OUCH!

SANS SECURITY AWARENESS

Az Ön havi biztonságtudatossági hírlevele

Igen, célpont vagy

Áttekintés

A legtöbben – hibásan – azt gondoljuk, hogy nem lehetünk kibertámadás célpontjai, mi és a rendszereink vagy fiókjaink nem képviselnek elég értéket egy támadáshoz. Ennél távolabb már nem is állhatnánk az igazságtól. Amennyiben bármilyen módon is használjuk a technológiát - akár a munkahelyünkön, akár otthon - higgyük el, van értékünk a rossz fiúk számára. De, szerencsések vagyunk, mert már rendelkezésünkre áll a legjobb védelmi eszköz a kibertámadások ellen: Önmagunk.

Miért vagyunk célpontok?

Napjainkban az interneten több típusú támadó van jelen, és mindegyiknek más és más motivációja van. Szóval, miért is akarna minket bármelyikük is megtámadni? Azért, mert azzal, hogy meghackel minket, közelebb kerül céljai eléréshez. Az alábbiakban található két elterjedt példája a támadók típusainak, és az okok, amiért minket is célba vehetnek:

⚠ **Kiberbűnöző:** Ezek az emberek azért dolgoznak, hogy a lehető legtöbb pénzt szerezzék. Számukra az teszi az Internetet olyan értékessé, hogy akár egy gombnyomással bárkit megtámadhatnak a világon. Nagyon sok módja van annak, hogy hogyan lehet pénzt szerezni tőlünk. Például pénzt lophatnak el a bankszámlánkról vagy nyugdíj elő takarékossági számlánkról, hitelkártyát készíttethetnek a nevünkben, melynek számláit mi fogjuk megkapni, felhasználhatják a számítógépünket, hogy mások számítógépét támadják meg róla, vagy feltörik a közösségi média, vagy játék fiókjainkat és eladják azokat más bűnözőknek. A lista majdnem végtelen, hogy a rossz fiúk miként szerezhetnek pénzt tőlünk. Több százezer olyan bűnöző van, aki minden reggel azzal a céllal ébred fel, hogy a lehető legtöbb embert meghackelje, minket is beleértve.

☆ **Célzott támadások:** Ezek a magasan képzett támadók gyakran nemzetállamoknak, bűnözői csoportoknak, vagy versenytársaknak dolgozva a munkahelyünkön céloznak meg minket. Talán úgy véljük, hogy a mi munkánk nem kelti fel senki érdeklődését sem, de nagyon meglepődnénk az igazságon:

- Az információnak, amit a munkahelyünkön kezelünk, borzasztó nagy értéke lehet különböző szervezetek vagy kormányok számára.
- A célzott támadások kivitelezői nem csak azért támadhatnak meg minket a munkahelyünkön, mert kifejezetten mi vagyunk a célpontok, hanem azért is, hogy rajtunk keresztül más munkatársunkat, vagy más rendszereket is megtámadhassanak.

- **Ezek a támadók annak alapján is célba vehetnek minket, hogy milyen más cégekkel vagy partnerekkel dolgozunk együtt.**

Van vírusirtóm, biztonságban vagyok

Rendben, célpontok vagyunk, nem probléma. Akkor egyszerűen telepítünk egy vírusirtót és egy tűzfalat a számítógépünkre, és védve is vagyunk, ugye? Nos, sajnos nem. Sok ember érzi úgy, hogy valamilyen védelmi eszköz telepítésével már védve is van. Sajnos, ez nem teljes mértékben igaz. A kiberbűnözők folyamatosan fejlődnek, és sok támadási metódusuk könnyen megkerüli a biztonsági technológiákat. Például gyakran készítenek olyan speciális malwareket, amelyeket a vírusirtónk nem tud észlelni. Elkerülik az elektronikus levélszűrőnket egy személyre szabott adathalász támadással, vagy felhívnak minket telefonon, és megtévesztéssel rávesznek arra, hogy adjuk meg a hitelkártya adatainkat, jelszavunkat, vagy pénzünket. A technológia fontos szerepet játszik a védelmünkben, de végső esetben mi magunk vagyunk a legjobb védekezés.

Szerencsére, biztonságosnak lenni nem olyan nehéz. Alapvetően a józanész és pár alapvető viselkedési forma a legjobb védekezés. Ha kapunk egy e-mailt, egy üzenetet vagy telefonhívást, ami rendkívül sürgős, furcsa, vagy gyanús, az akár támadás is lehet. Azért,hogy megbizonyosodjunk róla, hogy a számítógépeink és eszközeink biztonságban vannak, tartsuk őket naprakészen, és engedélyezzük az automatikus frissítést rajtuk. Végül, használjunk erős, egyedi jelmondatot minden fiókunkhoz. “Kiber-ébernek” maradni a legvégső védelmi vonal. Nem tudjuk, hol kezdjük? Iratkozzunk fel a havi OUCH! hírlevélre a sans.org/ouch oldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

A szerzőről

Matt Bromiley *(@mbromileyDFIR) egy incidenskezelő és digitális nyomrögzítő, több, mint nyolc éves tapasztalattal a háta mögött, aki a világ számos pontján dolgozott már szervezetekkel és különböző incidensekkel. Matt továbbá digitális nyomrögzítést és incidenskezelést tanít a SANS FOR508 és FOR572 tanfolyamain.*

Hivatkozások

Állítsuk meg a malwereket: https://www.sans.org/u/L1J
A pszichológiai manipuláció: https://www.sans.org/u/L1O
Telefonhívásos támadások és csalások: https://www.sans.org/u/L1T
Jelmondatok: https://www.sans.org/u/L1Y
Poszter – Ön a célpont: https://www.sans.org/u/L23