

OUCH!

Det månedlige nyhedsbrev om IT-sikkerhed til dig

Find dig selv online

Oversigt

Du har højst sandsynligt hørt, hvor vigtigt det er at beskytte dit privatliv og de oplysninger, du deler online. For at demonstrere dette, skal vi prøve noget nyt. Vi skal vise dig, hvordan du selv undersøger og finder ud af, hvilke oplysninger, der er offentligt kendt om dig. Processen hedder OSINT, en fancy måde at sige "Open Source Intelligence". Det betyder at undersøge offentlige ressourcer for at se, hvor meget information, du kan finde om en computerens IP-adresse, en virksomhed eller endda en person som dig selv. Husk, at IT-kriminelle bruger de samme værktøjer og teknikker. Jo mere angribere kan lære om dig, desto bedre kan de skabe et målrettet angreb. Dette koncept har eksisteret i årevis, men de nyeste onlineværktøjer gør det så meget lettere.

Sådan finder du oplysninger

Du finder ikke alle oplysninger på et enkelt websted. Du skal begynde med et websted, her finder du nogle detaljer, som du så kan bruge til at finde flere oplysninger på andre websteder. Så samler og sammenligner du dine resultater for at oprette et dossier på dit emne. Et godt sted at starte er med søgemaskiner som Google, Bing eller DuckDuckGo. Hver af disse har indekseret forskellige oplysninger om dig, så brug mere end en søgemaskine. Start med at indtaste dit navn i citationstegn, men derefter skal udvide din søgning baseret på, hvad der kaldes "operators". Operators er specielle symboler eller tekst, du føjer til din søgning, der bedre definerer, hvad du leder efter. Dette er især vigtigt, hvis du har et almindeligt navn, så skal du muligvis tilføje flere oplysninger, f.eks. din e-mailadresse eller den by, du bor i. Lær mere om operators og avancerede søgeteknikker i afsnittet "hvis du vil vide mere" i slutningen af dette nyhedsbrev. Eksempler er:



- "Fornavn Efternavn"> Hvilke oplysninger kan jeg finde online om denne person
- "Fornavn Efternavn @"> Find mulige e-mailadresser tilknyttet denne person
- "Fornavn efternavn" filetype: doc> Eventuelle worddokumenter, der indeholder denne persons navn

Der er også websteder der er dedikeret til at lære om mennesker. Prøv et af disse websteder for at se, hvad, der er offentligt kendt om dig. Husk på, at disse websteder ikke altid er korrekte eller kan være landespecifikke. Du skal muligvis søge flere steder for at verificere de oplysninger, du finder.



- <https://pipl.com>
- <https://arkiv.dk>

Endelig er der mange andre websteder, du kan søge for at lære mere, f.eks. Google Billeder, Google Maps, Social Media-websteder og meget mere. For en interaktiv liste over alle de forskellige hjemmesider, du kan bruge til at lære om dig selv, anbefaler vi OSINT Framework på <https://osintframework.com>

Hvorfor bør du søge på dig selv online?



1. For at finde ud af, hvad andre folk eller organisationer har samlet, sendt eller delt om dig online (kirke, skoler, sportsklub eller andre lokalsamfundssider)
2. For at forstå, at disse samme ressourcer er tilgængelige for andre, herunder IT-kriminelle, der kan bruge disse oplysninger til at lave målrettede angreb mod dig. Vær mistænkelig, for eksempel, hvis du får et presserende telefonopkald fra en person, der hævder at være din bank. Selvom de har nogle grundlæggende oplysninger om dig, det er ikke nødvendigvis din bank. Du skal høfligt afslutte samtalen og så ringe til din bank på et kendt, betroet nummer for at bekræfte, at det er dem. Det samme med e-mail, bare fordi en e-mail har nogle kendte fakta om dig, betyder ikke, at det er legitimt.
3. For at overveje, hvad du deler offentligt, og hvilken indflydelse oplysningerne kan have på dig, din familie eller din arbejdsgiver.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på <https://www.welcomesecurity.net>.

Gæsteredaktør

Nico Dekens (@dutch_osintguy) er specialiseret i OSINT. Han lever og ånder for alt, hvad der har at gøre med indsamling og analyse af informationer på internettet. Nico er international underviser på emner som OSINT, IoT og "Operations Security" hos Fortune 500 virksomheder og regeringer.



Hvis du vil vide mere

- Social Engineering: <https://www.sans.org/u/LW6>
Top Tips for Social Media: <https://www.sans.org/u/LWb>
Search Engine Operators: <https://support.google.com/websearch/answer/2466433>
OSINT Framework: <https://osintframework.com/>
SANS OSINT Course SEC487: <https://www.sans.org/u/LWZ>

OUCH! er udgivet af SANS Security Awareness og distribueres under [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Du er velkommen til at videregive dette nyhedsbrev eller bruge det i dit eget arbejde med IT-sikkerhed så længe du ikke ændrer i nyhedsbrevet. Hvis du har spørgsmål til oversættelsen eller andet er du velkommen til at kontakte www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity