OUCH! | 2014. december

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

Mi az a vírusvédelem?

Áttekintés

A vírusvédelem olyan alkalmazás, amelyet a felhasználók a számítógépükre vagy mobil eszközeikre telepítenek azért, hogy megakadályozzák a káros szoftverek okozta fertőzéseket. A „káros szoftver" alatt együttesen értjük a vírusok, férgek, trójai- és kémprogramokat. A káros szoftver eredeti formájában (malware) a malicious (káros, ártalmas) és software szavak összevonásából alakult ki. Amennyiben egy támadó meg tudja fertőzni az áldozat rendszerét egy káros szoftverrel, képes megfigyelni a billentyűzet leütéseket, ellopni a dokumentumokat, vagy más számítógépek elleni támadásra felhasználni azt. Ellentétben az általános hittel, bármilyen operációs rendszert futtató számítógépet (akár Mac OS X-et vagy Linux-ot) meg lehet fertőzni káros szoftverekkel.

A szerzőről

Jake Williams a Rendition Infosec alapítója (**www.renditioninfosec.com**), valamint a SANS minősített oktatója és kurzusainak szerzője. Megtalálható a Twitter-en **@MalwareJake** néven, illetve a saját blogot vezet a **malwarejake.blogspot.com**-on.

A felhasználóknak lehetőségük van egy önálló vírusvédelmi, de akár egy komplett biztonsági szoftvercsomag megvásárlására is. Viszont komoly gondot jelent, hogy a vírusvédelmi szoftverek manapság már nem képesek tartani az iramot a kiberbűnözők által fejlesztett, újabb és újabb káros szoftverekkel. Olyan sok új változat jelenik meg naponta, amelyek ellen egyetlen vírusvédelmi szoftver sem képes 100%-os védelmet nyújtani. Ezért nagyon fontos tisztában lenni azzal, hogy bár a vírusvédelem segít tisztán tartani a felhasználó rendszerét, nem képes minden fenyegetést észlelni és megállítani! Ahhoz, hogy ezt megértsük, nézzük meg közelebbről ezen alkalmazások működését!

Hogyan működik a vírusvédelem?

Általánosságban elmondható, hogy kétfajta típus létezik: a szignatúrán és a viselkedés felismerésen alapuló megoldások. A szignatúra alapú felismerés úgy működik, mint az ember immunrendszere. Folyamatosan szkenneli a felhasználó rendszerét, olyan jellemzők és szignatúrák után kutatva, amelyek ismert káros szoftverekre utalnak. Erre a célra egy adatbázist használ, és ha talál valamit a számítógépen, ami egyezik az adatbázis egy elemével, akkor megpróbálja ártalmatlanítani. Hasonlóan az emberi immunrendszerhez, az adatbázist is rendszeresen frissíteni kell, hogy védelmet tudjon nyújtani az újabb káros szoftverek ellen. A vírusvédelem csak olyan ellen tud védelmet nyújtani, amit veszélyesnek ismer fel. Komoly problémát jelent, hogy a kiberbűnözők gyorsabban fejlesztik az újabb káros szoftvereket, mint ahogy a vírusvédelmi szoftverek készítői képesek az adatbázist frissíteni. Ennek eredményeként még a legnaprakészebb vírusvédelem esetén is lesz olyan újabb fejlesztésű káros szoftver, amely képes megkerülni azt.

Mi az a vírusvédelem?

A viselkedés megfigyelésekor a vírusvédelem nem próbálja meg azonosítani az ismert káros szoftvereket, hanem figyel minden számítógépre telepített alkalmazást. Ha egy program gyanúsan kezd viselkedni – például egy védett fájlhoz akar hozzáférni, vagy módosítani akar egy másik programot – akkor feljegyzi a tevékenységet, és értesítést küld a felhasználónak. Ez a megközelítés védelmet képes biztosítani olyan káros szoftverek ellen is, amelyek jelenleg nincsenek benne semmilyen adatbázisban sem. Viszont ennek a rendszernek is van hibája, például hamis riasztásokat küld. A felhasználó bizonytalan lehet, hogy melyik riasztást hagyja figyelmen kívül, vagy melyiket vegye komolyan, egy idő után pedig érzéketlenné válik a riasztások iránt, és minden esetben az „Elfogad” gombra kattint, ez viszont oda vezet, hogy a rendszer védtelenné válik, és könnyebben megfertőződhet. Ezen kívül előfordulhat, hogy a káros szoftver már azelőtt is ott volt a számítógépen, mint ahogy a vírusvédelem észrevette volna, így nem lehet tudni, hogy korábban milyen műveleteket hajtott végre.

