V-DETECT ANTIVÍRUS KFT.

Főbb informatikai biztonsági problémák és azok kezelése

Összefoglaló a Magyar Ügyvédi Kamara tagjai számára
2015.

Adathordozók elvesztése vagy ellopása

Az ügyvédi munka során keletkező adatokat és információkat különböző adathordozókon tároljuk. Notebookok, asztali számítógépek, szerverek, okostelefonok, memóriakártyák és USB kulcsok tárolják az szerződéseinket és munkánkat.

Nyilvánvaló, hogy ezeknek elvesztése vagy ellopása biztonsági kockázatot jelent. Pontosan ezért fontos, hogy a következő módszerekkel védekezzünk az információvesztés ellen:

1. Számítógépeinket, okostelefonjainkat védjük erős jelszóval. A megfelelő jelszó legalább 12 karakteres, tartalmaz kis- és nagybetűket, számokat, valamint egyéb írásjeleket (*/:+) is. Amikor nem dolgozunk az eszközzel, zárjuk azt le. Mobiltelefon esetében állítsuk rövidre az automatikus képernyőzárat, és a feloldáshoz használjunk jelszót vagy más azonosítási módszert.
2. Amennyiben erre lehetőség van (például Android operációs rendszerű telefonok esetében), kapcsoljuk be a titkosítást a készüléken. Notebookjainkon és az USB kulcsokon is létrehozhatunk titkosított könyvtárakat, melyekben jelszóval védett módon tárolhatunk fontos dokumentumokat. Ilyen funkcióval több biztonsági szoftver rendelkezik (például G Data TotalProtection).
3. Eszközeinket tegyük távolról törölhetővé. Androidos okostelefonunkra telepítsünk teljes körű biztonsági programot (például G Data InternetSecurity for Android), melynek segítségével távolról, SMS-ben küldött paranccsal törölhetjük a készülék összes adatát.

4. Készítsünk biztonsági mentéseket, és azokat lehetőleg tároljuk földrajzilag külön helyen. Betörés vagy tűzesemény ellen csak az olyan mentés nyújt védelmet, melyet nem az eredetileg lementett adathordozó mellett tárolunk.

Fontos tudni, hogy az adatokat a titkosítás csak akkor védi, ha a titkosítás feloldásához szükséges jelszót nem tudja más megszerezni. Ha a jelszavunk kitalálható, kikövetkeztethető vagy fenyegetéssel, kényszerítéssel megszerezhető, akkor a titkosítás nem ér sokat. Ezért fontos, hogy jelszavunkat ne osszuk meg másokkal, és fontos az is, hogy a különböző eszközeink védelmére ne ugyanazt a jelszót használjuk, amit már bármilyen internetes szolgáltatásban megadtunk.

Adathordozók helytelen törlése és leselejtezése

Az adatok makacs módon ragaszkodnak az adathordozókhoz, melyeken tároljuk őket. Ha újraformázzuk a notebook merevlemezét, ha újratelepítjük az operációs rendszert vagy ha alkalmazzuk a gyári beállítások visszaállítását a mobiltelefonunkon, ez mind nem elegendő az adatok alapos és teljes eltüntetéséhez. Az újraformázott adathordozókról játszi könnyedséggel lehet visszaállítani az adatoknak legalább egy részét, és ehhez nincs szükség laboratóriumi módszerekre sem. Ingyenes adat-visszaállító szoftverek tucatjával tölthetőek le az internetről.

Éppen ezért fontos, hogy amikor leselejtezünk egy adathordozót, ha odaadjuk másnak, hogy utánunk használja azt, vagy egy számítógépet vagy okostelefont a cégen belül egy másik alkalmazott kezd el használni, akkor a gazdaváltás előtt az adathordozót minősített módszerrel, felülírással fertőtlenítsük az adatoktól. Erre a feladatra a Blancco cég kínál szoftveres megoldásokat, melyek jegyzőkönyvezett módon képesek megtisztítani az adathordozókat.

A jegyzőkönyvek vezetése a jogi felelősséget is csökkenti, mivel hiteles módon igazolható, hogy az adathordozót körültekintően megtisztítottuk a gazdaváltás előtt.

Az adathordozók teljes fertőtlenítése szükség még két esetben: olyankor, amikor a számítógép vírussal fertőződik meg, illetve olyankor, ha arra illegális tartalom kerül.

A vírusirtó szoftverek képesek a fertőzés aktív komponenseit megszüntetni, leirtani, de nem garantálják, hogy a fertőzés semmilyen rést nem ütött a védelmi pajzson. Ezért érdemes tiszta lapot nyitni a megfertőzött számítógép életében, és teljes fertőtlenítés után újratelepíteni az operációs rendszert. Ugyanez igaz olyankor, ha illegális vagy kompromittáló tartalom került az adathordozóra: a Windows beépített törlési módszerei nem garantálják azt, hogy visszaállíthatatlan módon törlésre kerül az anyag. Ebben az esetben is javasolt a teljes adathordozó vagy pedig legalább az illegális, kompromittáló anyagok minősített, felülírással történő törlése (lásd még a következő pontot).

Fájlok és szerződések törlése

Amikor egy windowsos számítógépen a lomtárba húzunk egy szerződést, majd a lomtárat kiürítjük, valójában az eredeti anyag viszonylag könnyen visszaállítható. A Windows ugyanis árnyékmásolatokat és előző verziókat őriz meg a fájlokból annak érdekében, hogy az esetleges rendszerösszeomlásból származó károkat enyhítse. Emellett azok az adatok, melyeknek a helyét a merevlemezen még nem írtuk felül, könnyen visszaállíthatóak egy adatmentő szoftver segítségével.

Ezért érdemes a fontos megsemmisítendő anyagokat a számítógépeken shreddelnünk, azaz megsemmisítenünk. Ennek működési háttere az, hogy az adattörlést végző szoftver nem csupán letörli az eredeti dokumentumot, de annak helyét a merevlemezen felülírja egy, a titkosításhoz is használt algoritmus segítségével. Így a dokumentum (például egy szerződés vagy fotó) soha többet nem állítható vissza.

Ilyen jellegű, működés közbeni adattörlésre a Blancco cég kínál megoldást a Blancco File szoftver segítségével. A Windows operációs rendszeren működő alkalmazás pontosan ugyanúgy működik, mint az eredeti lomtár, azonban nem csak törli az egyes fájlokat, hanem azok eredeti helyét felülírja a merevlemezen.

Vírusfertőzés

Az esetleges vírusfertőzésre semmiképpen sem szabad legyinteni, mivel a mai kártevők rendkívül kellemetlen helyzeteket okozhatnak.

A kémprogramok hitelkártyaszámokra, jelszavakra és belépési adatokra vadásznak a számítógépeken. Ilyen kártékony kódokat bűnözők gyártanak, de elfordulhat, hogy irodánk célzott támadás vagy megfigyelés áldozatává válik.

A zsaroló kártevők a fertőzés után titkosítják a merevlemezen tárolt adatokat, majd váltságdíjat követelnek a titkosítás feloldásáért. Képesek arra, hogy az összes dokumentumot és fényképet elérhetetlenné tegyék a megfertőzött számítógépeken, és arra is, hogy a belső hálózaton keresztül átterjedjenek egyik számítógépről a másikra.

Az illegális tartalmakat terjesztő kártevők a megfertőzött számítógépeket egy úgynevezett botnet hálózat részévé teszik, majd arra használják, hogy kéretlen reklámleveleket vagy adott esetben gyermekpornográf anyagokat terjesszenek a segítségükkel. Ismertek olyan esetek, amikor nyomozó szervezetek azért inzultáltak egy ártatlan magánszemélyt, mert annak megfertőzött számítógépe illegális anyagokat terjesztett a háttérben.

