OUCH! | Januari 2017

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wat is Social Engineering**
- **Social Engineering Aanvallen Herkennen en Stoppen**

Social Engineering

Overzicht

Veel mensen maken de misvatting dat cybercriminelen enkel geavanceerde hacking tools en technologieën gebruiken om binnen te breken in computers of accounts. Dit is echter niet waar. Cyberaanvallers proberen je te misleiden zodat je een fout maakt, dit is de makkelijkste en snelste methode om jouw informatie te stelen, accounts te hacken of systemen te besmetten. In deze nieuwsbrief leer je hoe je zulke aanvallen, ook wel social engineering genoemd, werken en hoe je jezelf ertegen kan verdedigen.

Gast redacteur

James Lyne (**@jameslyne**) is een gecertifieerde SANS-instructeur en Global Head of Research bij Sophos. Hij ontleedt en 'reverse engineert' de nieuwste en beste creaties van cybercriminelen. Hij is auteur van de SANS-cursussen Metasploit (SEC580) en Social Engineering (SEC567).

Wat is Social Engineering

Social engineering is een pyschologische aanval waarbij een aanvaller je misleidt om iets te doen wat je niet zou mogen doen. Het concept social engineering is niet nieuw, het bestaat al sinds duizenden jaren. Net zoals oplichters en fraudeurs gaan ze gelijkaardig te werk. De huidige technologie maakt het makkelijk voor cybercriminelen omdat je ze niet fysiek ziet, zo kunnen ze zich makkelijk voordoen als iemand anders en eenvoudig miljoenen mensen bereiken over de hele wereld, waaronder jij. Daarenboven kunnen social engineering aanvallen veel security technologieën omzeilen. De makkelijkste manier om deze aanvallen te begrijpen en hoe je jezelf ertegen kan verdedigen, is door twee praktijkvoorbeelden te bekijken.

Je ontvangt een telefoontje van iemand die zich uitgeeft als een medewerker van een computerondersteuningsbedrijf, zoals jouw internetprovider of Microsoft Tech Support. De beller vertelt dat jouw computer actief het Internet scant, waardoor hij vermoedt dat jouw computer besmet is. De beller heeft zogezegd de taak om jouw computer te herstellen en beter te beveiligen. De beller imponeert je met verschillende technische begrippen en laat je verschillende acties uitvoeren om je te overtuigen dat jouw computer besmet is. Zo vraagt men dat je zoekt naar bepaalde bestanden op jouw computer en begeleiden ze je om deze te vinden. Wanneer je de bestanden hebt gevonden, overtuigt de beller je ervan dat de computer besmet is. Deze bestanden zijn echter standaard systeembestanden die je op iedere computer zal terugvinden. Eens ze je doen geloven dat jouw computer besmet is, dan oefent de beller druk uit zodat je security software koopt of vragen ze dat je hen toegang vanop afstand geeft om jouw computer te kunnen herstellen. In werkelijkheid verkoopt hij schadelijke software. Als je het aankoopt en installeert, ben je niet enkel misleid maar heb je ook jouw computer besmet

Social Engineering

en er ook nog voor betaald. Geef je hen toegang vanop afstand tot jouw computer, dan nemen ze de computer over en stelen ze jouw informatie.

Gezond verstand is de beste verdediging om de meeste social engineering aanvallen te herkennen en te stoppen.

Een ander voorbeeld van een aanval via e-mail is CEO-fraude, dat meestal op het werk gebeurt. Hier zal een cyberaanvaller jouw organisatie online onderzoeken en de naam van jouw collega of baas opzoeken. Vervolgens maakt de aanvaller een valse e-mail, onder naam van jouw collega of baas en richt deze aan jou. De e-mail vraagt om een dringende actie zoals het uitvoeren van een banktransfer of het e-mailen van vertrouwelijke informatie van bepaalde medewerkers. In de e-mail is er sprake van een noodgeval waardoor er een uitzondering is vereist op de normale security procedures, zo kan men vragen om de vertrouwelijke informatie door te sturen naar een persoonlijk @gmail.com adres. Wat deze soort van aanvallen zo gevaarlijk maakt, is dat men een grondig onderzoek heeft uitgevoerd op voorhand. Security technologieën zoals firewalls of antivirus kunnen dit niet herkennen of stoppen omdat er geen malware of schadelijke bijlages zijn toegevoegd aan het bericht.

Onthoud goed dat social engineering aanvallen niet alleen via telefoon of e-mail plaatsvinden. Ze kunnen ook gebeuren via SMS-berichten, berichten op social media of zelfs in het echte leven. Het is belangrijk dat je weet waarop je moet letten, jezelf en jouw gezond verstand vormen hier de beste verdediging.

Social Engineering Aanvallen Herkennen en Stoppen

Gelukkig kan je deze aanvallen makkelijk stoppen –jouw gezond verstand is hier de beste verdediging. Lijkt er iets verdacht of niet juist, dan is het meestal een aanval. De meest voorkomende tekenen van een social engineering aanval zijn:

- Iemand die heel dringend iets nodig heeft. Hier probeert men jou te misleiden om jou een fout te laten maken.
- Iemand vraagt informatie waartoe men geen toegang heeft of reeds zou moeten weten, zoals jouw bankgegevens.
- Iemand vraagt om jouw wachtwoord, geen enkele echte organisatie zal hierachter vragen.
- Iemand zet jou onder druk om security processen of procedures te omzeilen of negeren, die je zou moeten volgen.
- Iets wat té mooi is om waar te zijn. Bijvoorbeeld je krijgt een melding dat je de loterij of een iPad hebt gewonnen, ook al heb je nooit deelgenomen.

Social Engineering

- Je ontvangt een rare e-mail van een vriend of collega. Het taalgebruik komt niet overeen met die van de persoon. Mogelijk heeft er hier een cyberaanvaller zijn account gehackt en probeert men jou te misleiden. Hier kan je best jouw vriend contacteren via een ander communicatiekanaal. Ga even langs bij jouw vriend of gebruik de telefoon om na te gaan of hij het bericht heeft verstuurd.

Als je vermoedt dat iemand jou wil misleiden, reageer er dan verder niet op. Vind de aanval plaats op het werk, rapporteer het dan meteen aan de helpdesk of aan jouw informatiebeveiligingsteam. Onthoud dat jouw gezond verstand vaak de beste verdediging is.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Phishing:	https://securingthehuman.sans.org/ouch/2016#january2016
CEO Fraud:	https://securingthehuman.sans.org/ouch/2015#august2015
Ransomware:	https://sans.org/for585
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives
Leer valse mails herkennen:	https://www.safeonweb.be/nl/node/553/139
Hoe herken ik een nepmail:	https://veiliginternetten.nl/themes/situatie/hoe-herken-ik-een-nepmail/
Fraude helpdesk:	https://www.fraudehelpdesk.nl/

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Vertaald door: Sven Jacobs, Tom Palmaers