SZAKMAI LEÍRÁS

NYITOTT AJTÓK

A FELMÉRÉS RÁMUTATOTT: A NYOMTATÓK VÉDTELENEK A KIBERTÁMADÓKKAL SZEMBEN

Míg az IT-csapatok nagy figyelmet fordítanak a többi végpontra, a vállalati nyomtatók biztonságát gyakran elhanyagolják

A nyomtatók könnyű célpontot jelentenek: Rengeteg olyan hálózati nyomtató üzemel, amelyhez bárki hozzáférhet, és amelyeken semmilyen biztonsági rendszer sem található.

A fenyegetés azonban valós, és nem lehet figyelmen kívül hagyni. A vállalati szintű nyomtatók mostanra már nagy teljesítményű, hálózatba kapcsolt eszközzé fejlődtek, amelyek ugyanolyan sérülékenyek, mint a hálózat többi végpontja. Ezek a jellemzően nem megfelelően biztosított belépési pontok magukban rejtik a kibertámadások valós esélyét, emellett rajtuk keresztül a vállalat pénzügyi és személyes adatai könnyedén hozzáférhetők, amely komoly üzleti következményekkel járhat.

Ennek ellenére az a tanulmány, amelyet a Spiceworks végzett a közelmúltban több mint 300 vállalat IT-döntéshozója körében, rámutatott, hogy a válaszadók mindössze 16%-a gondolja azt, hogy a nyomtatók esetében az adattámadások esélye magas – ez az arány jóval magasabb a számítógépek/laptopok, illetve a mobileszközök esetében.[1] Ez az eredmény valós képet ad arról, hogy hogyan gondolkodnak az IT-szakemberek a hálózati biztonságról. Bár öt vállalatból mintegy három esetében megfelelő biztonsági intézkedések vannak érvényben a nyomtatókra nézve, ez az arány még mindig jóval elmarad a többi végponthoz képest – sebezhetővé téve ezzel a nyomtatókat, miközben egyszerű megoldások állnak rendelkezésre az ilyen típusú belépési pontok védelmére.

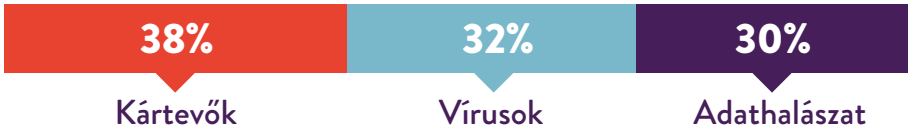
Ez a szakmai leírás bemutatja a nyomtatóbiztonsággal kapcsolatos adatokat a Spiceworks felmérése alapján, valamint a biztonsági támadások hatását, és azon modern beépített nyomtatóbiztonsági funkciók hatását, amelyek védelmet nyújtanak a kibertámadások ellen.

A VÁLASZADÓK **MINDÖSSZE 16%-A** GONDOLJA AZT, HOGY A NYOMTATÓK ESETÉBEN AZ ADATTÁMADÁSOK ESÉLYE MAGAS.[1]

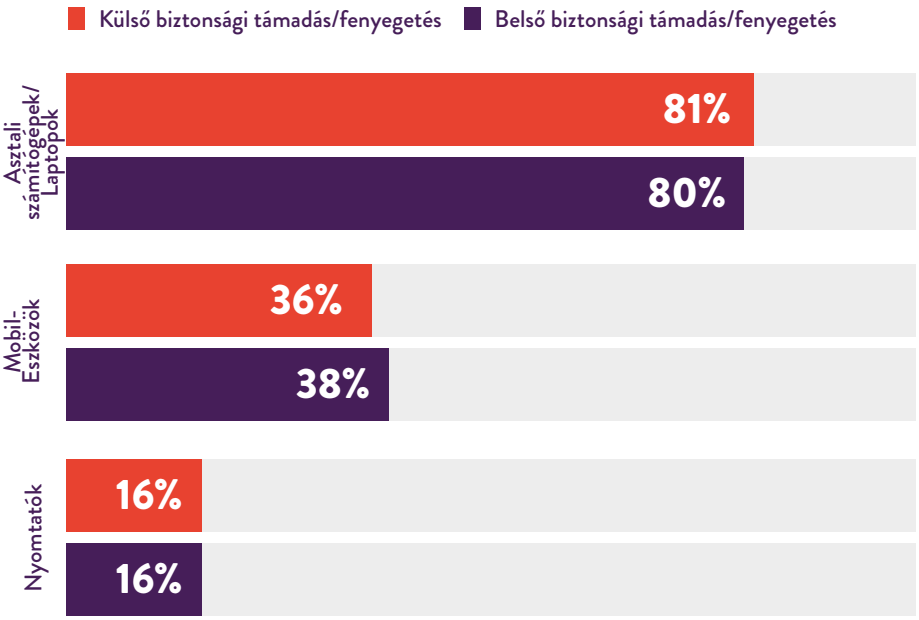
NYITOTT KAPUK A TÁMADÓK SZÁMÁRA

A Spiceworks felmérésében a válaszadók 74%-a (internet) nyilatkozott úgy, hogy vállalata az elmúlt évben bármilyen külső IT-biztonsági támadást vagy fenyegetést elszenvedett. 70% (internet) pedig belső IT-biztonsági támadásról vagy fenyegetésről számolt be, amely leggyakrabban felhasználói hibából, a személyi eszközök munka célra való használatából, illetve otthoni vagy nyilvános hálózat munka célra való használatából eredt.[1]

ELSZENVEDETT LEGJELENTŐSEBB KÜLSŐ IT-BIZTONSÁGI TÁMADÁSOK/ FENYEGETÉSEK



A leggyakoribb fenyegetések elsősorban asztali számítógépeken és laptopokon keresztül érkeztek, más esetekben pedig mobileszközökön és nyomtatókon át.[1] (A felmérés szerint a fenyegetések 16%-a érkezett nyomtatókon keresztül – ez az arány 4% volt egy 2014-es hasonló Spiceworks tanulmányban.) Az is lehetséges, hogy a válaszadók alulbecsülik a nyomtatókon keresztül érkező fenyegetéseket, mivel a nyomtatók felügyelete nem annyira szoros, mint a számítógépeké, illetve a mobileszközöké.



NEM FORDÍTUNK ELEGENDŐ FIGYELMET A NYOMTATÓKRA

Bármi legyen is a magyarázat, a Spiceworks felmérés egyértelműen rámutat, hogy a nyomtatóbiztonság sokszor csak egy elkésett gondolat.

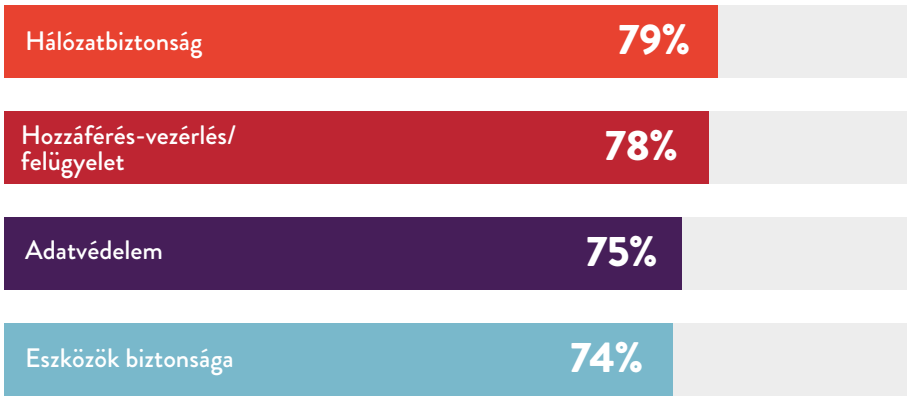
A vállalatok pontosan tisztában vannak a hálózat, a végpont és az adatbiztonság jelentőségével. A válaszadók nem kevesebb mint háromnegyede alkalmaz adatbiztonságot, hozzáférés-vezérlést/felügyeletet, adatvédelmet, illetve végponti biztonságot – vagy ezek ötvözetét.[1]

Ezeket a megoldásokat azonban elenyésző arányban alkalmazzák nyomtatókon. Míg a válaszadók 83%-a használ hálózati biztonságot az asztali számítógépeken/laptopokon, 55%-a pedig a mobileszközökön, nyomtatók esetében ez az arány csupán 41%.[1]

Az egyenlőtlenség a végpontbiztonság esetében még jelentősebb:

A válaszadók kevesebb mint egyharmada (28%) alkalmaz biztonsági tanúsítványokat a nyomtatók esetében – számítógépek esetében ez az arány 79%, mobileszközöknél pedig 54%.[1]

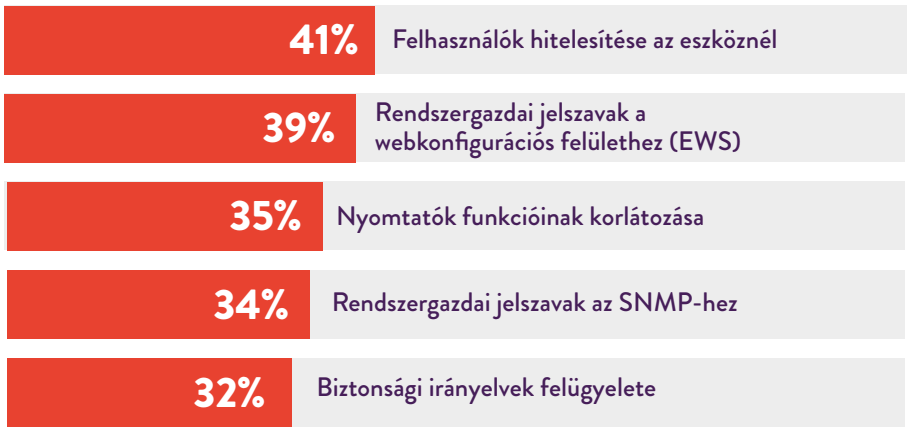
LEGFONTOSABB VÉGPONT-BIZTONSÁGI GYAKORLATOK



Ami az általános végponti eszközöknél használt védelmet illeti, a nyomtatók esetében leggyakrabban alkalmazott biztonsági intézkedés az adatbiztonság, a hálózati biztonság, valamint a hozzáférés-vezérlés volt, de a válaszadók kevesebb mint fele nyilatkozott úgy, hogy alkalmazza ezek bármelyikét a nyomtatók esetében.[1]

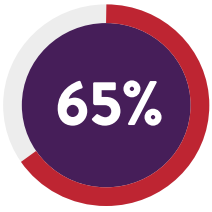
Néhány vállalat használ ugyan nyomtatóspecifikus biztonsági eljárásokat, de még ezek esetében is nagy eltérésekkel találkozhatunk. A vállalatok alig több mint 40%-a használ felhasználóhitelesítést, és kevesebb mint 40%-uk alkalmaz rendszergazdai jelszót a webkonfigurációs felületekhez.[1] Az erős védelemhez a vállalatoknak ezen megközelítések mindegyikét alkalmaznia kellene, és önmagában még ez sem elegendő.

A LEGFONTOSABB NYOMTATÓSPECIFIKUS BIZTONSÁGI GYAKORLATOK

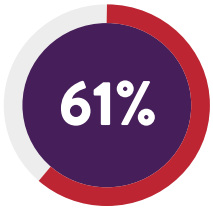


Ami a végpont megfelelőségét és az auditálási gyakorlatot illeti, a nyomtatóbiztonság szinte minden más végpont mögött elmarad. A vállalatok közel 90%-a alkalmaz információbiztonsági irányelveket, de ezek az irányelvek általában nem terjednek ki a nyomtatókra. Például míg a válaszadók 57%-a nyilatkozott úgy, hogy számítógépei kártevő elleni védelmi megoldásokat alkalmaznak, csak 17%-uk telepítette ezeket a nyomtatókra is.[1]

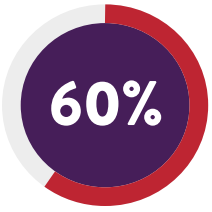
10-BŐL CSAKNEM 9 IT-SZAKEMBER ÁLLÍTJA, HOGY VÁLLALATA IT-BIZTONSÁGI IRÁNYELVEKET ALKALMAZ. ENNEK OKAI A KÖVETKEZŐK:



A megfelelőségi szabályok/szabványok betartatása



A kockázat elkerülése



Kockázattal/biztonsággal kapcsolatos gyakorlatok/irányelvek megszilárdítása a végfelhasználók hűségének fokozása érdekében

Egyértelmű, hogy a vállalatok nem veszik eléggé komolyan a nyomtatóbiztonságot – pedig ez nagyon fontos lenne.

