SANS SECURITY AWARENESS

Havi biztonság tudatossági hírlevél mindenkinek

Fel vagyok törve?

Áttekintés

Lehet bármilyen biztonságos a rendszerünk csakúgy, mint az autóvezetés esetében, előbb vagy utóbb baleset érhet minket. A továbbiakban ismertetünk néhány nyomot, ami alapján gyaníthatjuk, hogy meghekkeltek minket, valamint azt, hogy ha tényleg bekövetkezett, akkor mit tehetünk. Minél hamarabb felismerjük, hogy valami rossz történt, annál nagyobb valószínűséggel lehet a problémát orvosolni.

Gyanúra okot adó nyomok

A vírusirtó program üzenetet küld, hogy a rendszerünket megfertőzték. Bizonyosodjunk meg róla, hogy az üzenetet valóban a mi vírusirtónk küldte, és nem egy felugró ablak egy weboldalról, ami próbál átverni és rá akar venni, hogy hívjunk egy számot, vagy telepítsünk valami más programot. Bizonytalanok vagyunk benne? Nyissuk meg a saját vírusirtónkat.

Egy felugró ablak szerint a számítógépünk titkosításra került, és váltságdíjat kell fizetnünk azért, hogy adatainkat visszakapjuk.

A webböngészőnk olyan weboldalakat nyit meg, amiket eredetileg nem akartunk meglátogatni.

A számítógépünk vagy az egyik program folyamatosan leáll, ismeretlen programok ikonjai, vagy furcsa felugró ablakok jelennek meg a képernyőnkön.

A jelszavunk nem működik pedig tudjuk, hogy a helyes jelszót írtuk be.

A barátaink érdeklődnek, hogy miért küldünk nekik folyton (kéretlen) leveleket, miközben valójában mi nem küldtünk nekik ilyen leveleket.

A hitelkártyánkon olyan ismeretlen kiadás vagy készpénzfelvétel jelenik meg, amiket nem mi kezdeményeztünk.

Hogyan reagáljunk

Ha azt gyanítjuk, hogy meghekkeltek minket akkor minél gyorsabban reagálunk annál jobb. Ha a hackelés a munkánkkal kapcsolatos, ne próbáljuk meg orvosolni, inkább azonnal jelentsük az esetet a munkahelyünkön. Ha a személyes használatú rendszerünk, vagy fiókunk fertőződött meg, az alábbi intézkedéseket tehetjük:

Jelszómódosítás: Nemcsak a számítógépes és mobil jelszavaink megváltoztatása, hanem az online hozzáféréseink, fiókjaink jelszavainak megváltoztatása is ide tartozik. Ne a feltört gépen hajtsuk végre a jelszómódosításokat, használjunk egy másik gépet, amiben biztosak vagyunk, hogy biztonságos. Ha sok felhasználói fiókunk van, kezdjük a legfontosabbakkal. Ha nem tudjuk nyomon követni az összes jelszavunkat, akkor használjunk jelszókezelő programot.

Pénzügy: A bankkártyánkkal vagy folyószámlánkkal kapcsolatos ügyekben azonnal keressük a számlavezető bankunkat. Olyan megbízható telefonszámon hívjuk fel őket, amit például a bankkártya hátoldalán vagy a számlaértesítőn találunk, vagy keressük fel a bank weboldalát egy megbízható számítógépről. Mindezeken túl fontoljuk meg a bankszámlánk zárolását is.

Vírusvédelem: Ha a vírusirtónk egy lehetséges fertőzött fájlról tájékoztat minket, hajtsuk végre a vírusirtó által javasolt lépéseket. A legtöbb vírusirtó olyan hivatkozásokat ajánl fel, amiket felkeresve többet is megtudhatunk az adott fertőzésről.

Újratelepítés: Ha nem tudjuk a fertőzött gépet megjavítani, vagy biztosak szeretnénk lenni abban, hogy a gépünk biztonságos, akkor telepítsük újra az operációs rendszert. Ne a biztonsági mentésből telepítsük újra, a biztonsági mentést inkább csak a személyes adataink helyreállítására használjuk. Ha bizonytalanok vagyunk az újratelepítéssel kapcsolatban, vegyünk igénybe szakszerviz segítségét. Abban az esetben, ha számítógépünk vagy bármilyen érintett eszközünk túl öreg, talán egyszerűbb egy újat vásárolnunk helyette. Végül, amint visszaállítottuk a rendszerünket, vagy beszereztük az újat, bizonyosodjunk meg arról, hogy a rendszer friss és naprakész, illetve mindig engedélyezzük az automatikus frissítést, amennyiben erre lehetőségünk van.

Biztonsági mentés: Önmagunk védelme érdekében kulcslépés, hogy időben felkészüljünk a rosszra azzal, hogy rendszeres biztonsági mentéseket készítünk. Sok megoldás létezik az automatikus, napi, vagy akár óránként lefutó biztonsági mentések elvégzésére. Függetlenül az általunk választott megoldástól, mindig ellenőrizzük, hogy képesek vagyunk -e az elmentett adatok visszaállítására. Nagyon gyakran a biztonsági mentés visszaállítása az egyetlen módja annak, hogy egy heckelés után minden adatunkat visszaszerezzük.

Bűnüldözés: Ha bármilyen mértékben is fenyegetve érezzük magunkat, jelentsük az esetet a helyi bűnüldöző szerveknek. Amennyiben az Amerikai Egyesült Államokban élünk és visszaélnek személyazonosságunkkal, látogassuk meg a https://www.identitytheft.gov oldalt.

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

Dr. Johannes Ullrich *(@johullrich) a SANS Technológiai Intézet kutatásért felelős dékánja, a SANS Internet Storm Center igazgatója és a SANS partnere. Életre hívta a DShield együttműködő szenzorhálózatot, illetve az Internet Storm Center napi podcastjának a házigazdai teendőit is ellátja.*

Hivatkozások

Biztonsági mentések:	https://www.sans.org/u/JGP
Jelmondatok:	https://www.sans.org/u/JGU
Jelszókezelők:	https://www.sans.org/u/JGZ
Mi a Malware:	https://www.sans.org/u/JH4
Bankszámla zárolása:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/