mértékben ingyenes vállalati használat esetén is.

Bizonyos funkciókhoz, például a központi jelentéskészítéshez kereskedelmi forgalomban kapható eszközökre van szükség.

Üzleti nyelven

A víruskereső nem csodaszer. A biztonság mindenképpen folyamatos felügyeletet igényel, de víruskeresőre akkor is szükség van. Ez a víruskereső beépített és ingyenes.

Régebben sokan úgy gondolták, hogy Mac-környezetben biztonságosabb a munka, mint Windowson, mert kevesebb vírus fenyegeti. Ez elsősorban azért van, mert a Windows uralja a piac 88%-át, míg a Mac csak 9 százalékos részesedéssel rendelkezik (https://netmarketshare.com/operating-system-market-share.aspx)

Azok, akik hackerként keresik a kenyerüket, nyilván arra törekszenek, hogy a lehető legnagyobb célközönséget érjék el. Aki a Windows 10-et választja, továbbra is a 88%-os többséghez fog tartozni, de ugyanolyan szintű védelmet élvez, mint a 9%-os szegmens.

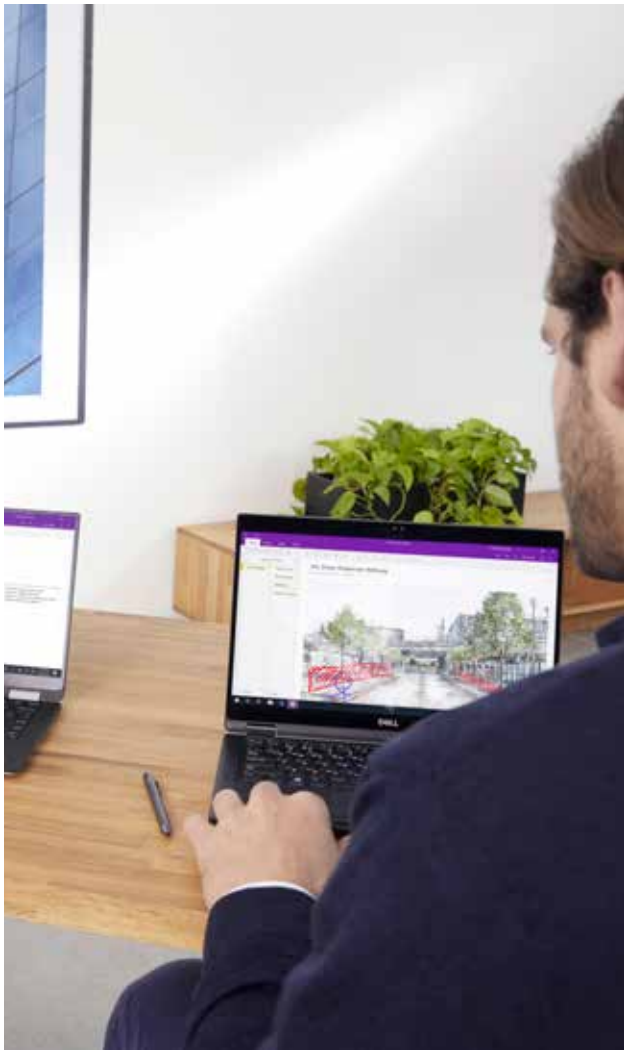
Veszélyforrás

Dokumentumok kiszivárgása

Megoldás

Azure Information Protection

Az Azure Information Protection dokumentációja



Informatikai nyelven

Ez a titkosításon és hozzáférési jogosultságok kiosztásán alapuló dokumentumvédelmi technológia lehetővé teszi a beállított korlátozások fenntartását akkor is, ha a dokumentumok kiszivárognak a szervezeten kívülre.

A technológia segítségével megvédhetők a bizalmas információk a vállalaton belül, illetve megelőzhető az adatok kiszivárgása.

Együttműködik az Office-alkalmazásokkal, így a felhasználók közvetlenül titkosíthatják a fájlokat a Microsoft Wordből és a Microsoft Exchange e-mailekből. Manuálisan és automatikusan is alkalmazható, a megadott szabályoknak megfelelően. Például automatikusan titkosítható a melléklet, ha egy munkatárs elküld egy melléklettel rendelkező e-mailt a vállalaton kívülre vagy bizonyos címekre, illetve bizonyos fájlokkal.

Ez a technológia egyaránt alkalmazható egyszerű dokumentumvédelmi megoldásként és összetettebb feladatokra is, például a dokumentumok szabályozási követelményeknek megfelelő besorolására és azt követő védelmére.

Üzleti nyelven

A védelmet igénylő vállalati adatok értékét tekintve ez a technológia nagyon jó befektetés. Még ha valaki meg is próbálna kijuttatni bizalmas információkat a vállalaton kívülre, akkor sem fogja tudni megnyitni a dokumentumokat.

Ha egy vezető e-mailben próbálna elküldeni egy ügyféladatbázist a versenytársaknak, azok nem tudnák elolvasni ezt az e-mailt, akárhogy is próbálnák.

Végezetül korlátozható a dokumentumokhoz való hozzáférés, hogy a kívülállók ne láthassák a nem nekik szánt információkat.

Veszélyforrás

További információ az adatszivárgásról

Megoldás

Microsoft 365 DLP

Az Microsoft 365 DLP részletes áttekintése

Informatikai nyelven

Bizalmas információk védelmét szolgáló házirendek az Exchange Online-hoz, a SharePoint Online-hoz, a OneDrive Vállalati verzióhoz és a Teamshez.

A házirendek segítségével letilthat bizonyos műveleteket, például hogy bizalmas információkat továbbítsanak a vállalaton kívülre vagy töltsenek le egy helyi számítógépre.

A rendszergazdák értesítést kaphatnak, ha a felhasználók tiltott műveleteket próbálnak végrehajtani.

A rendszer különböző információsablonok alapján képes felismerni a nemzetközi és a belföldi útlevelekben szereplő bizalmas adatokat. Egyéni sablonok is megadhatók kulcsszavak, reguláris kifejezések, a dokumentum elrendezése vagy egyéb, betanítható osztályozók alapján.

Üzleti nyelven

Az állam megköveteli a vállalatoktól a személyes adatok adatszivárgás elleni védelmét.

Mi történne, ha egy munkatárs véletlenül elküldene egy útlevéladatokat tartalmazó e-mailt?

Egy megtörtént eset: a 2015. évi brisbane-i G20-csúcstalálkozó előkészületei során az Ausztráliai Bevándorlási Hivatal egyik munkatársa véletlenül elküldött egy dokumentumot az Ázsia-kupa (ázsiai labdarúgó torna) szervezőinek, amely a G20-as országok vezetőinek (köztük Putyin, Obama, Merkel és Hszi Csin-ping) útlevéladatait tartalmazta. Amikor a munkatárs beírta a kollégája nevét az Outlookban, nem ellenőrizte az automatikus kitöltési funkció által felkínált címet, mielőtt elküldte volna az üzenetet.

A rendszergazda beállíthat egy olyan házirendet, amely letiltja azokat a kimenő e-maileket, amelyek útlevéladatokat vagy más személyes információkat tartalmaznak.

Veszélyforrás

És mi a helyzet az adatszivárgással a Teams esetében?

Megoldás

Microsoft 365 DLP használata a Teamsben

Informatikai nyelven

A DLP szolgáltatás a levelezőrendszer, a SharePoint és a OneDrive Vállalati verzió tárhelyszolgáltatása, továbbá a Microsoft Teams használata esetén is rendelkezésre áll.

A licencelés és az alkalmazási kör tekintetében fontos különbségek vannak.

A Microsoft Teams esetében a házirendek a privát beszélgetések és a csatornák üzeneteire érvényesek.

A Microsoft Teams használatával közzétett dokumentumok a OneDrive Vállalati verzió és a SharePoint tárhelyén találhatók, és ennek megfelelően a OneDrive Vállalati verzió és a SharePoint DLP-házirendjeinek hatálya alá tartoznak.

