iSolutions

Biztonság a felhőben

Fokozd vállalatod adatbiztonságát a hibrid munka legújabb elvárásai mentén!

Az utóbbi évek robbanásszerű digitális fejlődése és a felhőtechnológia térnyerése rengeteg pozitívumot hozott magával a magyar kkv szektorban. A sikertörténeteket a legtöbb cég esetében azonban számos veszély árnyékolja be.

A kiberbiztonsági kockázatok és a hackertámadások megnövekedése, valamint a gondatlan adatvesztésből következő károkozás csak néhány példa azokra a fenyegetésekre, amikkel 2023-ban is szembe kell nézniük a magyar vállalatoknak.

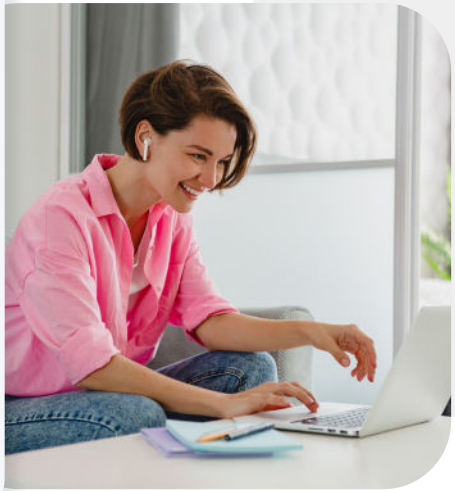
Ebben az ebookban körbejárjuk az elmúlt évek informatikai változásait, a modern munkavégzésből adódó új kihívásokat, valamint azt, hogy a felhőrendszerek miként tudják megteremteni a vállalatok IT biztonságát.
Emellett igyekszünk hasznos gyakorlati tanácsokat is adni, melyek segítségével egyszerűen csökkenthetőek az adatbiztonsági kockázatok.

Kritikus adatbiztonsági kockázatnak vannak kitéve a hazai kkv-k

A hibrid munkarend bevezetése az elmúlt években számos vállalat termelésére remek hatással volt. A rugalmas munkahelyek a vállalati felmérések alapján hatékonyabb munkavégzést eredményeztek és a nemrég kialakult nehéz gazdasági helyzetben is segítenek megtartani a cégeknek az értékes munkaerőt.

A hibrid munkavégzés a számos előnye mellett azonban újfajta kihívást is jelent a vállalatoknak. A digitális üzleti rendszerek bevezetése szempontjából nehéz helyzetben vannak a hazai cégek, akik többsége már eddig is nehezen birkózott meg a kiberbiztonsággal.

2023-ban IT-biztonsági irányelvek hiányában a vállalatok folyamatosan kritikus adatbiztonsági kockázatnak vannak kitéve. Ezt a tényt alátámasztják az elmúlt években elszaporodott zsarolóvírus támadások, amiknek hazánkban a legnagyobb vállalatok is áldozatául estek az utóbbi időben.



Függetlenül attól, hogy a hibrid munka hogyan fejlődik, minden vállalkozásnak fel kell készülnie arra, ami ezután következik.

Biztonság a felhőben

Amit minden vállalatnak tudomásul kell vennie, hogy a régi informatikai rendszereket nem a hibrid eszközökhöz és a modern munkavégzéshez tervezték. És itt nemcsak a felhasználói élményről beszélünk, a vezetők magas biztonsági kockázatnak teszik ki a szervezetüket, ha túlságosan ragaszkodnak az elavult IT rendszerekhez.

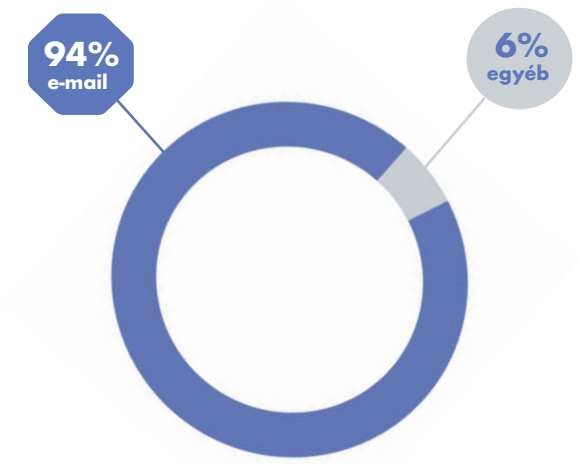
A felhőalapú megközelítéssel a szolgáltatói platformok folyamatosan frissülnek, ami nagymértékben csökkenti a szoftverjavítások szükségességét a vállalatok részéről. Ez a cégek egyszerűbb átállását és a kihívásokra való gyorsabb reagálását eredményezi.

Szerencsére mára számos vállalat felfedezte, hogy a már meglévő infrastruktúráik képességeit olyan módon kell bővíteniük, amelyek támogatják a hibrid munkavégzés gyakorlatát. A felhőalapú rendszerek megerősítik és védik a vállalat adatbiztonságát azáltal, hogy az eszközök, valamint földrajzi helyek szélesebb körére is kiterjedjenek, így az otthoni munkakörnyezet felügyelete is megvalósul.

