OUCH! | November 2014

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Social Engineering**
- **Social Engineering Aanvallen Detecteren/Stoppen**
- **Verdere Aanvallen Voorkomen**

Social Engineering

Overzicht

Een veelvoorkomende misvatting dat mensen hebben over cyberaanvallers is dat ze enkel geavanceerde hacking tools en technologieën zouden gebruiken om binnen te breken in computers, accounts en mobiele toestellen. Dit is echter niet waar. Cyberaanvallers hebben geleerd dat jou te misleiden door met jou te praten, één van simpelste manieren is om jouw informatie te stelen of computer te hacken. In deze nieuwsbrief leren we hoe deze menselijke aanvallen, genaamd social engineering aanvallen, werken en hoe je jezelf ertegen kan verdedigen.

Gastredacteur

Alissa Torres is een gecertifieerde SANS-instructeur, gespecialiseerd in gevorderde computer forensics en incident response. Haar ervaring in de industrie omvat het dienen in de frontlinies als incident handler en als digitaal forensisch onderzoekster bij een intern security team. Alissa is ook actief op Twiter als **@sibertor**.

Social Engineering

Social engineering is een type van een psychologische aanval waar de aanvaller jou misleidt om iets te doen. Social engineering bestaat al sinds duizenden jaren, het idee om iemand te misleiden of op te lichten is niet nieuw. Cyberaanvallers weten intussen dat deze techniek zeer doeltreffend is op het Internet en makkelijk gebruikt kan worden om miljoenen mensen te treffen. De eenvoudigste manier om social engineering te begrijpen is door een aantal echte en veelvoorkomende voorbeelden te overlopen.

Je ontvangt een telefoontje van iemand die zich uitgeeft als iemand die voor een computerondersteuningsbedrijf werkt, zoals bv. jouw ISP of misschien zelfs de technische dienst van Microsoft. De beller legt uit dat ze merken dat jouw computer vreemde activiteiten uitvoert, zoals het scannen van het Internet of het versturen van spam, hierdoor geloven ze dat jouw computer mogelijk geïnfecteerd is. Ze hebben de opdracht om het probleem te onderzoeken en zullen je helpen om jouw computer te beveiligen. Dit doen ze door je te overladen met verschillende technische begrippen en door je verwarrende zaken te laten uitvoeren om je uiteindelijk te doen geloven dat jouw computer geïnfecteerd is.

Bijvoorbeeld, ze vragen je om te kijken of je bepaalde bestanden hebt op jouw computer en begeleiden je hoe je deze kan vinden. Wanneer je deze bestanden vindt, zal de beller je doen geloven dat deze bestanden een indicatie zijn van een infectie, maar in realiteit zijn deze bestanden niet meer dan gewone systeembestanden die je terugvindt op iedere computer. Eens ze je doen geloven dat jouw computer geïnfecteerd is, dan zullen ze druk uitoefenen om naar een website te gaan en hun security software te kopen of ze vragen dat je toegang vanop afstand aan hen geeft tot jouw computer om zogezegd de infectie te herstellen. In werkelijkheid verkopen ze een schadelijke toepassing. Indien je het aankoopt en de

Social Engineering

software installeert, hebben ze jou niet enkel misleidt, maar heb je hen er ook voor betaald. Indien je hen toegang vanop afstand geeft om het te herstellen, zullen ze de computer overnemen en infecteren.

Onthoud dat social engineering aanvallen niet enkel via telefoongesprekken worden gevoerd, ze kunnen ook voorkomen met bijna elke andere technologie. Zoals phishing aanvallen via e-mail, tekstberichten, Facebook berichten, Twitter posts of zelfs online chatgesprekken. Belangrijk is dat je weet waarvoor je moet oppassen.

Leren hoe je een social engineering aanval kan voorkomen, herkennen en stoppen, is één van de meest effectieve stappen die je kan nemen om jezelf te beschermen.

Social Engineering Aanvallen Detecteren/Stoppen

De eenvoudigste manier om je te verdedigen tegen social engineering aanvallen is door je gezond verstand te gebruiken. Als er iets verdacht lijkt of niet goed aanvoelt, dan is het mogelijk een aanval. Algemene indicatoren van een social engineering aanval zijn:

- Iemand die iets heel dringends nodig heeft. Als je voelt dat je onder druk wordt gezet om snel te beslissen, wees dan op je hoede.
- Iemand die vraagt om informatie waartoe ze normaal geen toegang tot hebben of reeds zouden moeten weten.
- Iets wat te mooi is om waar te zijn. Een veelvoorkomend voorbeeld is wanneer je een melding ontvangt dat je de loterij hebt gewonnen, zelfs als je niet hebt meegedaan.

Indien je vermoedt dat iemand een social engineering aanval op je uitvoert, reageer dan niet meer op de persoon. Als iemand je belt, hang dan gewoon op. Als iemand met jou online chat, verbreek dan de verbinding. Is er een verdachte e-mail, verwijder deze dan. Als de aanval plaatsvindt op je werk, rapporteer deze dan meteen aan de helpdesk of aan jouw informatiebeveiligingsteam.

Verdere social engineering aanvallen voorkomen

Gelukkig zijn er voorzorgsmaatregelen die je kan nemen om te voorkomen dat je nog social engineering aanvallen ontvangt:

- **Deel nooit wachtwoorden**: geen enkele organisatie zal je ooit contacteren met de vraag om jouw wachtwoord te delen. Indien iemand om jouw wachtwoord vraagt, dan betreft het een aanval.

- **Deel niet te veel**: Hoe meer een aanvaller over je weet, hoe makkelijker het voor hem is om je te vinden en je te misleiden om je iets te laten doen. Zelfs het delen van onschuldige details over jezelf doorheen de tijd, kan

Social Engineering

bruikbare informatie zijn om een compleet beeld van jou te vormen. Hoe minder je publiek deelt op sociale media sites, via productrecensies of berichten op publieke fora en maillijsten, des te minder kans je hebt op een aanval.

- **Verifieer contactpersonen**: Je kan mogelijk worden opgebeld door jouw bank, creditcardmaatschappij, gsm-provider of door andere organisaties omwille van legitieme redenen. Als je twijfelt of het verzoek legitiem is, vraag dan achter de naam van de contactpersoon en zijn of haar toestelnummer. Raadpleeg dan een betrouwbare bron om het officieel telefoonnummer van de organisatie op te zoeken, zoals bijvoorbeeld het nummer op de achterkant van jouw kredietkaart, het nummer op bankafschriften, of het nummer op de website van de organisatie (geef in dit geval zelf de URL in, in jouw browser). Wanneer je de organisatie dan belt, ben je zeker dat je de echte organisatie aan de lijn hebt. Dit lijkt omslachtig maar deze stap is het waard om jouw identiteit en persoonlijke gegevens te beschermen.

Meer Weten?

Ga naar http://www.securingthehuman.org 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)

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Social Networking Safely:	http://www.securingthehuman.org/ouch/2013#march2013
Avoid Scams:	http://www.onguardonline.gov/topics/avoid-scams

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