„Számos nyomtatón az alapértelmezett jelszót használják, vagy nem is használnak jelszót egyáltalán, vagy tíz nyomtató alkalmazza ugyanazt a jelszót” – mondta Michael Howard, a HP vezető biztonsági tanácsadója a Computerworld júniusi számában. „Egy jelszó nélküli nyomtató aranybánya a hackerek számára. A támadások gyakori formája a közbeékelődéses támadás, ahol a hackerek a nyomtatót veszik célba, és [a bejövő dokumentumokat] átirányítják egy laptopra azok kinyomtatása előtt. A hackerek így gyakorlatilag mindent látnak, amit a vezérigazgató kinyomtat.”[2]

A NYOMTATÓRA VALÓ BEHATOLÁS KÖVETKEZMÉNYEI

A Bitdefender e-biztonsági elemzője, Bogdan Botezatu szerint a nyomtatók jókora potenciális biztonsági rést jelentenek. „Rengeteg telemetriai adattal rendelkezünk a sebezhetőséget értékelő laboratóiumainkban. Napjainkban már nem az útválasztó a legveszélyesebb eszköz az interneten: ezt a szerepet a nyomtató vette át.”[3]

A sebezhetőség jelentős hatást gyakorol a vállalatok működésére. Egyetlen olyan nyomtató, amelynek biztonsága hiányos, sebezhetővé teszi az összekapcsolt eszközökből álló hálózatot, és lehetőséget ad a hackereknek a hálózati eszközök lenyomozására – veszélybe sodorva ezzel a teljes hálózatot.

Mindannyian találkoztunk már a biztonsági támadások következményeivel. A Spiceworks felmérésében a megkérdezettek a támadások közül az alábbiakat sorolták az első öt helyre:[1]

1. Az ügyfélszolgálati hívások hatékonyabb kezelése és gyorsabb támogatás

2. Alacsonyabb termelékenység/ hatékonyság

3. Kevesebb rendszerleállás

4. Gyorsabb támogatás

5. Szigorúbb megközelítés a végfelhasználói irányelvek betartatása terén

A nyomtatók elleni támadások azonban még ennél is súlyosabbak lehetnek, különösen olyan többfunkciós nyomtatók használata esetén, amelyek elektronikus formában tárolják a kinyomtatott adatokat. A nyomtató

gyorsítótárjában tárolt nyomtatási feladatok révén a hackerek hozzáférést nyerhetnek az érzékeny személyes vagy üzleti adatokhoz.

Ami még ennél is nagyobb aggodalomra ad okot: a hiányos biztonsággal ellátott nyomtatón keresztül a vállalat szélesebb hálózatához is hozzáférhetnek, és olyan adatokat tulajdoníthatnak el, mint például a társadalombiztosítási számok, pénzügyi adatok, belső feljegyzések és dokumentumok. Az eltulajdonított információk nem csak az alkalmazottakat érinthetik, hanem a versenytársak is felhasználhatják azokat, illetve jelentősen ronthatják a vállalat jó hírnevét.

AZ EGYSZERŰ MEGOLDÁS: BEÁGYAZOTT BIZTONSÁGI FUNKCIÓK

A vállalatoknak minden területen, így a nyomtatók esetében is a biztonságra kell törekedniük. A mai vállalati szintű nyomtatók némelyike könnyen használható beépített biztonsági megoldásokat tartalmaz, amely felveszi a harcot a nyomtatók elleni támadásokkal. Ilyenek például a következők:

- Automatikus támadásérzékelés, védelem és javítás
- A használat nyomon követése az illetéktelen használat megakadályozása érdekében
- Egyszerű bejelentkezési lehetőségek, pl. PIN vagy okoskártya
- Közelségérzékelő kártyát leolvasó eszköz, amelynek segítségével a felhasználó gyorsan elvégezheti az azonosítást, és belépőkártyája révén biztonságosan nyomtathat a nyomtatón
- Biztonságos titkosított nyomtatás érzékeny dokumentumokhoz

Amikor legközelebb nyomtatót vásárol – legyen szó akár asztali, akár többfunkciós nyomtatóról –, válasszon olyan készüléket, amely integrált biztonsági funkciókat kínál – és aktiválja is azokat. Az egyszerű, nyomtatóspecifikus funkciók mellett semmi nem indokolja, hogy nyomtatója továbbra is sebezhető legyen; a dolgok internete révén úgyis számos dolog miattt kell aggódni –**nyomtatója ne tartozzon ezek közé!**

BIZTONSÁGOSABB NYOMTATÓT KERES?
TOVÁBBI INFORMÁCIÓK ›

Források:

[1] A Spiceworks 309 IT-döntéshozó körében Észak-Amerikában, az EMEA és az APAC országaiban, a HP megbízásából végzett felmérése, 2016. november

[2] „Nyomtatóbiztonság: valóban biztonságban vannak-e vállalata adatai?” Computerworld, 2016. június 1. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] “Printers Now the Least-secure Things on the Internet,” The Register, September 8, 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/