OUCH! | Januar 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Hvad er Social Engineering?
- Hvordan opdager og stopper man et Social Engineering angreb?

# Social Engineering

## Overblik

En gængs misforståelse om IT-kriminelle er, at de kun benytter sig af meget avancerede værktøjer og teknikker til at bryde ind i folks computere eller online konti. Dette er langt fra sandheden. IT-kriminelle har lært, at den letteste måde at stjæle information, hacke din computer eller online konti er ved at snyde dig til at lave en fejl. I dette nyhedsbrev kan du læse om, hvordan disse angreb, som man kalder ”Social Engineering”, fungerer samt hvad du kan gøre for at beskytte dig selv.

### Gæsteredaktør

James Lyne (**@jameslyne**) er certificeret SANS instructor og Global Head of Research ved Sophos. Han analyserer de nyeste tiltag fra IT-kriminelle. Han er forfatter til “Metasploit (SEC580)” og ”Social Engineering (SEC567)” kurserne ved SANS.

## Hvad er Social Engineering?

Social Engineering er et psykologisk angreb, hvor en angriber snyder dig til at gøre noget, du ikke burde gøre. Social Engineering er ikke et nyt koncept. Det har eksisteret i flere tusind år. Tænk blot på svindlere og trick kunstnere. Nutidens teknologi gør angrebene mere effektive, fordi du ikke kan se de IT-kriminelle. De har let ved at lade som om, de er en anden person, end de er, samtidig kan de ramme flere millioner over hele kloden, inklusive dig. Oveni dette kan angreb, der benytter sig af Social Engineering, slippe gennem mange sikkerheds teknologier. Den letteste måde at få forståelse for, hvordan angrebene virker, og hvordan du kan beskytte dig mod dem, er ved at tage udgangspunkt i to eksempler fra den virkelig verden.

Du modtager et telefonopkald fra en, der udgiver sig for at være fra en IT-support virksomhed, din internetudbyder eller måske Microsoft Tech Support. Personen forklarer dig, at din computer er i gang med at scanne internettet, og de tror, den er ramt at en virus. De har fået til opgave at hjælpe dig med at sikre din computer. I samtalen bruger de en masse tekniske begreber, og forvirrer dig for at overbevise dig om at din computer er inficeret. De kan eksempelvis spørge dig, om du har nogle bestemte filer på din computer. Herefter hjælper de dig med at finde dem. Når du har fundet filerne overbeviser de dig om, at det er et bevis på, at din computer er ramt. I virkeligheden er det helt almindelige systemfiler som findes på næsten alle computere. Når først du er overbevist om, at din computer er inficeret, presser de dig til at købe deres sikkerhedssoftware

## Social Engineering

eller til at give dem fjernkontrol over din computer, så de kan ordne problemet. Imidlertid er det program, de sælger dig, ondsindet. Hvis du køber og installerer deres program, har de ikke kun inficeret din computer, du har også betalt dem for at gøre det.

Et andet eksempel er et e-mail angreb, der kaldes CEO svindel, dette finder oftest sted på din arbejdsplads. Ved denne type angreb undersøger de IT-kriminelle din arbejdsplads online, og finder navnene på din chef og dine kollegaer. Den IT-kriminelle skriver herefter en e-mail til dig, hvor han udgiver sig for at være denne person. I e-mailen bliver du presset til at gøre et eller andet, eksempelvis at overføre penge eller sende følsomme informationer om medarbejdere. Mailen giver ofte udtryk for, at der er tale om en nødsituation og du presses til at gå udenom de normale sikkerhedsprocedurer. Du kan også blive bedt om at sende meget følsomme informationer til en personlig @ gmail.com konto. Det, der gør denne type angreb farlige, er at de IT-kriminelle har undersøgt virksomheden grundigt. Sikkerhedsteknologier som anti-virusprogrammer og firewalls kan ikke identificere eller stoppe disse angreb, fordi der ikke er involveret ondsindet software eller links.


*Sund fornuft er dit bedste forsvar til at identificere og stoppe de fleste Social Engineering angreb.*

Du skal være opmærksom på, at Social Engineering angreb ikke er begrænset til telefonopkald eller e-mail, de kan også være tekstbeskeder på din telefon, over sociale medier eller fra en person. Nøglen, til at undgå at blive snydt, er at vide, hvad man skal kigge efter. Du er dit eget bedste forsvar.

## Hvordan opdager og stopper man et Social Engineering angreb?

Heldigvis er det lettere at stoppe disse angreb end man skulle tro, almindelig sund fornuft er dit bedste forsvar. Hvis der er noget, der virker mistænkeligt eller ikke føles rigtig, kan det være et angreb. De mest almindelige tegn på at det er et social engineering angreb er:

- En person skaber et indtryk af at det er en presset situation, han prøver at snyde dig til at lave en fejl.
- En person spørger om information, som personen ikke burde have adgang til eller som personen allerede har, så som dit kontonummer.

## Social Engineering

- En person spørger om dit password, ingen lovlig organisation vil nogensinde spørge dig om det.
- En person presser dig til at bryde de almindelige sikkerhedsprocedurer du er forventet at følge på dit arbejde.
- Noget er for godt til at være sand. Eksempelvis, hvis du bliver orienteret om, at du har vundet i lotto, selvom du ikke har deltaget.
- Du modtager en underlig e-mail fra en ven eller kollega, der er skrevet i et andet sprog end det plejer. Det kan være en IT-kriminel, der har hacket deres konto og prøver at snyde dig. For at passe på dig selv kan du få indholdet bekræftet ved at bruge en anden kommunikationsmetode så som ansigt til ansigt eller over telefonen

Hvis du mistænker nogen for at prøve at snyde dig skal du stoppe al kommunikation med personen. Hvis angrebet er arbejdsrelateret skal du informere din leder med det samme. Husk sund fornuft er ofte dit bedste forsvar.

## Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

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.

## Tidligere udgivelser

| | |
|---|---|
| Phishing: | https://securingthehuman.sans.org/ouch/2015#december2015 |
| CEO svindel (oversat til dansk): | https://securingthehuman.sans.org/ouch/2016#july2016 |
| Ransomware (oversat til dansk): | https://securingthehuman.sans.org/ouch/2016#august2016 |
| OUCH Archives: | https://securingthehuman.sans.org/ouch/archives |

## Licensinformation



Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus