ELVESZETT ADATAINK

ADATHORDOZÓINK A MODERN TECHNOLÓGIÁNAK KÖSZÖNHETŐEN EGYRE KISEBBEK ÉS EGYRE TÖBB ADATOT TUDUNK TÁROLNI RAJTUK, AMI A SOK ELŐNY MELLETT EGY ÓRIÁSI HÁTRÁNYT IS MAGÁBAN HORDOZ. EGYETLEN APRÓ ÉSZREVÉTLEN MOZDULATTAL VAGY EGY KIS FIGYELMETLENSÉGGEL IS ÓRIÁSI MENNYISÉGŰ ADATOT TUDUNK ELVESZÍTENI, AMI KOMOLY ANYAGI KÁROKAT IS OKOZHAT NEKÜNK.

CSIZMADIA-DARAB ISTVÁN, IT BIZTONSÁGI SZAKÉRTŐ, ANTIVIRUS.BLOG.HU

TECHNOLÓGIAI HÁBORÚ

Az ilyen incidens sajnos hazánkban is elég gyakori. Az ESET biztonságtechnológiai termékek hazai disztribútora, a Sicontact Kft. partnereit és ügyfeleit kérdezte meg az adathordozókkal kapcsolatos felmérésében, ahol több mint 1700 fő válaszolt a kérdésekre. A felmérésből kiderült, hogy a válaszadók harmada (33%) vesztett már el adathordozót. Az 1787 darab online beküldött válasz alapján a megkérdezettek 18%-a hagyta már el személyes adatokat is tartalmazó eszközét, amely végül biztonságban megkerült. Nem volt ilyen szerencsés az a 15%, amelynek sohasem lett meg az eszköze, így csak bizakodni tud abban, hogy nem kerültek illetéktelen kezébe a személyes adatai. Az elhagyott USB adathordozók mellett a válaszadók 20 százaléka talált már ilyen, más által elhagyott eszközt, és jelentős részük meg is nyitotta ezek tartalmát. Egyébként a vállalati biztonságtudatossági oktatások része az is, hogy gyanakodjunk, ha ilyen eszközt találunk, mert lehet, hogy szándékosan helyezték azt oda nekünk. Kutatással-fejlesztéssel foglalkozó cégek esetében gyakori trükk, hogy valamilyen kémprogramot tartalmazó USB kulcsot dobnak a vállalati parkolóba, ahol aztán a gyanútlan és felelőtlen alkalmazott beviszi a munkahelyére, és ezzel megfertőzi a rendszert.

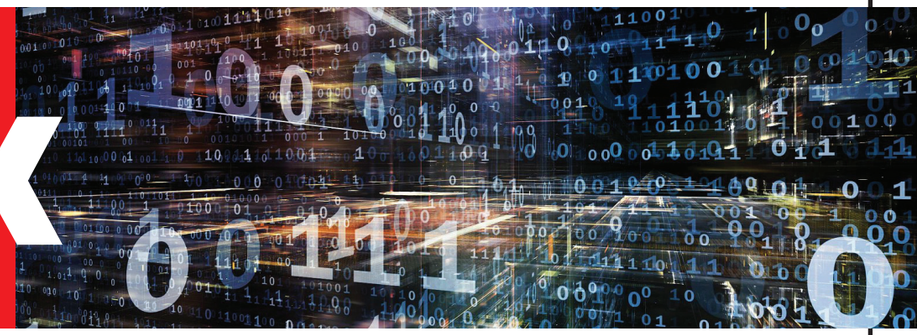
jellemzőbb ez a fajta tudatosság vállalati környezetben – sőt, valahol egyenesen a biztonsági policy része, azaz előírás is. Ekkor azt is meghatározhatják például, hogy csak egy bizonyos gyártótól származó, titkosított eszközt lehet használni, a többit pedig központilag letiltják – ennek lehet egy összetettebb megoldása egy DLP (Data Leakage Prevention) rendszer bevezetése.

Esetlegesen elvesztett adathordozóink védelmére nagyon jó módszer, ha titkosító megoldásokat használunk a különböző készülékeinken, így ha azok elvesznének, bizalmas adataink akkor sem kerülhetnek illetéktelenek, például számítógépes bűnözők kezébe. Ehhez adunk most öt tippet:

1. GONDOLKOZZUNK KOMPLEXEN!

Az adatbiztonsági stratégiában ne hagyatkozzunk kizárólag a titkosításra. Adataink számos módon kompromittálódhatnak, és a titkosítás ezek egy részére ad csupán választ. Ha a titkosítás során valami elromlik, akkor szándékaink ellenére adatainkat saját magunktól is „megvédhetjük”, azaz elérhetetlenné tehetjük. Ezért soha ne felejtsük el fontos adataink mentését. A titkosítás nem más, mint egy további biztonsági réteg adataink és a kiberbűnözők (hackerek, lehallgatók és ipari kémek) között. Az is igaz, hogy