Üzleti nyelven

A Microsoft Teams népszerűsége és sokoldalúsága miatt sok szempontból előnyös, de néhány új kihívást is felvet. Például:

01 Egy munkatárs meghívja egy partnercég munkatársát az egyik Teams-csatorna használatára, és véletlenül elküld egy bizalmas adatokat tartalmazó üzenetet.

02 Egy munkatárs közzétesz egy bizalmas adatokat tartalmazó dokumentumot az említett Teams-csatornában.

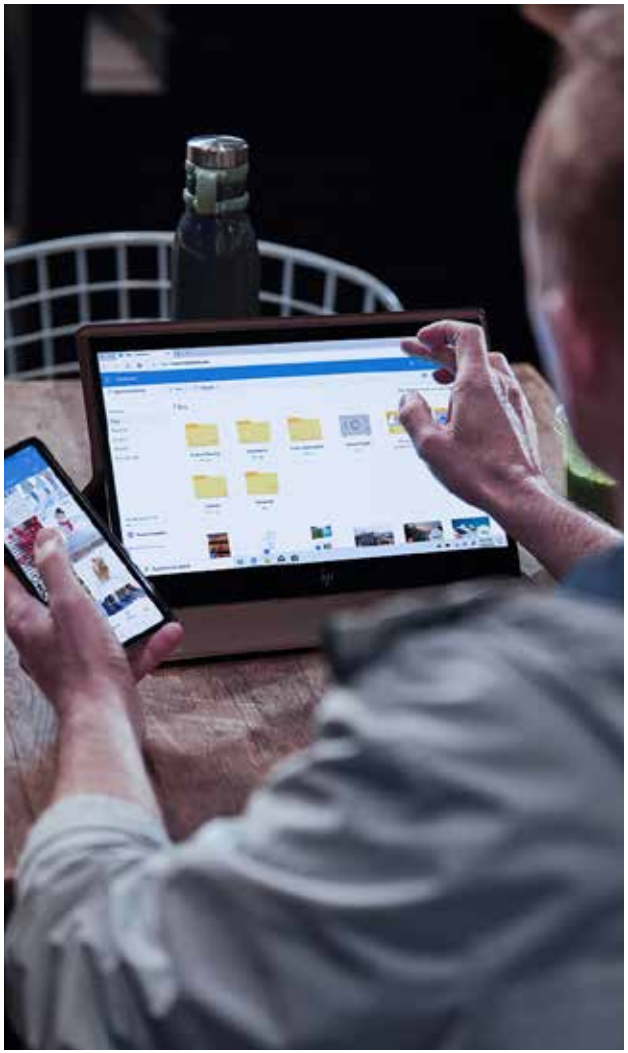
A partnercég munkatársa egyik esetben sem fogja elérni az üzenetet, illetve a dokumentumot, így a bizalmas információk a vállalaton belül maradnak.

Veszélyforrás

További információ az adatszivárgásról és az árnyékinformatikáról

Megoldás

Office 365 Cloud App Security



Informatikai nyelven

A Microsoft Cloud App Security (CAS) a felhőelérési biztonsági közvetítő (CASB) szoftverek családjába tartozik. A Microsoft CAS funkcionalitása olyan széles körű, hogy külön könyvet érdemelne. Van egy „kistestvére" is, az Office 365 CAS, amely csak az Office 365-alkalmazásokért felel.

Az Office 365 CAS segítségével nyomon követhetők a felhasználók tevékenységei az Exchange Online-ban, a SharePoint Online-ban és a OneDrive Vállalati verzióban. Például ki lehet deríteni, melyik munkatárs töltött le egy bizonyos fájlt, hozott létre egy névtelen hivatkozást, törölt egy e-mailt stb.

A szoftver a rendszergazdák tevékenységeit is naplózza, így azokat is nyomon lehet követni.

A házirendek révén értesítést küldhet bizonyos tevékenységekről, vagy akár le is tilthatja őket.

Üzleti nyelven

Képzelje el, hogy egy kilépő munkatárs le szeretne tölteni néhány dokumentumot, amelyek fontosak a vállalatnak (és a versenytársaknak).

Ha időben fény derül a szándékára, akkor meg lehet akadályozni, hogy megtegye. Erre használhatók a házirendek. Például:

01 Egy dolgozó letölt 30 dokumentumot egy percen belül.

02 Egy munkatárs letölt 10, bizalmasként megjelölt dokumentumot.

03 Egy dolgozó létrehoz egy névtelen hivatkozást bizalmas dokumentumok letöltéséhez... És így tovább.

Veszélyforrás

Fizikai biztonság

Megoldás

Adatközpontok használata

Informatikai nyelven

Az infrastruktúra biztonsága több részből tevődik össze, amelyek egyike a fizikai biztonság. A vállalat saját területén található berendezések esetében komoly feladatot jelenthet a fizikai biztonságról való gondoskodás.

Íme néhány megfontolandó szempont:

01 Megfelelő módon kell kiválasztani a szerverszoba helyét. Ügyelni kell például arra, hogy a szerverszoba ne a külső falak mellett legyen, és ne legyen ablaka.

02 Alkalmazni kell egy hőmérséklet- és páratartalom-szabályozó rendszert a meghatározott értékek biztosítása érdekében.

03 Az ajtókat elektronikus zárral kell felszerelni.

04 Az adatközpontban álpadlót kell alkalmazni.

05 Az adatközpontnak rendelkeznie kell tűzoltó rendszerrel.

06 A hardvereket és az adattároló rendszereket titkosítani kell.

07 Gondoskodni kell az épületek átfogó fizikai biztonságáról.

Az adatközpont tulajdonosai már intézkedtek a fentiekről. Biztonsági szempontból az adatok védelme sokkal jobban biztosított egy olyan helyen, ahol teljesül az ehhez szükséges összes feltétel.

Üzleti nyelven

Ha minden adatot a közelben tárol, természetes, hogy nyugodtabbnak érzi magát. Mindazonáltal gondolni kell arra, hogy így bárki, aki engedéllyel vagy illetéktelenül bejut a vállalat területére, szintén megszerezheti az adatokat. Ehhez nem is kell feltétlenül hackernek lenni, elég, ha valaki egyszerűen fogja és elveszi az adott eszközt.

Az adatközpontok rendelkeznek beléptetőrendszerekkel, ellenőrzőpontokkal, 24 órás videós megfigyelőrendszerrel és biztonsági őrökkel. Külső félként hozzáférni az adatokhoz rendkívül nehéz, jóformán lehetetlen, különösen akkor, ha az adatok tárolására szolgáló adatközpont egy másik országban van.

A kisebb cégek általában nem engedhetik meg maguknak, hogy önállóan megvalósítsák ezt a biztonsági szintet, a helyi szerverek védelmét, a beléptetőrendszert és a szervereket felügyelő videós megfigyelő rendszert.

Veszélyforrás

Az adatok archiválása

Megoldás

Az adatközpontban tárolt biztonsági másolat

Az Azure Backup dokumentációja

Informatikai nyelven

A Microsoft Azure biztonsági mentési eszköze alapszintű adatarchiválási és -helyreállítási megoldást nyújt, amely kiegészíti a meglévő archiválási eszközöket.

Még ha egy helyi archívum el is veszne vagy megsérülne, az Azure-adatközpontban tárolt biztonsági másolat a kívánt ideig megőrzésre kerül.

Üzleti nyelven

Az eszközök elromolhatnak, és az adatok – véletlenül vagy szándékosan – törlődhetnek. Ezekben az esetekben segítenek a biztonsági másolatok.

De mi van akkor, ha a másolat is megsemmisül? Ez is előfordulhat egy tűzeset vagy rablás következtében, vagy az adathordozó gondatlan tárolása esetén.

Bizonyára Ön is ismeri a Toy Story – Játékháború 2. című animációs filmet. És azt is hallotta, hogy a felvett anyag nagy része véletlenül megsemmisült, és a gondatlan tárolás miatt az archívumból sem tudták visszaállítani? A filmet pusztán a szerencse mentette meg, mivel nem sokkal az incidens előtt a stáb egyik tagja lemásolta az anyagot, és hazavitte, hogy otthon dolgozhasson rajta.

