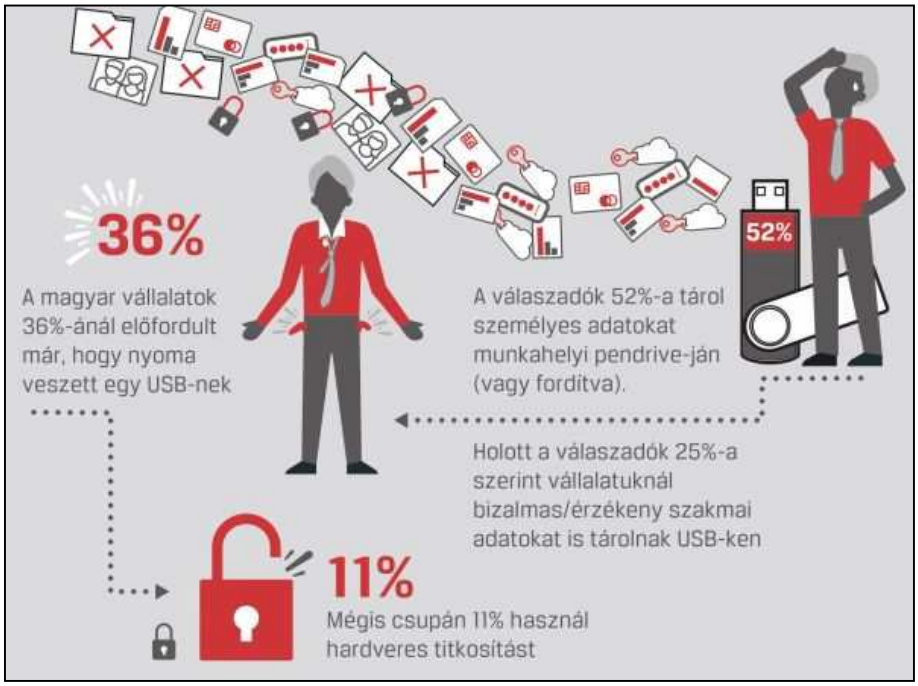
A pendrive-használat a céges adatvédelem leggyengébb pontja

A Kingston kutatása szerint a vállalatoknál még mindig alulértékelt kockázati tényezőknek számítanak az USB-k adatkezelési szempontból.

A felmérés szerint a szervezetek mintegy kétharmada nem alkalmaz megfelelő biztonsági intézkedéseket annak érdekében, hogy biztonságosan tárolják az adatokat a pendrive-okon. A hazai vállalatok 34 százaléka, illetve az EMEA-térségben működő cégek fele nem is tervez semmilyen változtatást ezen a téren annak ellenére, hogy a mobil adathordozók megfelelő titkosítása az új európai uniós adatvédelmi rendelet (General Data Protection Regulation – GDPR) előírásai miatt is fontos tényezőnek számít.

„A GDPR számos területen támaszt új követelményeket a vállalatokkal szemben. Az egyik legfontosabb elem, hogy az adatvédelmi incidenseket 72 órán belül kötelesek jelenteni. Sok szervezet nincs tisztában azzal, hogy még egy pendrive elvesztése is adatvédelmi incidensnek minősül, ha személyes adatokat tartalmaz és nincs titkosítva. Ha azonban olyan titkosított USB-meghajtón tárolták ezeket az információkat, akkor pusztán biztonsági incidensnek minősül a helyzet. Az ilyen jellegű eseteket pedig nem feltétlenül kell jelenteni, amivel komoly hírnévbeli és egyéb veszteségtől kímélhetik meg magukat a cégek, ráadásul az adataikat is nagyobb biztonságban tudhatják” – mutatott rá *Kaszál Norbert*, a *Kingston Technology* Magyarországért és Szlovéniáért felelős üzletfejlesztési menedzsere.



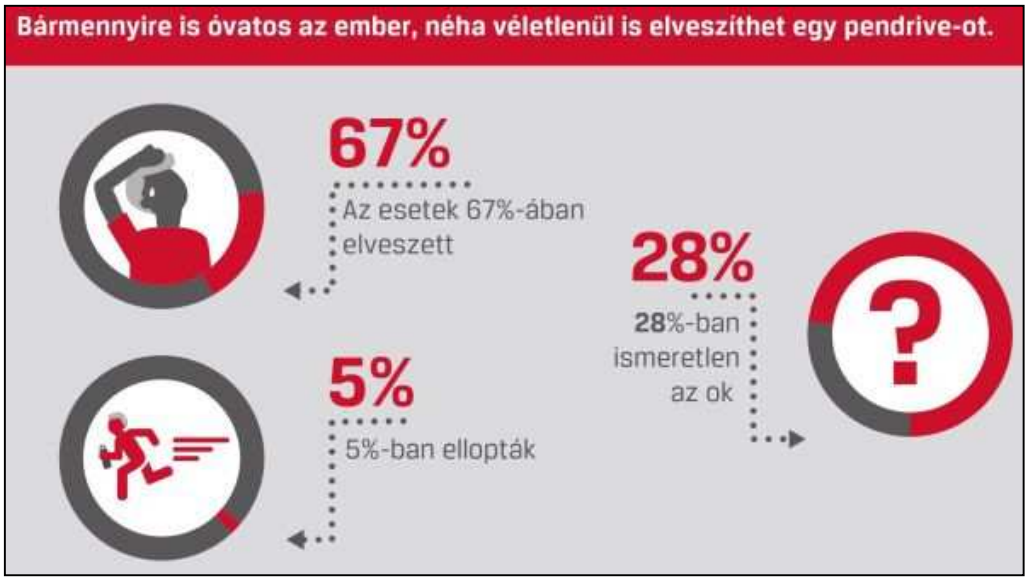
A probléma széles kört érint, hiszen a Kingston kutatása szerint rendkívül elterjedt az USB-k használata a szervezeteknél: szinte minden alkalmazott (84 százalék Magyarországon, 92 százalék az EMEA-országokban) és minden vállalat (94 százalék Magyarországon, 92 százalék az EMEA-régióban) használ pendrive-okat. Ráadásul a válaszadók több mint fele (52 százalék Magyarországon, 64 százalék az EMEA-országokban) vállalati és privát adatokat is tárol ugyanazon a USB-kulcson. Bizalmas és érzékeny adatokat hazánkban a válaszadók 25 százaléka, az EMEA-régióban pedig 21 százalékuk tárol pendrive-okon, ami titkosítás nélkül kockázatosnak számít.

Ezeknek az eszközöknek gyakran lába kél: a magyar vállalatok 36 százalékánál és az EMEA-régióban működő vállalatok 44 százalékánál előfordult már, hogy valamilyen módon eltűntek pendrive-ok. Magyarországon az esetek 5 százalékában ellopták a pendrive-okat, míg ez a szám az EMEA-országokban 11 százalék. Az aggasztó trendek ellenére a hazai válaszadók mindössze 11 százaléka alkalmaz hardveralapú titkosítást ezeken az eszközökön, a régióban pedig 6,7 százalék. Ez azt mutatja, hogy az USB-s adatbiztonság terén nincsenek felkészülve a szervezetek a GDPR követelményeire.

Bár a GDPR hivatalosan közel másfél éve érvénybe lépett, a magyar vállalatok megkésve, csak a kétéves felkészülési idő végéhez közeledve reagálnak rá, régiónkban azonban némileg jobb a helyzet. A PwC Magyarország 2017. nyári GDPR konferenciája után felmérést végzett a résztvevők és ügyfelei között, melyből kiderült, hogy szeptemberig megközelítőleg csupán a cégek negyede tartott a megoldások megvalósításánál, másik negyede pedig azonosította már az érintett adatokat, de így a vállalatok fele nem tett még érdemi lépéseket. Legtöbben csupán jogi problémaként kezelik az elvárásokat: az esetek több, mint 40 százalékában a jogi osztály vezeti a megfelelési projekteket, és csak fele ennyi esetben irányítja dedikált projektszervezet.

Az elvárások, bár jogi szempontból részletesebben meghatározottak, nem biztosíthatók megfelelő IT-biztonsági kontrollok nélkül. A nélkülözhetetlen biztonsági elvárásokon túl kulcsfontosságú a biztonság-tudatosság és a megfelelő védelmi, valamint kockázatcsökkentő technikai protokollok működtetése a vállalatoknál. „Alapvető IT biztonsági hiányosságok könnyen alááshatják a megfelelési törekvéseinket, ezt nagyon könnyű alábecsülni” – hívta fel a figyelmet *Gyimesi Csaba*, a PwC kiberbiztonsági szolgáltatásokért felelős vezető menedzsere.

Az új szabályozások értelmében egy incidens súlyosságát befolyásolja, hogy mekkora kockázatot jelent az érintettek jogainak sérülésére. Így a hiányos kontrollkörnyezet vagy ismeretek kiemelt szerepet játszanak, főként az adatok tárolásánál, kiadásánál vagy átvitelénél. „Projektjeink során gyakran segítünk a szervezeteknek meghatározni a szükséges lépéseket a titkosítatlan adatátvitellel, kontrollálatlan eszközök használatával vagy tudatossági hiányosságokkal kapcsolatban” – tette hozzá Gyimesi Csaba.



Az USB-n tárolt adatok biztonságát illetően a Kingston azt tanácsolja a vállalatoknak, hogy használjanak olyan titkosított pendrive-okat, amelyeket a legmagasabb szintű biztonságot igénylő adatok védelmére terveztek. Az USB-k különféle titkosítási szinteknek megfelelően széles választékban elérhetők, különálló vagy felügyelt megoldásként is. A megfelelő technológia használata mellett az is elengedhetetlen, hogy megtanítsák az alkalmazottakat a pendrive-ok helyes használatára, mivel a friss felmérés eredményei azt mutatják, hogy sok vállalatnál hiányosak az ismeretek azok kezelésére vonatkozóan. A szervezeteknek ezenfelül célszerű biztonsági házirendeket bevezetniük a mobil adathordozók alkalmazásánál, mielőtt előfordulhatna valamilyen adatszivárgás.

Forrás: **https://sg.hu/cikkek/it-tech/128486/a-pendrive-hasznalat-a-ceges-adatvedelem-leggyengebb-pontja**

Válogatta: Berke Barnabásné