OUCH! | December 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Overzicht
- Phishing
- Jezelf Beschermen

Phishing

Overzicht

E-mail is een van de belangrijkste manieren waarmee we communiceren. We gebruiken het niet alleen dagelijks op het werk, maar ook om contact te houden met onze vrienden en familie. Tevens gebruiken bedrijven e-mail om hun online diensten aan te bieden of te ondersteunen. Zo zijn er bijvoorbeeld e-mails die jouw online aankopen bevestigen. Of worden e-mailmeldingen gebruikt om aan te geven dat er nieuwe bankafschriften beschikbaar zijn. Net omdat e-mail zo ingeburgerd is bij veel mensen, is het één van de belangrijkste aanvalsmethodes van een cybercrimineel. In deze nieuwsbrief gaan we dieper in op phishing, dit is een veel gebruikte aanvalsmethode via e-mail en leggen we uit welke stappen je kan ondernemen om e-mail op een veilige manier te gebruiken.

Gast redacteur

Dr. Lance Hayden is een managing director bij Berkeley Research Group. Hij is een expert op het gebied van security cultuur en gedrag. Hij is auteur van het boek “People-Centric Security: Transforming Your Enterprise Security Culture” bij uitgeverij McGraw-Hill. Je kan hem vinden op **www.linkedin.com/in/drhayden**.

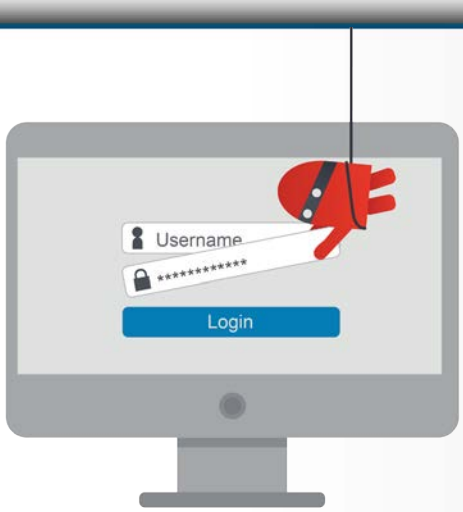
Phishing

Phishing verwijst naar een aanvalstactiek, dat met behulp van een e-mail of een social media bericht wordt uitgevoerd. Men wil je misleiden of overtuigen om een handeling uit te voeren. Zoals het klikken van een link of het openen van een bijlage. Als je het slachtoffer wordt van zo’n aanval, riskeer je dat jouw gevoelige informatie wordt gestolen en dat jouw computer wordt besmet. Aanvallers doen hun uiterste best om je te overtuigen met hun e-mails. Zo zullen ze bijvoorbeeld doen alsof de e-mail van iemand anders komt die je kent of herkenbaar is, zoals een vriend of een bekende onderneming. Er worden zelfs logo’s van jouw bank gebruikt of ze vervalsen het e-mailadres zodat het er zo echt mogelijk uitziet. Daarna versturen de aanvallers de phishing e-mails naar miljoenen mensen. Phishing is zoals vissen met een net, je weet op voorhand niet wat je zal vangen maar hoe groter het net des te meer vissen je zal vangen. Aanvallers gebruiken phishing op verschillende manieren om te krijgen wat ze willen.

- **Verzamelen van informatie**: Het doel hier is om jouw persoonlijke gegevens te verzamelen zoals jouw wachtwoord, kredietkaartnummers of bankgegevens. Dit doet men door jou een e-mail met een link te sturen of je een website die er echt uitziet te laten bezoeken. Op deze website dien je jouw account- of persoonlijke gegevens in te voeren. De website is echter vals, alle gegevens die je invoert, worden meteen doorgestuurd naar de aanvaller.

Phishing

- **Schadelijke links**: Hier wil de aanvaller de controle van jouw toestel overnemen, door je een e-mail met daarin een link te versturen. Als je op de link klikt, dan ga je naar een website die meteen jouw toestel zal aanvallen en mogelijk jouw systeem besmet.
- **Schadelijke bijlages**: hier is het doel van de aanvaller hetzelfde, jouw toestel te besmetten of controle erover te nemen. In plaats van een link krijg je een e-mail met daarin een besmet bestand, zoals een Word-document. Als je de bijlage opent, begint de aanval, waarbij een aanvaller mogelijk toegang krijgt tot jouw systeem.
- **Oplichting**: Bepaalde e-mails komen van oplichters die de weg naar de digitale wereld ontdekken. Ze proberen je te misleiden door te zeggen dat je de loterij hebt gewonnen, doen zich voor als een goed doel dat geld inzamelt of vragen jouw hulp bij het versluizen van miljoenen dollars. Indien je hier op ingaat, vraagt men meteen naar een betaling voor hun diensten of willen ze toegang tot jouw bankrekening. Op deze manier wilt men jouw geld afhandig maken.



Jouw gezond verstand is de beste verdediging. Indien een e-mail of bericht vreemd, verdacht of te mooi is om waar te zijn, is het een phishingpoging.

Vaak is er bij het openen en lezen van een e-mailbericht geen vuiltje aan de lucht. Om een phishingaanval te doen slagen zal men proberen jou iets te laten doen. Gelukkig kan je een dergelijk bericht herkennen aan de volgende kenmerken:

- Het e-mailbericht bevat een noodsituatie waarbij het belangrijk is om snel te handelen alvorens er iets slechts gebeurt, zoals het afsluiten van jouw account. De aanvaller wilt dat je hier snel een vergissing maakt zonder erover na te denken.
- Je ontvangt een e-mail met een bijlage die je niet verwacht of de e-mail wil jou aansporen om de bijlage te openen. Bijvoorbeeld een bericht met daarin een bijlage die geheime informatie bevat over een ontslagronde, lonen van medewerkers of een waarschuwing van de belastingdienst.
- In plaats van dat men jouw naam gebruikt, bevat de e-mail een generieke aanhef zoals “Beste Klant”. De meeste bedrijven en vrienden zullen jouw naam gebruiken als ze je contacteren.
- In het e-mailbericht wordt er gevraagd naar vertrouwelijke gegevens, zoals jouw kredietkaartnummer of wachtwoord.
- De e-mail komt van een officiële organisatie, maar bevat taal- en grammaticafouten, of gebruikt een persoonlijk e-mailadres als @google.com, @yahoo.com of @hotmail.com.

Phishing

- De link ziet er verdacht of niet officieel uit. Beweeg je muis over de link totdat er een pop-up verschijnt die jou de werkelijke locatie toont van de link. Indien de link in die e-mail niet hetzelfde is als die van de pop-up, klik dan niet op de link. Op mobiele toestellen houd je jouw vinger op een link om een pop-up te krijgen. Een veiligere methode is de URL van de e-mail te kopiëren en te plakken in jouw browser of de juiste link zelf te typen.
- Je ontvangt een boodschap van iemand die je kent, maar de stijl of woordgebruik van het bericht lijkt niet op de stijl van de persoon. Indien je twijfelt, contacteer dan de afzender en verifieer of ze het bericht hebben verzonden. Voor cyberaanvallers is het zeer eenvoudig om een e-mail te versturen .

Indien je vermoedt dat een e-mail of een bericht een phishingaanval is, verwijder het bericht dan. Gezond verstand biedt de beste verdediging tegen phishing.

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)

Social Engineering:	https://www.securingthehuman.org/ouch/2014#november2014
Five Steps to Staying Secure:	https://www.securingthehuman.org/ouch/2014#october2014
I'm Hacked, Now What?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

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