A felhőalapú vállalati rendszereket folyamatosan fejlesztik annak érdekében, hogy ne maradjanak nyitva a biztonsági rések a hackerek előtt. Ám az alapvető szerverek és alkalmazások naprakészen tartása mellett a cégeknek figyelembe kell venniük a digitális eszközök egyre változatosabb keverékét is, valamint azt, amit a legnehezebb: az IT biztonság emberi oldalát.

Az IT biztonság emberi oldala

A rendszergazdák körében gyakori közhely, hogy az ember a leggyengébb láncszem az IT biztonságban.



Számítógépekre érkező rosszindulatú programok

Iparági jelentések szerint a rosszindulatú programok 94%-át e-mailben juttatják célba, és a rosszindulatú e-mail mellékletek közel 50%-a fertőzött dokumentumok formájában érkezik.

✖ ✖ ✖

Az, hogy a munkahelyi laptopok kikerültek az iroda ellenőrzése alól, nagymértékben megnehezíti a biztonsági problémák meghatározását és javítását az informatikai csapatok számára.

Gondoljunk csak bele, a legtöbb munkavállaló az otthoni személyes rendszereit is használhatja a munkahelyi eszközökön és megoszthatja azokat más felhasználókkal, akik nem kizárt, hogy rosszindulatú szoftverekkel teli weboldalakat böngésznek.

Vagy ami még rosszabb: sokan a szabadidejükben is a vállalati laptopjukat használják, sőt, még a családtagoknak is megengedik, hogy zenét, filmet vagy alkalmazásokat töltsenek le a céges eszközeikre.

Az Acronis tavalyi globális felmérése szerint 2021-ben a céges leállások több mint egyharmadát, azaz 36%-át kibertámadások okozták.
A jelentésből az is kiderült, hogy továbbra is a zsarolóvírusok jelentik az első számú fenyegetést a közép - és nagyvállalatokra és az általuk okozott károk 2023-ra meg fogják haladni a 30 milliárd dollárt.*

*Acronis Cyberthreats Report 2022

Modern idők, modern eszközök

A legtöbb szervezet számára a hibri munkarendre való átállás a házirendek és a biztonsági eszközök teljes újragondolását igényli. A végpontvédelmi szolgáltatásoknak át kell állniuk a felhőből nyújtott szolgáltatásokra. Emellett figyelembe kell venni a digitális eszközfejlesztést is, hiszen, ha a munkatársak nem rendelkeznek megfelelő felszereléssel, nem tudják kezelni azokat a modern rendszereket, amelyek megteremthetik készülékeiken az elvárt adatbiztonságot.

A felhőalapú infrastruktúra fejlesztése során a biztonsági szempontokat prioritásként kell kezelni, hiszen csak ezután valósulhat meg az üzleti folyamatok javítása és a rendszerekben rejlő új lehetőségek kiaknázása.

A cégek vezetőinek és az IT szolgáltatóknak közösen kell felülvizsgálniuk az adatvédelemre, a biztonsági mentésekre és a krízis-helyreállításra vonatkozó vállalati irányelveket és megbizonyosodniuk arról, hogy ezek a távoli környezetben is működnek.

A biztonság és termelékenység fenntartása mindig is nagy próbatételt jelentett a hazai vállalatoknak, de soha nem volt még nagyobb kihívás, mint napjainkban.

Vállalati együttműködés és IT biztonság a Google Workspace-ben!

A Google Workspace megteremti a biztonság, a rugalmasság és az együttműködés alapjaira épülő hibrid munka jövőjét!

Trust Nothing

A Workspace beépített ellenőrzésekkel és titkosítással teszi lehetővé a maximális adatbiztonságot a vállalat számára attól függetlenül, hogy a munkatársak honnan dolgoznak. A zéró bizalom megközelítés (Zero Trust Policy) lehetősége továbbá kiküszöböli a VPN-ek szükségességét is. Az adminisztrátorok eszköz szinten meghatározhatják, hogy ki, mikor és hogyan férhet hozzá a vállalati Workspace-hez.

Cloud-First

Egy olyan böngésző alapú megközelítés, amely hatékony architektúrával rendelkezik folyamatosan frissül, és helytől, eszköztől függetlenül bárhonnan elérhető. Így nincs szükség helyi eszközökre, natív alkalmazásokra vagy e-mail mellékletekre.

Detect Everything

A Workspace mindent észlelő funkciója globális szinten működik, hogy megvédje a cég adatait a rosszindulatú programoktól, a zsarolóvírusoktól, adathalászattól és az ellátási láncot érő támadásoktól, ehhez pedig nincs szüksége kiegészítőkre.

Protect Everyone

A Workspace mindenkit védő funkciója biztonságos végpontokkal védi az eszközöket, így a vállalat által biztosított, vagy az otthonról hozott privát berendezések sem igényelnek biztonsági frissítést és egyéb extra védelmet.

A Google Workspace megteremti a biztonságos együttműködést az irodai és a távolról dolgozó munkatársak között. A felhőalapú rendszernek köszönhetően a hibrid csapatok valós időben dolgozhatnak együtt és bárhonnan, bármilyen eszközről kapcsolódhatnak.

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 fenntartásokkal 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 ránk 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!

Elérhetőségeink

2040 Budaörs, Baross utca 89.
Új érdeklődés, konzultációs igény: + 36 70 777 6226
Ügyfélszolgálat, support: +36 1 506 0900
gondolatebreszto@isolutions.hu

iSolutions

Google Cloud Partner