OUCH!

SANS SECURITY AWARENESS

Az Ön havi biztonságtudatossági hírlevele

Keressünk rá Magunkra

Áttekintés

Minden valószínűség szerint mindannyian hallottunk már arról, mennyire fontos, hogy megvédjük a magánéletünket és azon információkat, melyeket megosztunk online felületeken. Hogy ennek fontosságát bemutassuk, valami újjal próbálkozunk: megmutatjuk, hogy miként "kutathatjuk" fel Önmagunkat, és nézhetjük meg, hogy milyen publikus információk lelhetőek fel rólunk. Ezt az eljárást OSINT-nak nevezik, ami egy új, divatos elnevezése "Nyílt Forrású Információszerzésnek", avagy Open Source Intelligence-nek. Ez a módszer tulajdonképpen nyílt, online információk felkutatását jelenti, mely által láthatjuk, hogy mi minden tudható meg egy számítógép IP címe alapján egy cégről vagy akár egy személyről – akár Rólunk is. Ne feledjük, hogy a kiberbűnözők is ugyanezeket az eljárásokat és technikákat használják. Minél többet tudnak meg a támadók Rólunk, annál jobban elő tudnak készíteni egy célzott támadást ellenünk. Ez a koncepció, módszer már évek óta létezik, de a legújabb online eszközök immár sokkal könnyebbé teszik a végrehajtását.

Hogyan keressünk információt?

Nem fogunk minden információt egyetlen weboldalon megtalálni. Ahelyett, hogy egy adott weboldallal kezdenénk, keressünk pár információmorzsát, majd használjuk ezeket a részleteket a további keresésekhez, és szerezzünk más oldalakról még több információt. Ezt követően hasonlítsuk és össze az eredményeket és kombináljunk annak érdekében, hogy a keresésünk tárgyáról egy profilt vagy dossziét össze tudjunk állítani. Jó kiinduló pontok lehetnek a keresőmotorok, mint a Google, Bing vagy a DuckDuckGo. Mindegyik különböző információkat tárol el Rólunk, szóval a keresésünket több, mint egy motor használatával kezdjük. Kezdjük azzal, hogy a nevünket idézőjelekbe téve gépeljük a keresőbe. Ezt követően bővítsük a kereső kifejezést úgynevezett speciális operátorokkal. Az operátorok olyan speciális szimbólumok vagy szövegek, amik segítségével jobban le tudjuk írni a keresés során, hogy mit is keresünk pontosan. Ez különösen fontos, ha gyakori nevünk van, ekkor több kezdeti információ megadása válhat szükségessé, mint például az e-mail címünkre, vagy a város neve ahol élünk. Az operátorokról és a kereséséi technikákról bővebben olvashatunk a dokumentum végén lévő hivatkozások között. Példák a kereső kifejezésekre:

⚠

- **"Keresztnév Vezetéknév" > milyen információkat találhatok erről a személyről online**
- **"Keresztnév Vezetéknév@" > ehhez a személyhez köthető e-mail címek keresése**
- **"Keresztnév Vezetéknév" filetype:doc > bármilyen Word dokumentum, ami tartalmazza az adott személy nevét**

Vannak továbbá olyan oldalak is, melyek kifejezetten személyek felkutatásával foglalkoznak. Próbáljuk ki a lenti oldalak egyikét, hogy megnézzük, mi található meg Rólunk ezen módszerekkel. Tartsuk szem előtt, hogy ezek az oldalak nem mindig pontosak, illetve akár ország specifikusak is lehetnek. Lehet, hogy több oldalon kell keresést végezni ahhoz, hogy ellenőrizhessük, validálhassuk a máshol talált információkat.

- https://pipl.com
- https://cubib.com
- https://familytreenow.com

Végezetül, számos olyan oldal létezik, amely segítségével többet tudhatunk meg az emberekről, mint például a Google Images, Google Maps, Közösségi média oldalak, és még sok más. Javasoljuk az OSINT keretrendszer használatát, ami egy interaktív listát nyújt azokról a különböző weboldalakról, amiket használva további információkat szerezhetünk magunkról.

Miért keressünk rá Önmunkra?

1. **Azért,hogy megismerhessük, hogy más emberek, szervezetek milyen információkat gyűjtöttek össze, osztottak meg rólunk online (templom, iskola, sport klub, vagy más, helyi közösségi oldalakon).**
2. **Tartsuk szem előtt, hogy ezek az erőforrások bárki - a kiberbűnözők számára is- számára hozzáférhetőek, akik a megszerzett információkat akár ellenünk is felhasználhatják. Legyünk mindig gyanakvóak. Például ha egy sürgős hívást kapunk valakitől, aki azt állítja,hogy a bankunk az alkalmazottja, attól, hogy tud rólunk néhány alap információt, az még nem bizonyítja, hogy valóban a bankunk képviselője. Ilyenkor udvariasan szakítsuk meg a hívást, és keressük fel a bankunkat egy ismert, megbízható számon, melyen igazolni tudják, hogy valóban Ők kerestek minket. Ugyanez igaz az elektronikus levelekre is: csak azért, mert egy e-mail tartalmaz néhány alap információt rólunk, az még nem garancia arra, hogy a levél legitim.**
3. **Gondoljuk át, hogy mit osztunk meg publikusan Önmagunkról, és azt, hogy annak milyen hatása lehet ránk, a családunkra, vagy a munkáltatónkra.**

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

Niko Dekens *(@dutch_osintguy) a nyílt forráson alapuló felderítésre (OSINT) specializálódott. Kiber információszerzéssel és elemzéssel kel és fekszik, ez tölti ki minden egyes percét. Nico a Fortune 500 –as vállalatoknál és kormányzati szerveknél tart előadásokat OSINT, IoT és műveleti biztonság témakörökben.*

Hivatkozások

A pszichológiai manipuláció:	https://www.sans.org/u/LW6
Közösségi média top tippek:	https://www.sans.org/u/LWb
Kereső operátorok:	https://support.google.com/websearch/answer/2466433
OSINT keretrendszer:	https://osintframework.com/
SANS OSINT tanfolyam SEC487:	https://www.sans.org/u/LWZ