…évi 22 000 pendrive a ruha-tisztítóban…



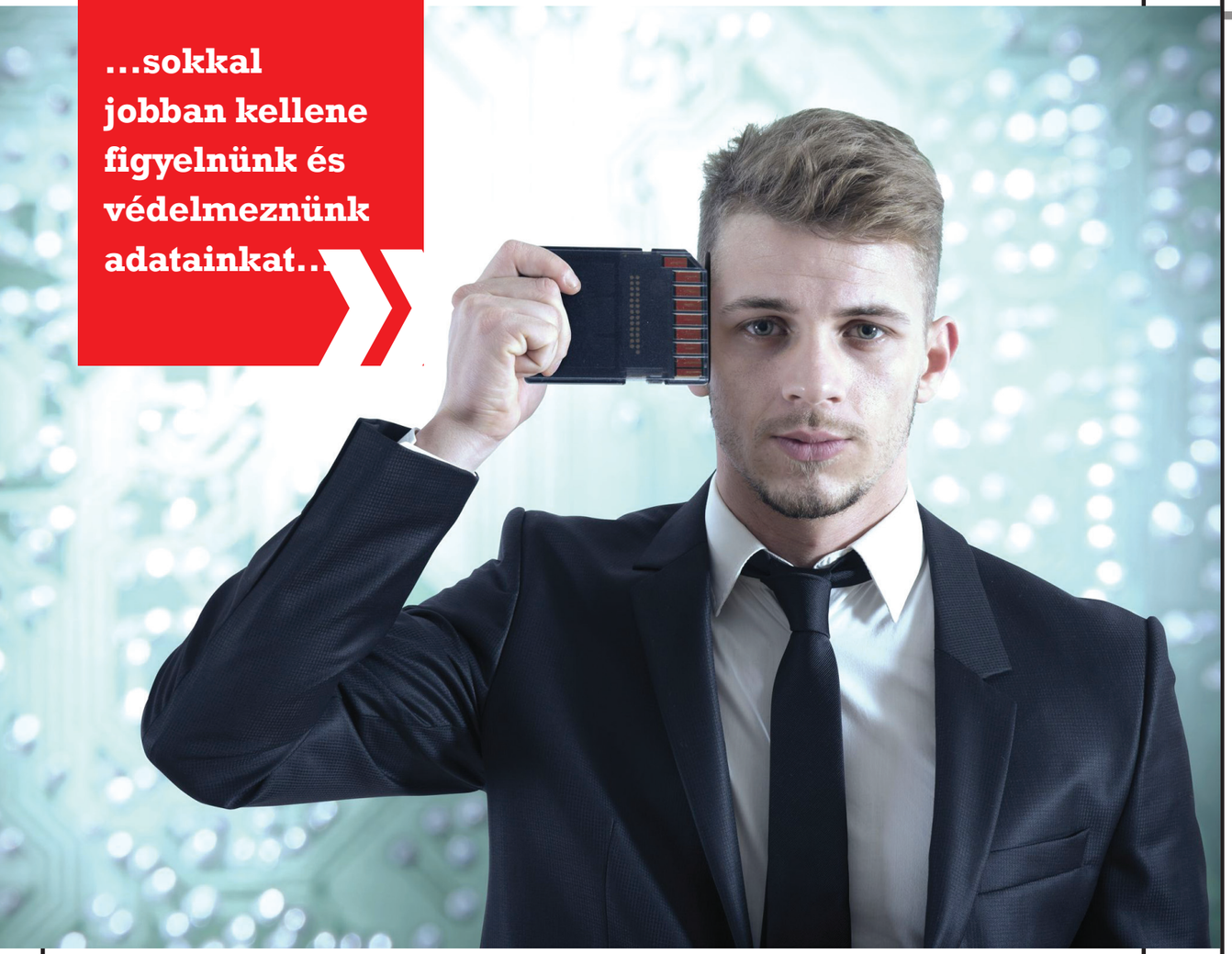
A hazaihoz hasonló eredményt mutat az ESET egy közelmúltban végzett angliai felmérése is, ahol 500 ruhatisztítót kérdeztek meg. Ott a kabátokban, zakókban felejtett évi 22 ezer darab eszköznek mindössze 45%-a jut vissza eredeti gazdájához, a maradék körülbelül tízezer pendrive és a rajtuk lévő adatok sorsa mindenki számára ismeretlen marad.

A számos elhagyott adathordozó egyértelműen rávilágít arra, hogy sokkal jobban kellene figyelnünk és védelmeznünk eszközeinket, valamint adatainkat. A titkosított USB kulcsok használata a magánfelhasználóknál nem gyakori. Sokkal inkább a titkosítás megvédi adatainkat saját, kockázatokkal teli viselkedésünktől is. Másrészről az adatok titkosítása sem jelent védelmet, ha hitelesítő adataink gondatlanság vagy egyéb ok miatt a hackerek kezébe kerülnek. Számos egyéb veszély is leselkedik adatainkra: elegendő, ha a felhőszolgáltatásokra vagy az e-mail kommunikációra gondolunk.

2. TITKOSÍTSUNK!

Egyik első lépésként a titkosítás jó választás lehet. Adataink értéket képviselnek számunkra, akár magánemberként, vállalkozóként vagy munkavállalóként. Sajnos azonban ezek az adatok nem

…sokkal jobban kellene figyelnünk és védelmeznünk adatainkat…



csak a mi számunkra értékesek. A titkosításnak számos előnye van, míg a hátrányok könnyen kezelhetőek. Ezek közül is jó néhány – például hogy lelassítja a számítógépet – nem több városi legendánál. Igaz ugyan, hogy évekkel ezelőtt érezhető volt lassulás egy teljes merevlemez titkosítása esetén. De ma, amikor a számítógépek már ritkán használják ki teljes kapacitásukat, a különbség alig érezhető a mindennapi munka során. Összefoglalva: a titkosítás jelentős előnyöket hordoz, minimális hátrányok mellett. Ha komolyan vesszük adataink védelmét, a legkönnyebb és leghatékonyabb út, ha stratégiánkat a titkosításra építjük.

3. FIGYELJÜNK A RÉSZLETEKRE!

A titkosító megoldás választásánál fontos a használhatóság, de ne feledkezzünk meg a termék rugalmasságáról és skálázhatóságáról sem! A titkosító megoldás legyen egyszerűen bevezethető és a mindennapokban könnyen használható. Skálázhatónak is kell lennie, hogy a fejlettebb funkciók is elérhetőek legyenek szükség esetén. Válasszunk olyan megoldást, amelyet megújításkor vagy frissítéskor nem szükséges újratelepíteni. Ne feledjük, ha a titkosító megoldás nemcsak éves licence-ekkel, hanem örök licence-szel és éves támogatási szerződéssel is elérhető, akkor költségeink menedzselésével pénzügyi rugalmasságot is nyerünk.

4.VÁLASSZUNK MEGBÍZHATÓ PARTNERT!

Számos kereskedelmileg elérhető titkosító program van a piacon. Vannak racionálisan árazott termékek, de olyanok is, amelyek elképesztő költségeket jelentenek. Olyan megoldást válasszunk, amely az ipar által elfogadott titkosítási algoritmust használ, és rendelkezik olyan kulcsmegosztó megoldással, ami biztosítja, hogy az összes felhasználó között biztonságosan cserélhető az adat, titkosított módon.

5. NE ÁLLJUNK MEG FÉLÚTON!

Fejlesszük kialakított adatbiztonsági stratégiánkat, és folyamatosan törődjünk adataink védelmével! Ne hagyatkozzunk kizárólag a titkosítási megoldásunkra! Ne feledjük: amint adataink bármilyen módon elérhetővé váltak, csak enyhíteni tudjuk az ezzel járó kockázatokat, teljesen kiküszöbölni nem. Online elérhető adatok esetében a titkosítás jelentős előnyökkel rendelkezik. De nem várhatjuk, hogy a titkosítás megoldja az összes adatbiztonsági problémánkat. Csak egy példát említünk: könnyen tönkretehetünk minden korábbi erőfeszítést, ha az alkalmazott jelszavak erőssége nem megfelelő, ha több helyen használjuk a jelszavainkat, vagy megosztjuk azokat másokkal.

EGYÉB JÓ TANÁCSOK

Okostelefonoknál javasolt az úgynevezett lopásvédelmi megoldások használata a komplex védelmi megoldás alkalmazása során, e funkció segítségével az eszközök távoli lezárása, távtörlése és valamilyen formában történő (GPS vagy WIFI háromszögelés) megtalálása. A mobil OS gyártóknál is létezik egyébként alapszintű titkosítás; abban az esetben, ha jelkódot vagy PIN kódot beállít a tulajdonos, akkor az eszköz beépített adattárolójának a titkosítását is elvégzi automatikusan az operációs rendszer. Ezen felül természetesen lehetőségünk van szoftveres vagy hardveres, harmadik féltől származó megoldással is élni az okoseszközökön és a számítógépeinken is. A kínált megoldásokban kiválaszthatjuk, hogy egy fájlt, mappát vagy a teljes tárhelyet, merevlemezt szeretnénk titkosítani. Egy ingyenes alternatíva lehet például a nyílt forráskódú GPG, amivel fájlokat, mappákat lehet titkosítani megfelelő módon. Vállalati környezetben gyakori az MDM (Mobil Device Managment) és a MAM (Mobil Application Managment) alkalmazások használata. Nagyon fontos terület és szerencsére egyre több szolgáltatás esetén elérhető a kétfaktoros azonosítás használata is, például banki oldalra való belépéskor. Itt kapunk a telefonunkra egy kódsort tartalmazó sms-t, ami egy második számú azonosítási faktornak minősül a felhasználónév és jelszó használata mellett.

Összességében reméljük, hogy egyre többen érzik át ennek a területnek a súlyát, és alkalmazzák majd a jövőben ezeket a megoldásokat. Mi is ezért dolgozunk, hogy ez a fajta tudatosság beépüljön az emberek mindennapjaiba.