Félti a vállalkozását az **internetes bűnözőktől**?

EGY LÉPÉSSEL MÁSOK ELŐTT A WINDOWS 10 RENDSZERREL

A fenyegetések területe VÁLTOZÓBAN VAN

A fenyegetések területe drámaian megváltozott az elmúlt években. Szinte már mindennap arról olvashatunk a főcímekben, hogy feltörték egy újabb vállalat rendszerét. Erre válaszul az alapoktól építettük fel a Windows 10 új architektúráját – nem pusztán magasabbra emeltük a falakat, hanem megkíséreljük teljesen kizárni a bűnözőket. A Windows 10 teljes körű védelemmel rendelkezik a legújabb biztonsági fenyegetések ellen.

A BIZTONSÁGI SZABÁLYOK MEGSÉRTÉSÉNEK HATÁSA A VÁLLALATOKRA:

USD 3,5 mil

A BIZTONSÁGI SZABÁLYOK MEGSÉRTÉSÉNEK ÁTLAGOS ESETI KÖLTSÉGE

Forrás: Ponemon. (2016). 2016 Cost of Data Breach: Global Analysis.

2x

Az IT-igazgatók körében végzett legutóbbi felmérés szerint a **biztonságtechnikai célú befektetések növekedési mértéke kétszer akkora, mint más jellegű befektetések esetében**.

Forrás: Forrás: McCarthy, John C. Brief: Technology Spending is Reaching a Tipping Point. Forrester Research, Inc., December 15, 2014.

AZONOSÍTÓVÉDELEM

75% **valószínűséggel mindössze három vagy négy jelszót használnak** összes fiókjukhoz a felhasználók.

Forrás: http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email

PROBLÉMA: A jelszavak nem biztonságosak. Illetéktelen személyek úgy férnek hozzá a vállalati hálózathoz, hogy másnak hisszük őket.

MEGOLDÁS: A Windows 10 a **Windows Hello**[1] és a **Credential Guard**[2] szolgáltatásokkal könnyen telepíthető és használható alternatívát kínál a jelszavak leváltására, és megvédi a felhasználókat a pass the hash típusú támadásoktól.

INFORMÁCIÓVÉDELEM

87% **felső vezetők közül** ennyien szivárogtattak már ki vállalati adatokat felügyelet nélküli, magáncélból felkeresett helyeken.

Forrás: Sitrol Friedberg, „On The Pulse: Information Security Risk In American Business". 2015.

57% ekkora arányban fordult elő, hogy véletlenül másnak küldtük az adatokat.

Forrás: Gross, Art. „A look at the cost of healthcare data breaches." HIPAA Secure Now, 2012. március 30.

MEGOLDÁS: A Windows 10 által eszköz- és fájlszinten egyaránt kínált **Bitlocker**[3] és **Windows Information Protection**[4] szolgáltatás segítségével garantálható, hogy a vállalati adatok se véletlenül, se szándékosan ne szivároghassanak illetéktelen kezekbe és helyekre.

FENYEGETÉSEKKEL SZEMBENI ELLENÁLLÁS

ILLETÉKTELEN HOZZÁFÉRÉS ELŐTT

TÖBB MINT

300 000

Mindennap újabb kártékony fájlok készülnek, amelyek aztán elterjednek az interneten.

Forrás: http://www.kaspersky.com/about/news/virus/2015/number-of-the-year

MEGOLDÁS: A Windows 10 vállalati szintű vírusirtót tartalmaz, olyan szolgáltatásokkal, mint a **Windows Defender**, a **Microsoft Edge**, egy szigetelt böngésző és a **Device Guard**, mely teljes mértékben lezárja a készüléket a nem megbízható alkalmazások számára.

ILLETÉKTELEN HOZZÁFÉRÉS UTÁN

200+NAP

Most, hogy a dolgozók a saját eszközeiket használják munkavégzésre, a támadók észrevétlenül tevékenykedhetnek **az Ön környezetében** – ami nagyon ijesztő!

Forrás: Mandiant. (2016). M-TRENDS 2016. Milpitas: Mandiant Consulting.

BÓNUSZ: **A Windows Defender Advanced Threat Protection** egy új szolgáltatás, amely lehetővé teszi a Windows vállalati ügyfelei számára a hálózatukon belül felmerülő fenyegetések és illetéktelen hozzáférések észlelését, vizsgálatát és elhárítását.

ESZKÖZBIZTONSÁG

Napjaink kiberfenyegetéseit nem lehet egyszerű szoftveres megoldással kezelni. Az ellenük való védekezés a hardveres kapacitás és speciális szoftverek megfelelő kombinációját igényli.

MEGOLDÁS: A Windows 10 által kínált **UEFI Secure Boot** és **virtualizáció alapú biztonság** segít megbízonyosodni arról, hogy a készüléken legelőször a Windows egy eredeti példánya indul el, illetve a legfontosabb Windows-folyamatokat egy biztosított végrehajtási környezetbe helyezi át, amely segít megelőzni az illetéktelen behatolásokat és fokozni az észlelési valószínűséget.

VEGYE FEL A KEZDEMÉNYEZŐ POZÍCIÓT AZ INTERNETES BŰNÖZŐKKEL SZEMBEN, A WINDOWS 10 SEGÍTSÉGÉVEL

TOVÁBBI INFORMÁCIÓK: **security.windows.com**

Microsoft

1 – A Windows Hello használatához különleges hardverek szükségesek, beleértve az ujjlenyomat-olvasót, a megvilágított IR-érzékelőt vagy az egyéb biometrikus érzékelőket.
2 – UEFI 2.3.1 vagy újabb verzió szükséges Trusted Boot szolgáltatással. A virtualizációs kiterjesztéseket, mint például az Intel VT-x, az AMD-V és a SLAT, engedélyezni kell. Windows x64 verzió szükséges. IOMMU, például Intel VT-d vagy AMD-Vi szükséges. BIOS Lockdown szükséges. Az eszközállapot-igazolási tanúsítványhoz TPM 2.0 ajánlott (ha nincs TPM 2.0, a szoftvert használja).
3 – A TPM-alapú kulcsvédelemhez a TPM 1.2 vagy újabb verziója szükséges.
4 – A Windows Information Protection, korábban Enterprise Data Protection (EDP) használatához a Mobile Device Management (MDM) vagy a System Center Configuration Manager telepítése szükséges, a beállítások kezelésére. Az Active Directory megkönnyíti a kezelést, de telepítése nem feltétlenül szükséges.