Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

A biztonság megőrzése öt lépésben

Áttekintés

A technológia nemcsak egyre fontosabb szerepet tölt be az életünkben, hanem egyre bonyolultabbá is válik. Figyelembe véve a technológia fejlődési sebességét, nincs könnyű dolgunk akkor, ha naprakészek akarunk lenni biztonsági szempontból. Úgy tűnik, hogy mindig jönnek újabb és újabb útmutatók, tanácsok, amelyek megmondják, hogy mit kellene, és mit nem kellene tennünk. Bár a részletek változnak, az internetes biztonság alapjai tulajdonképpen ugyanazok, mint korábban. Függetlenül attól, hogy milyen technológiát használunk, vagy éppen hol vagyunk, javasolt az alábbi öt fontos lépés megtétele.

A szerzőről

Lenny Zelster az NCR Corp. szakértője, fő területe az ügyfelek IT infrastruktúrájának védelme, ezen kívül pedig a SANS Intézetnél a káros szoftverek elleni védekezést oktatja. Lenny elérhető a Twitteren a **@lennyzeltser** címen, és rendszeres blogot vezet a **blog.zeltser.com**-on.

Öt fontos lépés

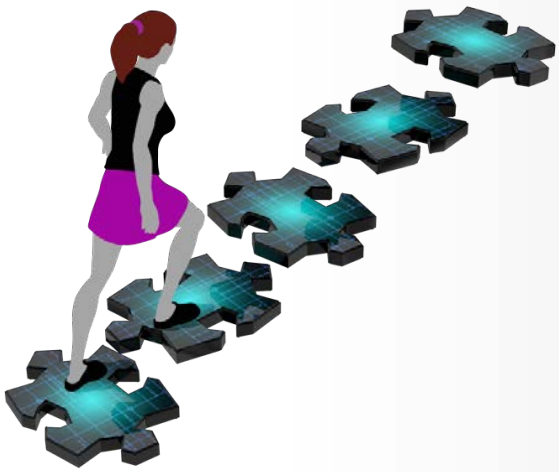
Az alábbiakban mindegyik lépésről adunk egy rövid áttekintést. Az egyes pontokról részletesebb leírást a hírlevél végén található Hivatkozások alatt található linkeken lehet olvasni.

1. **A felhasználó**: az első és legfontosabb, hogy mindig észben tartsuk, a technológia önmagában nem fog megvédeni bennünket, a támadók mindig találnak egy egyszerű módszert arra, hogy kijátsszák a biztonsági megoldásokat. Ha meg akarják szerezni a jelszavunkat vagy a hitelkártyaszámunkat, akkor különféle egyszerű trükkökkel el fogják érni, hogy mi magunk adjuk meg nekik. Például kapunk egy telefonhívást valakitől, aki azt állítja, hogy a Microsoft technikusa és úgy látja, hogy fertőzött a számítógépünk. A valóságban egy kiberbűnözőről van szó, aki így akar hozzáférést szerezni a rendszerünkhöz. Vagy ha kapunk egy email-t, amelyben azt állítják, hogy a megrendelt csomagunkat nem tudják kiszállítani, és ezért kattintsunk egy hivatkozásra, ahol meg tudjuk adni a címünket. Ezzel szemben a link egy hamis weboldalra vezet minket, amin keresztül káros szoftverek segítségével fel tudják törni a számítógépünket. Végső soron a támadások elleni legjobb védelem mi magunk vagyunk. Legyünk óvatosak, használjuk a józan eszünket, és így felismerhetjük a legtöbb támadást!

2. **Frissítés**: mindig legyünk naprakészek, telepítsük a legfrissebb operációsrendszer frissítéseket, a legújabb alkalmazásokat minden számítógépre, mobil eszközre vagy bármire, amivel csatlakozunk az Internetre! A kiberbűnözők folyamatosan keresik az aktuálisan használt technológiákban lévő sebezhetőségeket. Ha találnak egy sérülékenységet, akkor speciális programok segítségével kihasználják azokat, hogy betörjenek az általunk használt rendszerekbe és hálózatokba, bármilyen technológiát is használjunk. Eközben a szoftver-

A biztonság megőrzése öt lépésben

gyártók is folyamatosan dolgoznak azon, hogy az ismertté vált sérülékenységeket kijavítsák, majd ezeket frissítések formájában nyilvánosságra hozzák. Azzal, hogy mindig telepítjük a szoftvergyártók által készített javításokat, megnehezítjük a kiberbűnözők a dolgát, hogy betörjenek a számítógépünkbe. Ennek érdekében - amikor lehetőségünk van rá - kapcsoljuk be a frissítések automatikus letöltését! Ezt a szabályt ne csak a számítógép és mobil készülék esetén tartsuk szem előtt, hanem minden olyan eszköz esetén, amely kapcsolódik az Internetre – TV, baba monitor, otthoni router, játékkonzol, vagy akár az autónk. Ha a számítógépünk operációs rendszere, mobil eszközünk, vagy egy általunk használt technológia már nem támogatott és nem érhető el hozzá új frissítés, javasolt olyan új verzió beszerzése, amin van támogatás.



Az említett biztonsági lépések megtételével jó úton járunk ahhoz, hogy megvédjük magunkat, miközben felhasználjuk a legújabb technológiákat.

3. **Jelszavak**: a védekezés következő lépése az, hogy egyedi, erős jelszót válasszunk minden egyes Internetre kapcsolódó eszköznek, online fióknak és alkalmazásnak! Nagyon fontos, hogy erős és egyedi jelszó legyen! Az erős azt jelenti, hogy a hacker-ek vagy az automatikus programjaik ne tudják könnyen megfejteni. Egyetlen szóból álló jelszó helyett használjunk több szóból állót, amelyekbe számokat és írásjeleket is keverünk. Az egyedi azt jelenti, hogy minden eszközt és online fiókot saját jelszóval védjük. Ez azt jelenti, hogy ha valaki megszerzi a jelszavunkat, akkor más internetes szolgáltatások és eszközök nem kerülnek veszélybe. Nem emlékszel az erős, egyedi jelszavakra? Nem kell aggódni, néha mi sem. Ezért javasolt, hogy mindenki használjon egy jelszókezelő programot, amely képes titkosított formában tárolni a mobil eszközökön vagy számítógépen használt online fiókok jelszavait! Végezetül pedig mindig kapcsoljuk be a kétlépcsős hitelesítést minden olyan felhasználói fiókhoz, amely erre lehetőséget ad!

4. **Titkosítás**: negyedik lépésként javasolt a titkosítás használata, amely lehetővé teszi azt, hogy csak mi, illetve az általunk megbízhatónak ítélt emberek férjenek hozzá az adatainkhoz. Az adatok titkosítása két helyen történhet meg: vagy a helyi fájlokat titkosítjuk, vagy az adatok átvitelét két számítógép közt. A helyi állományok titkosítása a merevlemezen vagy USB meghajtókon tárolt fájlokra értendő. Az operációs rendszerek többsége lehetővé teszi, hogy a teljes lemezt titkosítsuk (Full Disk Encryption) valamilyen módszer segítségével. Javasolt ezt minden olyan eszközön bekapcsolni, ahol rendelkezésre áll. Az adatátvitel titkosítása azt jelenti, hogy a saját számítógépünkről vagy egyéb mobil eszközünkről egy másik eszköznek elküldött adatokat titkosítjuk (például az online banki tranzakciók közben). Könnyen le tudjuk ellenőrizni, hogy egy weboldal használ-e titkosítást: ha a megnyitott weboldal címe „https”-sel kezdődik, és van mellette egy zárt lakat, akkor az oldalon titkosított adatátvitelt használunk.

A biztonság megőrzése öt lépésben

5. **Biztonsági mentések**: annak ellenére, hogy megteszünk minden óvintézkedést, előfordulhat, hogy mégis feltörik valamelyik eszközünket vagy fiókunkat. Az ilyen esetekben csak akkor lehetünk teljesen biztosak abban, hogy megszabadultunk a káros szoftver okozta fertőzéstől, ha teljesen töröljük az eszközön lévő rendszert, és újratelepítjük azt. Ha például a támadó megakadályozott bennünket abban, hogy hozzáférjünk a személyes állományainkhoz, képeinkhez, dokumentumainkhoz, stb., akkor az egyetlen lehetőségünk az, hogy egy korábbi biztonsági mentésből helyreállítjuk ezeket. Azért, hogy egy hasonló esetben cselekedni tudjunk, nagyon fontos, hogy rendszeresen készítsünk biztonsági mentést a személyes adatainkról, illetve hogy ellenőrizzük azt is, hogy a mentésből helyre tudjuk állítani azokat. Az operációs rendszerek és mobil eszközök többsége támogatja az automatikus mentést.

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

Adathalász email támadások:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_hu.pdf
A tabletek biztonsága:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_hu.pdf
Erős jelszavak:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_hu.pdf
Jelszókezelő megoldások:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_hu.pdf
Kétfaktoros hitelesítés:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_hu.pdf
Titkosítás:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_hu.pdf
Biztonsági mentés:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_hu.pdf

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

