SANS SECURITY AWARENESS

OUCH!

Ikmēneša informācijas drošības izdevums Tev

Pārbaudiet informāciju par sevi tiešsaistē

Pārskats

Jūs droši vien esat dzirdējuši, cik svarīgi ir aizsargāt savu privātumu un informāciju, ar kuru dalāties tiešsaistē. Lai to nodemonstrētu, mēs izmēģināsim ko jaunu - mēs parādīsim, kā veikt izpēti par sevi un noskaidrot, kāda informācija par jums ir publiski pieejama. Gudrā vārdā šo procesu sauc par OSINT (Open Source Intelligence). Tas nozīmē veikt tīmeklī publiski pieejamu resursu izpēti, lai noskaidrotu, cik daudz informācijas jūs varat iegūt par datora IP adresi, uzņēmumu vai kādu personu, tādu kā jūs. Paturiet prātā, ka kiberuzbrucēji izmanto tādus pat rīkus un metodes. Jo vairāk uzbrucēji var uzzināt par jums, jo labāk viņi var pielāgot uzbrukumu. Šī metode ir sena, bet jaunākie tiešsaistes rīki ir padarījuši tās pielietošanu daudz vienkāršāku.

Kā informāciju atrast?

Jūs neatradīsiet visu informāciju vienā tīmekļa vietnē. Jūs sākat ar vienu tīmekļa vietni, noskaidrojat atsevišķas detaļas, tad izmantojat šīs jauniegūtās zināšanas, lai meklētu tālāk citās tīmekļa vietnēs. Tad jūs apvienojat un salīdzinat rezultātus, lai izveidotu jūsu pētāmā subjekta profilu vai dosjē. Labs sākumpunkts ir meklēšanas rīki, tādi kā Google, Bing vai DuckDuckGo. Katrs no tiem ir noindeksējis kādu atšķirīgu informāciju par jums, tāpēc sāciet savu izpēti, izmantojot vairāk nekā tikai vienu meklēšanas rīku. Sāciet ar sava vārda ierakstīšanu pēdiņās, bet pēcāk paplašiniet meklēšanu, pievienojot arī tā saucamos operatorus. Operatori ir speciālie simboli vai teksts, ko jūs varat pievienot jūsu meklētajam vārdam, lai labāk paskaidrotu, kas ir tas, ko meklējat. Tas ir īpaši noderīgi, ja jums ir plaši izplatīts vārds, tad var pievienot tādu papildinformāciju kā jūsu e-pasta adrese vai pilsēta, kurā dzīvojat. Iegūstiet vairāk informācijas par operatoriem un paplašinātās meklēšanas metodēm Resursu sadaļā raksta beigās. Daži piemēri:

- **“Vārds Uzvārds” > kādu informāciju es varu atrast tiešsaistē par šo personu**
- **“Vārds Uzvārds@” > atrast iespējamās e-pasta adreses, kas saistītas ar šo personu**
- **“Vārds uzvārds” filetype:doc > jebkurš Word dokuments, kas satur šīs personas vārdu**

Ir arī tīmekļa vietnes, kas ir radītas ar mērķi iegūt informāciju par cilvēkiem. Izmēģiniet kādu no šīm vietnēm, lai redzētu, kas par jums publiski ir zināms. Ņemiet vērā, ka šīs veitnes var būt kļūdainas vai var būt orientētas uz kādu konkrētu valsti. Jums var nākties pārbaudīt vairākas vietnes, lai pārliecinātos par atrastās informācijas patiesumu.

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

Un visbeidzot, ir virkne citu vietņu, kuras jūs varat izmantot, lai meklētu papildinformāciju, piemēram, Google Images, Google Maps, sociālie tīkli un citas. Interaktīvam dažādu vietņu sarakstam, kuras jūs varat izmantot, lai iegūtu informāciju par sevi, mēs iesakām OSINT ietvaru https://osintframework.com

Kāpēc meklēt informāciju par sevi tīmeklī?

1. **Uzziniet, ko citi cilvēki vai organizācijas ir uzkrājušas vai publicējušas par jums tīmeklī (skola, sporta klubs, baznīca vai cita aktivitāšu kopiena).**
2. **Saprotiet, ka šie paši resursi ir pieejami jebkuram citam, arī kibernoziedzniekiem, kas var izmantot šo informāciju, lai sagatavotu pret jums vērstus uzbrukumus. Esiet aizdomu pilni. Piemēram, ja jūs saņemat steidzamu telefona zvanu, kurā zvanītājs apgalvo, ka zvana no jūsu bankas, tikai tāpēc, ka viņš zina minimālu pamatinformāciju par jums, nebūt nenozīmē, ka viņš tiešām pārstāv banku. Pieklājīgi pārtrauciet sarunu, tad veiciet zvanu uz savu banku, izmantojot labi zināmu, uzticamu numuru, un pārliecinieties, ka viņi tiešām zvanīja. Tieši tāpat ar e-pastiem – tikai tāpēc, ka e-pasts satur kaut kādu par jums vispārzināmu informāciju nenozīmē, ka tas ir leģitīms.**
3. **Pārdomājiet, kādu informāciju jūs par sevi publicējat un kādu ietekmi tas var atstāt uz jums, jūsu ģimeni vai jūsu darba devēju.**

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Nico Dekens *(@dutch_osintguy) ir OSINT speciālists. Viņš dzīvo un elpo visu, kas saistīts ar kiberinformācijas vākšanu un analīzi. Nico lasa starptautiskas lekcijas par tādām tēmām kā OSINT, IoT un procesu drošība Fortune 500 kompānijās un valsts pārvaldē.*

Resursi

Sociālā inženierija:	https://www.sans.org/u/LW6
TOP ieteikumi sociālajiem medijiem:	https://www.sans.org/u/LWb
Meklēšanas rīku operatori:	https://support.google.com/websearch/answer/2466433
OSINT ietvars:	https://osintframework.com/
SANS OSINT kursi SEC487:	https://www.sans.org/u/LWZ

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: Edgars Tauriņš