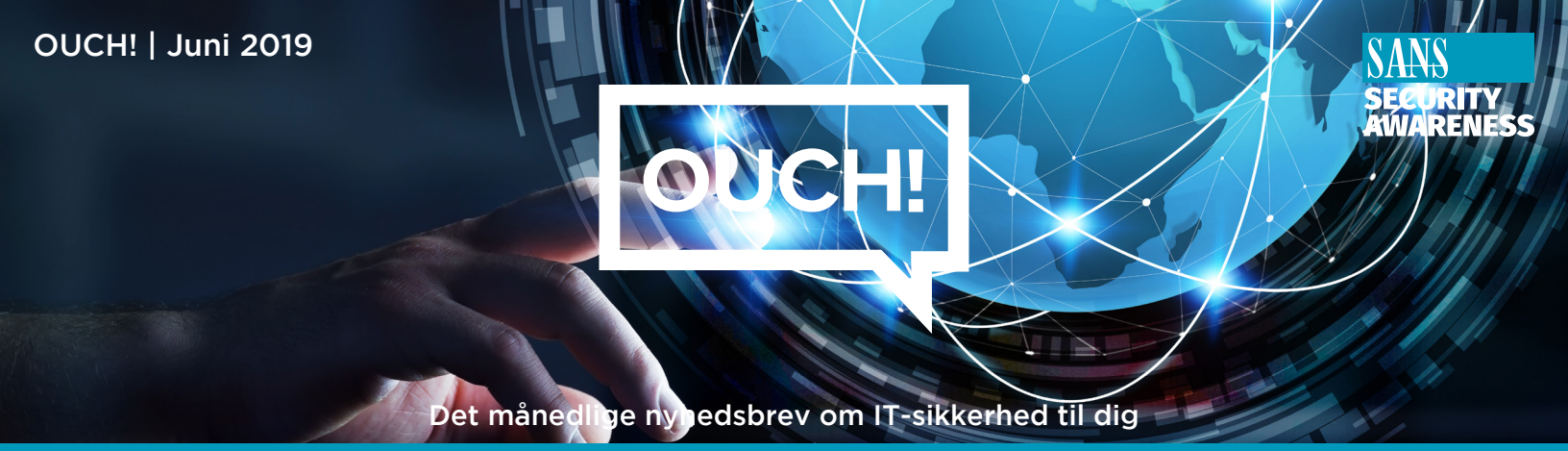

Det månedlige nyhedsbrev om IT-sikkerhed til dig

"Dark Web"

Overblik

Du har måske hørt betegnelsen "Dark Web", blive brugt af andre eller i medierne, og spekulerede på "*Hvad er Dark Web?*" Eller "*skal jeg gøre noget ved det?*". I dag forklarer vi, hvad "Dark Web" er, og hvad det betyder for dig.

Hvad er det?

"Dark Web" består af systemer på internettet designet til at kommunikere eller dele information sikkert og anonymt. Der er ikke et enkelt "Dark Web"; det er ikke som Facebook, der drives af en enkelt organisation. I stedet er "Dark Web" en samling af forskellige systemer og netværk, der forvaltes af forskellige mennesker, der anvender det til forskellige formål. Disse systemer er stadig forbundet med og er en del af internettet, men du vil generelt ikke finde dem ved hjælp af dine normale søgemaskiner. Du har ofte brug for speciel software på din computer for at finde eller få adgang til dem. Et eksempel er Tor projektet. For at få adgang til dette "Dark Web", skal du downloade og installere en Tor browser. Når du opretter forbindelse til webserverne ved hjælp af Tor browseren, bevæger din krypterede trafik sig gennem andre computere der også bruger Tor. Når du med denne browser hopper gennem disse mange computere, ændres kilde-IP-adressen, hvilket betyder, at når du kommer til webstedet, er din onlineaktivitet anonymiseret. Andre eksempler på "Dark Webs" omfatter Zeronet, Freenet og I2P.

Hvem bruger det?

IT-kriminelle er store forbrugere af "Dark Web". De opretholder websteder og fora i "Dark Web" for at håndtere deres kriminelle aktiviteter som at købe stoffer eller sælge gigabyte af hackede data - alt anonymt og sikkert. For eksempel, når en IT-kriminel hacker en bank eller en online-butik, stjæler de så mange oplysninger som muligt og sælger disse oplysninger til andre IT-kriminelle på websteder på "Dark Web".

Der er også legitime anvendelser af "Dark Web". For eksempel kan mennesker i lande, hvor der er censur, bruge "Dark Web" netværk til at dele information og se, hvad der sker i verden samtidig med at de beskytter deres privatliv og forbliver anonyme.

Journalister, whistleblowers og personer, der vil bevare deres privatliv, kan bruge "Dark" Web til at øge deres anonymitet og omgå censur. Med teknologier som Tor har man ikke blot adgang til "Dark Web", men man kan anonymt browse det almindelige internet.

Hvad skal jeg gøre?

Medmindre du har en særlig grund til at besøge "Dark Web", advarer vi dig imod det. Nogle "Dark Web" websteder bruges til ulovlige formål, mange af webstederne bruger din computer i et peer-netværk for at nå deres mål, og i nogle tilfælde kan computeren endda blive testet eller angrebet. Nogle virksomheder tilbyder overvågningstjenester for at fortælle dig, om dit navn eller andre oplysninger er blevet stjålet af IT-kriminelle og fundet på "Dark Web". Den faktiske værdi af disse tjenester er tvivlsom. Den bedste måde at beskytte dig på er at antage, at nogle af dine oplysninger allerede findes på "Dark Web" og bruges af de IT-kriminelle. Som resultat . . .

⚠

- **Vær mistænkelig overfor alle telefonopkald eller e-mails, som foregiver at være officielle organisationer, og presser dig til at gøre noget, som at betale en bøde. Kriminelle kan endda bruge oplysninger, som de har fundet om dig, til at skabe personlige angreb.**
- **Tjek dit kreditkort- og kontoudtog. Måske kan du endda oprette daglige advarsler om eventuelle transaktioner. På den måde kan du opdage, om der sker økonomisk svindel. Hvis du registrerer det, skal du rapportere det til dit kreditkortselskab eller bank med det samme.**

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

Micah Hoffman *(@WebBreacher) er "Principal Investigator" på Spotlight Infosec LLC, er certificeret SANS Institut instruktør og forfatteren til SANS OSINT kurser. Micas passion for cyber og "open source intelligence" skinner igennem i hans projekter, kursusmateriale og undervisning.*

Hvis du vil vide mere

Personificeret Angreb:	https://www.sans.org/u/RfW
Social Engineering:	https://www.sans.org/u/Rg1
Identitets Tyveri:	https://www.identitytheft.gov
Tor browser:	https://www.torproject.org/
SANS OSINT Course:	https://sans.org/sec487