OUCH! | Juli 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wat is CEO-fraude?**
- **Jezelf Beschermen**

CEO-fraude

Wat is CEO-fraude?

Cybercriminelen zijn zeer sluw – ze zijn continu op zoek naar nieuwe methodes om te krijgen wat ze willen. Een van hun meest doeltreffende methodes is om mensen zoals jou te viseren. Cyberaanvallers weten dat mensen de zwakste schakel zijn in elke organisatie, maar ze vergeten dat getrainde mensen -zoals de lezers van OUCH!- net de beste verdediging zijn.

Gast redacteur

Angela Pappas is directrice van information security training en awareness bij Thomson Reuters. Angela is verantwoordelijk voor het ambassadeurprogramma, eLearning en het opleiden van medewerkers over het onderwerp phishing.

Cybercriminelen hebben een methode ontwikkeld die men CEO-fraude noemt. Hier doet de cybercrimineel zich voor als de CEO of als een ander directielid van jouw organisatie. De criminelen sturen een e-mail naar medewerkers zoals jou om je iets te laten doen wat je eigenlijk niet mag doen. Deze methode is zeer efficiënt aangezien de cybercriminelen dit nauwgezet voorbereiden. Ze doorzoeken de informatie op de website door te kijken naar de locatie waar men zich bevindt, wie de directieleden zijn en met welke organisaties er wordt gewerkt. Cybercriminelen gebruiken ook sites als LinkedIn, Facebook of Twitter om meer te leren over jouw collega's. Eens ze de organisatiestructuur hebben verkend, zullen ze bepaalde medewerkers gaan onderzoeken en viseren als doelwit. Ze kiezen het doelwit in functie van hun missie. Zijn ze op zoek naar geld, dan kijkt men naar de medewerkers binnen de dienst boekhouding. Is men op zoek naar belastingsinformatie, dan is de personeelsdienst het doel. Willen ze toegang tot de databases dan is IT het slachtoffer.

Eens ze hebben wat ze willen en weten wie het doelwit is, begint de aanval. De meest gebruikte methode is spear phishing. Phishing is een aanvaller die een e-mail stuurt naar miljoenen mensen met als doel om hen om de tuin te leiden en een actie te laten uitvoeren, zoals het openen van een besmette bijlage of het bezoeken van een schadelijke website. Spear phishing is net zoals phishing, alleen wordt de mail naar een select groepje van mensen verstuurd. Deze mails zien er zeer realistisch uit en zijn moeilijk om te herkennen. Ze komen vaak van mensen die je kent of met wie je samenwerkt, zoals een collega of zelfs jouw baas. Deze mails zien er echt uit en bevatten vaak hetzelfde

CEO-fraude

jargon dat ook door jouw collega's wordt gebruikt. Of bevatten het logo van de organisatie of zelfs de officiële handtekening van een directeur. Deze mails creëren vaak een gevoel van urgentie, waarbij er wordt gevraagd om onmiddellijk actie te ondernemen en tegen niemand iets te vertellen. Het doel van de cybercrimineel is om jou snel een vergissing te laten maken. Hier zijn enkele veel voorkomende scenario's:

CEO-fraude is een krachtige aanval die de meeste verdedingsmiddelen omzeilt. Uiteindelijk ben jij onze beste verdediging.

- **Bankoverschrijving**: Hier is men uit op geld. De cybercrimineel onderzoekt wie er bij de boekhouding werkt of bij de afdeling Financiën. Er wordt een mail verstuurd van de zogezegde baas, die meldt dat er een dringend geval is en dat er meteen geld moet worden gestort op een bepaalde rekening.

- **Belastingsfraude**: Cybercriminelen willen informatie stelen over de medewerkers van een organisatie om aan belastingsfraude te doen. Ze gaan na wie er in de organisatie omgaat met personeelsinformatie, bijvoorbeeld iemand binnen de personeelsdienst. Daarna sturen de cybercriminelen e-mails die in naam zijn van directieleden of iemand van de juridische dienst, om bepaalde documenten meteen te bezorgen.

- **Imitatie**: Niet alleen e-mail wordt gebruikt bij CEO-fraude, andere middelen als de telefoon kunnen ook worden ingezet. Een cybercrimineel zal jou eerst een mail sturen waarbij hij doet alsof hij directielid is en meldt dat een advocaat jou zal contacteren in verband een dringende zaak. Wat later ontvang je een telefoon van een crimineel die zich uitgeeft als de advocaat. Deze 'advocaat' creëert dan een gevoel van urgentie, omdat het gaat over een gevoelige kwestie die spoedig moet worden afgehandeld. Hierdoor zal je geneigd zijn om snel te handelen.

Jezelf Beschermen

Wat kan je doen om jezelf en jouw organisatie te beschermen? Jouw gezond verstand is de beste verdediging. Indien je een bericht van jouw baas of van een collega ontvangt en het klinkt verdacht, dan is het mogelijk een aanval. Let op zaken als een gevoel van urgentie, een handtekening die er vals uitziet, of een bepaalde toon die je niet verwacht, of een

CEO-fraude

naam in het bericht die verschilt van de persoon die jou contacteert. Een andere indicatie is dat de aanvaller een onbekend e-mailadres of telefoonnummer gebruikt of een e-mailadres dat lijkt op dat van jouw baas of collega. Als je twijfelt, neem dan contact op met de persoon (antwoord niet via e-mail) of ga even langs en ga na of hij de mail heeft verzonden. Volg altijd de security policies of procedures. Jouw organisatie heeft wellicht procedures rond het goedkeuren van betalingen of het delen van vertrouwelijke informatie. Wordt er gevraagd om af te wijken van deze procedures, ongeacht wie de aanvrager is, dien je voorzichtig te zijn en eerst te verifiëren vooraleer je actie onderneemt. Twijfel je, neem dan contact op met jouw leidinggevende, de helpdesk of het informatieveiligheidsteam.

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)

Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip of the Day:	https://www.sans.org/tip-of-the-day

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