Éppen ezért rendkívül fontos, hogy windowsos, androidos és OS X operációs rendszerrel rendelkező eszközeinken folyamatosan naprakész, jogtiszta vírusirtó szoftvereket futtassunk. A kártevők ellen kizárólag a vírusvédelem tudja megvédeni adathordozóinkat.

Illegális vagy nem kívánt tartalom elleni védekezés

Biztonsági kockázatot jelenthet szervezetünk számára, ha az alkalmazottak otthonról vagy más helyről nem kívánt anyagokat hoznak be a benti számítógépekre, vagy illegális szoftvereket töltenek le az internetről, esetleg olyan weboldalakat tekintenek meg munkahelyi számítógépükről, melyek kompromittálhatják a szervezetünket.

Az ilyen veszélyek ellen a központilag menedzselhető, úgynevezett végpontvédelmi megoldások nyújtanak megoldást, melyek jellemzően a vállalati vírusvédelemmel vannak egy szoftverbe csomagolva. Az ilyen megoldások használata már informatikai tudást feltételez, ugyanakkor a következő funkciókat nyújtják szervezetünk számára:

- Külső eszközök, például USB kulcsok és CD-meghajtók korlátozása annak érdekében, hogy a munkatársak ne tudjanak nem kívánt anyagokat behozni.
- Nem kívánt alkalmazások (például torrent kliensek) futtatásának megakadályozása a védett számítógépeken.
- Internetes tartalomszűrés, a pornográf, erőszakos, szerencsejátékkal vagy hackeléssel kapcsolatos weboldalak tiltása.

Hálózat feltörése

Egy cég belső hálózatát az interneten keresztül is támadás érheti. Ezek ellen jellemzően a tűzfalak nyújtanak védelmet.

A tűzfalak lehetnek szoftveres vagy hardveres megoldások. Szoftveres tűzfal jellemzően minden fejlett biztonsági programcsomagban megtalálható, ezek használata alapvetően fontos a notebookok esetében.

A hardveres tűzfalak ára a százezres nagyságrendtől kezdődve tart a milliós nagyságrendig. Ezek az eszközök képesek arra, hogy egy cég teljes internetes forgalmát felügyeljék, kiszűrjék és megakadályozzák a betörési kísérleteket. A hardveres tűzfalak használat azonban informatikai szaktudást igényel. Amennyiben cégünk forgalma ezt megengedheti magának, alkalmazásuk mindenképpen javasolt.

Távmunka védelme

Amennyiben szeretnénk, hogy irodánk belső számítógépes hálózatát az irodán kívülről is el tudjuk érni (például azért, hogy hozzáférjünk a benti

számítógépünkön tárolt anyagainkhoz), mindenképpen gondoskodnunk kell az ilyen kapcsolatok biztonságossá tételéről.

A virtuális magánhálózatok (VPN – Virtual Private Network) alkalmazása ebben az esetben megoldást jelent a biztonságos kapcsolatok létrehozására. A VPN esetében egy titkosított csatorna jön létre a kint tartózkodó és a benti számítógép között, így az adatforgalmat nem lehet visszafejteni és felhasználni.

VPN megoldások jellemzően a hardveres tűzfalakban találhatóak, de alkalmazhatunk szoftveres VPN hálózatot is. Ezek kiépítése informatikai szaktudást igényel.

Levelezés és egyéb felhő alapú szolgáltatások feltörése

Amennyiben levelezésünkre felhő alapú szolgáltatást (például Office365 vagy Gmail) használunk, rendkívül fontos, hogy ezt egyedi és összetett jelszóval védelmezzük a feltörés ellen. Minden szolgáltatáshoz más és más jelszó választása javasolt.

Támadás a webszerver ellen

Amennyiben irodánk weboldallal rendelkezik, vagy a fájlok megosztására úgynevezett FTP szervert használ, fontos, hogy megbízható és jól védett hosting partnert válasszunk. Általánosságban elmondható, hogy a hosting feladatok ellátásával egy, az ilyen feladatokra szakosodott céget bízzunk meg.