Az archívum biztonságos tárolása költséges feladat. Még a megfelelően megszervezett tárolás sem nyújt védelmet az emberi hibákkal szemben.
Egy nagy Utah állambeli kórház biztonságos tárolóhelyen őrizte a páciensek adatait tartalmazó archívumait. Egy futárcég szállította az adathordozókat a tárolóhelyre minden nap. Egy alkalommal, éppen hétvége előtt, a futár úgy döntött, hogy aznap már nem kézbesíti a küldeményt, és éjszakára az autóban hagyta a dobozt. Az autót az éjszaka során feltörték, az adathordozókat pedig ellopták. A vállalatnak végül több millió dollárt kellett fizetnie a pácienseknek.

A felhőalapú tárolás technikai szempontból is megbízható, és az emberi hiányosságoktól is mentes.

Legyen szó egy éves beszámolóról, bérszámfejtési adatbázisról vagy bármilyen más adatról, még a szándékos törlést követően is visszaállíthatja őket.

Veszélyforrás

Ha mégis betörnek

Megoldás

Advanced Threat Analytics (helyi)
Microsoft Defender for Identity (korábbi nevén Azure Advanced Threat Protection) (felhőalapú)
Az Microsoft Defender for Identity dokumentációja

Informatikai nyelven

Nincs 100%-osan biztos védelem. Az a baj, hogy a vállalatok gyakran csak hónapokkal az incidens után veszik észre, hogy betörés történt, amikor a támadó már az összes adatot megszerezte. Ennek megelőzése érdekében védelemre és folyamatos monitorozásra is szükség van.

Ezt a feladatot jellemzően valamilyen behatolásérzékelő rendszer (Intrusion Detection System – IDS) szokta végezni, aminek a korszerű változata a felhasználói viselkedéselemzés (User Behavior Analysis – UBA).

Az UBA-rendszerek folyamatosan vizsgálják a dolgozók viselkedésének bizonyos jellemzőit: mikor dolgoznak, milyen eszközökre jelentkeznek be, milyen fájlokat nyitnak meg, milyen csoportokhoz tartoznak stb. Miután ez alapján felépítik a felhasználó viselkedési profilját, a rendszer képes jelenteni az esetleges magatartásbeli eltéréseket, ami lehet egy belső ember ténykedése, de egy támadó is okozhatja, aki feltörte egy felhasználó fiókját.

Az UBA-rendszer kétféle módon helyezhető üzembe:

01 Helyileg, az Active Directory-forgalom elemzése céljából. Ez a Microsoft ATA.

02 A felhőben, a tartományvezérlőkön helyileg telepített ügynökökkel. Ez a Microsoft Defender for Identity.

Üzleti nyelven

Nincs 100%-osan biztos védelem. Különösen nehéz védekezni azok ellen, akik eredendően megbízhatónak minősülnek, vagyis a cég munkatársai ellen. Nincs garancia arra, hogy egy dolgozó, aki nem kapta meg a várt bónuszt, nem fog szabotázst elkövetni vagy lemásolni bizonyos adatokat. Az alkalmazotti viselkedéselemző rendszer segít azonosítani a szokatlan magatartásformákat.

Ha például egy munkatárs sokáig bent marad az irodában, hogy bizalmas adatokat nyomtasson ki, a rendszer kiadja a megfelelő értesítést.

A rendszer azt is jelzi, ha egy alkalmazott olyan dokumentumokhoz próbál hozzáférni, amelyek általában nem szükségesek a feladatai elvégzéséhez.

Veszélyforrás

Ha mégis betörnek. Vagy ha még nem történt meg.

Megoldás

Microsoft Defender for Endpoint

A rosszindulatú tevékenységek zömét támadók hajtják végre a munkaállomásokon és a szervereken. Ha például sikerül megtéveszteni egy felhasználót egy adathalász e-maillel, a támadó hozzáférhet az illető munkaállomásához, ahonnan azután más gépekhez csatlakozhat.

A munkaállomásokon alapértelmezésben szokott lenni vírusvédelmi szoftver, de az ilyen programok képességei korlátozottak. A szoftver a munkaállomás erőforrásait használja, és a kifinomultabb támadások figyelése komolyan hátráltathatja a számítógép működését.

Az észlelés és a blokkolás kihelyezhető a felhőbe. Ilyenkor egy beépített szolgáltatás továbbítja a számítógépen történő eseményeket a felhőszolgáltatásnak, amely analizálja őket a mesterséges intelligencia és a Microsoft tudásbázisa segítségével.

Sokkal könnyebb kivizsgálni az incidenseket, ha a vállalat rendelkezik biztonsági műveleti központtal (SOC).

Veszélyforrás

Sérül egy kiemelt jogosultságokkal rendelkező felhasználó biztonsága

Megoldás

Azure AD Privileged Identity Management

A helyi Active Directoryban a jogosultságok biztonságos delegálásának egyik alapelve az, hogy a rendszergazdának több fiókkal kell rendelkeznie, amelyekhez más-más engedélyek tartoznak. Például:

01 Van egy fiókja, amely az internetes tevékenységekhez szükséges jogosultságokkal rendelkezik.

02 Van egy fiókja a munkaállomások rendszergazdai feladatainak ellátásához.

03 Van egy fiókja a szerverek rendszergazdai feladatainak ellátásához.

04 Van egy fiókja a tartomány rendszergazdai feladatainak ellátásához.

05 És így tovább.

Ha valamelyik fióknak sérülne a biztonsága, a támadó akkor sem szerezné meg az összes fontos jogosultságot. De mivel a különböző fiókok között váltogatni elég kényelmetlen, így sajnos nem minden vállalat fogadja meg ezt az ajánlást.

A felhőben is hasonló problémákat okoz, ha egy fiókhoz számos jogosultság tartozik.

Az Azure AD PIM szolgáltatása biztonságossá teszi a jogosultságok kiosztását anélkül, hogy több fiókot kellene fenntartani hozzá.
Ekkor a rendszergazda csak a szokásos felhasználói jogosultságokkal rendelkezik, a többi engedélyt pedig szükség szerint lehet aktiválni.

Vegyük a következő példát: egy támogatási mérnöknek módosítania kell egy felhasználó jelszavát. Ez a következő módon történik:

01 A mérnök bejelentkezik, és kiválasztja az Azure AD PIM funkciót. Rákattint az „Ügyfélszolgálati adminisztrátor szerepkör aktiválása” lehetőségre.

02 Ezután átesik egy többfaktoros azonosításon.

03 Megadja, hogy mennyi időre szeretné aktiválni ezt a jogosultságot.

04 Megkapja az illetékes jóváhagyó engedélyét.

05 Az engedélyezett ideig használhatja a rendszergazdai jogosultságokat.
Ha sérülne a fiók biztonsága, a támadó akkor sem szerezne kiemelt jogosultságokat.

Ez a szolgáltatás részben megtalálható a helyi Active Directoryban is, Privileged Access Management (PAM) néven.

Zárszó

A fent bemutatott fenyegetések és védelmi megoldások fényében elmondhatjuk, hogy a biztonság kérdését átfogó megközelítéssel érdemes kezelni. Nincs egyetlen varázsgomb, amelyet megnyomva univerzális védelemre tehetünk szert. Ugyanígy nincs egyetlen szoftver, amely képes lenne minden szinten gondoskodni a védelemről. A kényelem és a költségtakarékosság szempontjait szem előtt tartva a Microsoft termékei különálló összetevőként és csomagban is elérhetők. A fent bemutatott legtöbb szolgáltatást tartalmazó csomag neve Microsoft 365. A Microsoft 365-ajánlatokkal kapcsolatos további információért tájékozódjon a hivatalos webhelyünkön: https://www.microsoft.com/microsoft-365.


Microsoft