OUCH! | July 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Sociale Media

Overzicht

Sociale media sites als Facebook, Twitter, Instagram en LinkedIn zijn interessante plaatsen, waar je mensen kan ontmoeten en informatie kunt delen. Met al deze interessante functies gaan er echter risico's gepaard, niet enkel voor jezelf maar ook voor jouw familie, vrienden en werkgever. In deze nieuwsbrief gaan we dieper in op de gevaren van sociale media en hoe je ze op een veilige en verantwoorde manier kan gebruiken.

Gastredacteur

Tanya Baccam is een doorwinterde security consultant. Ze is een SANS-auteur en instructeur voor meer dan 10 jaar voor de cursussen SEC502, SEC542, SEC401, MGT414, AUD507 en vele andere cursussen. Volg haar op Twitter via **@tbaccam**.

Privacy

Een grote bezorgdheid bij sociale media is het beschermen van jouw persoonlijke gegevens. Mogelijke gevaren hier zijn:

- **Gevolgen voor jouw toekomst**: Sommige bedrijven doorzoeken sociale media sites bij sollicitatieprocedures. Gênante foto's of ongepaste berichten kunnen mogelijk een impact hebben op het binnenhalen van een nieuwe job of het krijgen van een promotie. Veel universiteiten voeren gelijkaardige controles uit bij kandidaat studenten.
- **Aanvallen tegen jou**: cyberaanvallers kunnen jouw berichten analyseren en ze gebruiken om toegang te krijgen tot jouw of jouw werkgever zijn informatie. Bijvoorbeeld, ze kunnen deze informatie gebruiken om antwoorden op jouw veiligheidsvragen te raden om jouw online wachtwoorden te kunnen resetten. Om je gerichte phishing mails te sturen, ook bekend als spear phishing, of om iemand van jouw collega's te bellen waarbij hij zich voordoet als jou. Deze aanvallen kunnen overgaan naar de echte wereld, waarbij iemand jouw identiteit gebruikt.
- **Schade voor jouw werkgever**: criminelen of concurrenten kunnen jouw berichten over je bedrijf gebruiken tegen jouw werkgever. Bovendien kunnen de berichten mogelijk reputatieschade veroorzaken voor jouw bedrijf. Lees zeker de beleidsrichtlijnen na, alvorens je post over jouw job. Jouw sociale media berichten kunnen ook worden gemonitored door jouw werkgever.

De beste bescherming is dat je beperkt wat je post. Privacy instellingen kunnen wat bescherming bieden, maar vaak zijn ze verwarrend en veranderen ze regelmatig zonder jouw medeweten. Wat je dacht dat beperkt zichtbaar is, is plots leesbaar voor iedereen omwille van verschillende redenen. De privacy van je berichten is dus relatief, het is maar zo

Sociale Media

veilig als met wie je dit bericht allemaal deelt. Hoe meer vrienden of contacten je hebt, des te groter de kans dat de informatie publiekelijk wordt. Ga er van uit dat alles wat je post mogelijk publiek kan worden of permanent deel zal uitmaken van het Internet.

Ten slotte, wees bewust van wat vrienden over je posten. Als ze iets posten waardoor je je ongemakkelijk voelt, vraag hen dan of ze het verwijderen. Indien ze dit weigeren of negeren, neem dan contact op met de sociale media site en vraag of ze deze inhoud voor jouw willen verwijderen. Wees respectvol met wat je over anderen post.



Sociale media sites zijn plezierig en krachtig, maar wees voorzichtig met wat je deelt en met wie je dit deelt.

Beveiliging

Naast de privacy bezorgdheden zijn er ook enkele stappen die je kan nemen om je sociale media accounts en online activiteiten te beveiligen.

- **Login**: Beveilig elke account met een sterk, uniek wachtwoord en deel ze niet met anderen. Sociale media sites ondersteunen vaak nog extra authenticatie methodes zoals tweestapsverificatie, schakel deze extra methode in wanneer dit mogelijk is. Gebruik jouw sociale media account niet om in te loggen op andere sites, indien deze gehacked wordt, zijn opeens al jouw accounts bekend.
- **Privacyinstellingen**: indien je privacyinstellingen gebruikt, controleer en test deze dan regelmatig. Sociale media sites veranderen vaak hun privacyinstellingen, waardoor je snel een fout zal maken. Veel apps en diensten laten toe om jouw fysieke locatie toe te voegen bij de berichten die je post (nl. geotagging). Verander deze instellingen indien je jouw fysieke locatie niet wenst te delen.
- **Encryptie**: Sociale media sites gebruiken HTTPS-encryptie om jouw online verbinding met de site te beveiligen. Sommige sites als Twitter en Google+ bieden dit standaard aan, terwijl je bij anderen dit manueel dient in te schakelen. Controleer daarom de instellingen en schakel altijd HTTPS in als standaard verbinding.
- **E-mail**: Wees aandachtig met e-mails die komen van sociale media sites, deze kunnen gemakkelijk worden gespoofed door cybercriminelen. De veiligste manier om op deze berichten te antwoorden is door zelf in te loggen op jouw sociale media account, misschien vanaf een opgeslagen bladwijzer, en via deze manier te reageren op berichten of notificaties van de website.
- **Verdachte links/scams**: wees voorzichtig voor verdachte links of mogelijke oplichtingspraktijken via sociale media sites. Sociale media zijn populair bij slechteriken. Omdat een bericht van een vriend komt wilt niet altijd zeggen dat dit bericht echt van hem komt, accounts kunnen worden gehacked. Indien een vriend of familielid een vreemd bericht deelt, waarvan je de echtheid niet kan verifiëren (bijvoorbeeld ze zijn bestolen en vragen om geld

Sociale Media

te sturen), bel ze dan op hun mobiele telefoon en vraag hen om dit feit te bevestigen.

- **Mobiele Apps**: de meeste sociale media sites voorzien mobiele apps om jouw accounts te raadplegen. Zorg ervoor dat je deze apps downloadt van een vertrouwde locatie en dat jouw smartphone voorzien is van een sterk wachtwoord. Als je jouw smartphone verliest en als deze niet vergrendeld is, kan iedereen jouw sociale media sites raadplegen en onder jouw naam berichten posten.

Sociale media sites zijn een prachtige manier om in contact te blijven met de wereld. Als je onze tips volgt, zal je dit op een veiligere manier doen. Om meer te leren over hoe je sociale media sites veilig gebruikt of om verdachte activiteiten te rapporteren, raadpleeg de beveiligingspagina van jouw sociale media site.

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)

Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Securely Using Mobile Apps:	http://www.securingthehuman.org/ouch/2015#january2015
Educating Kids on Cyber Safety:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook Security:	https://www.facebook.com/safety

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