Bár a vírusvédelem fontos része a számítógép védelmének, mégsem tud minden fenyegetést kivédeni. Végeredményben nem a technológia, hanem a felhasználó a védekezés legfontosabb eleme.

A vírusvédelem fontos része a számítógépek és mobil eszközök védelmének, ezért javasolt – amikor lehetőség van rá – a telepítése és aktív használata. Azonban fontos észben tartani, hogy a működési elvtől függetlenül, soha nem lesz képes védelmet nyújtani az összes lehetséges káros szoftver ellen. Végeredményben elmondhatjuk, hogy mindig a felhasználó – és nem a technológiai megoldások – képesek a legjobban védeni a kibertámadások ellen.

Vírusvédelmi tanácsok

1. Csak ismert és megbízható forrásból szerezzük be a vírusvédelmi szoftvert! A kiberbűnözők gyakran alkalmazzák azt a cselt, hogy hamis vírusvédelmi szoftvert árulnak, amely tulajdonképpen egy káros szoftver.
2. Mindig a vírusvédelmi szoftver legújabb verzióját használjuk, ügyeljünk arra, hogy az előfizetés rendezve legyen, és hogy a program automatikusan letöltse a frissítéseket! Ha a számítógépet leválasztjuk az Internetről, vagy kikapcsoljuk, akkor újraindítás vagy újrakapcsolódás után ne mulasszuk el a szoftver és adatbázis frissítését!
3. Állítsuk be úgy a szoftvert, hogy automatikusan vizsgálja át a hordozható eszközöket (például USB pendrive), illetve kapcsoljuk be a valós idejű védelmet!
4. Olvassuk el a vírusvédelem által küldött üzeneteket! A legtöbb figyelmeztetés vagy tartalmaz további információkra mutató hivatkozást, vagy valamilyen cselekvési, védekezési javaslatot. Ha a munkahelyi számítógép küld ilyen üzenetet, akkor értesítsük az ügyfélszolgálatot vagy a rendszergazdát!

Mi az a vírusvédelem?

5. Ne kapcsoljuk ki, vagy távolítsuk el a vírusvédelmi szoftvert azért, mert lelassítja a számítógépet, megakadályozza bizonyos weboldalak elérését, vagy megtiltja a programok telepítését! A vírusvédelem kikapcsolása szükségtelen kockázatot hordoz magában, amely a számítógép megfertőződésével végződhet. Céges számítógépnél problémák esetén inkább keressük meg az ügyfélszolgálatot, ha pedig az otthoni számítógéppel adódnak gondok, akkor a vírusvédelmi szoftver gyártóját, esetleg cseréljük le egy másik megoldásra!
6. Ne használjunk egy időben két különböző vírusvédelmi terméket! Ilyen alkalmakkor előfordulhat, hogy a két program zavarni fogja egymást, amely az általános biztonsági szint csökkentését idézheti elő.
7. Tanuljuk meg felismerni a vírusvédelem által küldött üzeneteket! A kiberbűnözők egyik trükkje, hogy weboldalak segítségével hamis üzeneteket küldenek, amelyek azt állítják, hogy „segítenek megjavítani" a számítógépet. Az ilyen üzenetre történő kattintás veszélybe sodorja a számítógépet.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Anti-virus termékek összehasonlítása:	http://www.av-test.org/en/
A pszichológiai manipuláció:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf
Adathalász email támadások:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_hu.pdf
Feltörtek, mit tegyek?:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor