Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Overzicht
- Vijf Essentiële Stappen

Vijf stappen om veilig te blijven

Overzicht

Technologie neemt een steeds belangrijke plaats in ons leven, maar de complexiteit ervan neemt telkens toe. Op de hoogte blijven met de laatste beveiligingsadviesen kan soms verwarrend zijn. Het lijkt alsof er telkens nieuwe richtlijnen komen over wat je moet doen en wat je niet moet doen. Alhoewel de details van hoe je je exact kunt beveiligen wijzigen, zijn er een aantal fundamentele stappen die je altijd kunt naleven om jezelf te beveiligen. De volgende vijf stappen raden we aan, ongeacht welke technologie dat je gebruikt.

Gastredacteur

Lenny Zeltser focust zich op het veilig houden van IT-operaties bij klanten van NCR Corp en leert hoe men malware moet bestrijden bij het SANS instituut. Lenny is actief op Twitter als **@lennyzeltser** en heeft een security blog op **blog.zeltser.com**.

Vijf Essentiële Stappen

Elk van de vijf stappen wordt hieronder beknopt uitgelegd. Indien je meer wilt weten over een bepaalde stap, raadpleeg dan de 'Bronnen' sectie aan het einde van deze nieuwsbrief.

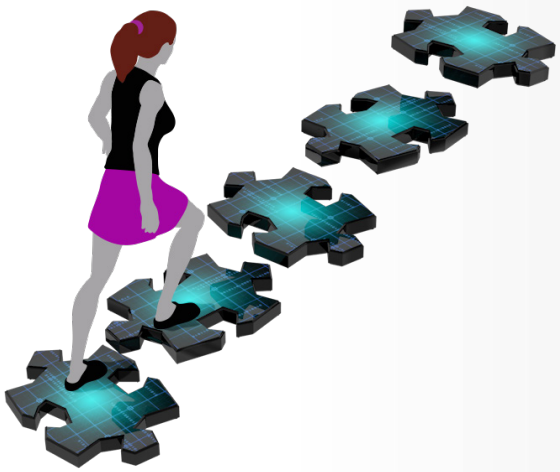
1. **Jezelf**: Het belangrijkste is dat je beseft dat enkel technologie niet voldoende is om je te beschermen. Aanvallers beseffen dat beveiligingstechnologie het makkelijkst kan worden omzeild door jou aan te vallen. Indien ze jouw wachtwoord of jouw kredietkaart willen, is de meest eenvoudige manier jou om de tuin leiden om hen deze informatie te geven. Bijvoorbeeld, ze contacteren jou onder het voorwendsel dat ze van de technische dienst van Microsoft zijn. Ze beweren dat jouw computer geïnfecteerd is, terwijl het gewoon cybercriminelen zijn, die toegang willen verkrijgen tot jouw computer. Of misschien versturen ze jou een e-mail met daarin een uitleg dat jouw postpakket niet aan jou kan worden bezorgd en vragen daarom dat je op een link klikt om jouw adres te bevestigen. Hun bedoeling is om je te leiden naar een geïnfecteerde website waarmee men jouw computer kan hacken. Ten slotte ben jijzelf de beste verdediging tegen aanvallers. Wees daarom dus op je hoede en gebruik je gezond verstand om de meerderheid van aanvalspogingen te herkennen en te stoppen.

2. **Updates**: Zorg ervoor dat jouw computers, mobiele toestellen, apps en alle andere toestellen die verbonden zijn met een netwerk, de laatste software versies bevatten. Cybercriminelen zijn constant op zoek naar kwetsbaarheden (zogenaamde vulnerabilities) in de technologieën die je gebruikt. Wanneer ze zulke kwestbaarheden vinden, gebruiken

© The SANS Institute 2014

Vijf stappen om veilig te blijven

ze speciale programma's om deze kwetsbaarheid te exploiteren en vervolgens de technolgie die je gebruikt te hacken. Dit kan jouw netwerk, computer of zelfs jouw mobiel toestel zijn. Intussen, werken de fabrikanten, van de door jou gebruikte technologie, hard om de versies up-to-date te houden. Eens een kwetsbaarheid openbaar is, zullen ze een patch maken om het probleem te dichten en maken ze dit bekend. Door jouw computers en mobiele toestellen te voorzien van deze updates, beperk je het aantal bekende kwetsbaarheden en ben je moeilijker te hacken. Om op de hoogte te blijven van updates, schakel je best zoveel mogelijk automatische updates in, overal waar het kan. Deze regel geldt voor iedere technologie dat verbonden is met een netwerk, zelfs Smart TV's, babyfoons, de router thuis, spelconsoles of op een dag zelfs jouw auto. Indien het besturingssysteem van je computer, mobiel toestel of iedere andere technolgie, niet meer ondersteund wordt, zal je geen updates meer ontvangen. In dit geval kan je best een nieuwe versie bemachtigen, die wel ondersteund wordt.



Door deze vijf essentiële stappen toe te passen, bescherm je jezelf op een goede manier wanneer je de nieuwste technologiëen gebruikt.

3. **Wachtwoorden**: De volgende stap om jezelf te beveiligen is door een sterk en uniek wachtwoord voor elk van jouw toestellen, online accounts en toepassingen te gebruiken. De nadruk hier ligt op sterk en uniek. Een sterk wachtwoord is er een die hackers of computer programma's niet gauw kunnen voorspellen. In plaats van één woord, gebruik een paszin van meerdere woorden met daarin enkele symbolen en nummers. Een uniek wachtwoord betekent dat je een een verschillend wachtwoord gebruikt voor elk toestel en online account. Als een wachtwoord dan wordt geraden, zullen je andere accounts en toestellen steeds veilig zijn. Ken je al deze sterke en unieke wachtwoorden niet uit het hoofd? Maak je dan geen zorgen, want dat kunnen we ook niet. Daarom raden we aan om een password manager te gebruiken, dit is een speciale toepassing voor jouw smartphone of computer die op een veilige manier al jouw wachtwoorden bewaart in een versleuteld formaat. Ten slotte, als jouw account twee-factor-authenticatie ondersteunt, raden we aan om dit altijd in te schakelen omdat dit de sterkste methode is om jouw account te beschermen.

4. **Encryptie**: Een vierde stap die we aanraden is het gebruik van encryptie. Encryptie zorgt ervoor dat enkel jij en de mensen die je vertrouwt, toegang hebben tot jouw informatie. Gegevens kunnen worden versleuteld op twee manieren: in rust en in beweging. Data-in-rust versleutelen, betekent het beveiligen als het is opgeslagen in de vorm van bestanden op jouw harde schijf of op een USB-stick. De meeste besturingssystemen, maken het mogelijk om automatisch jouw data te versleutelen door functionaliteit genaamd Full Disk Encryptie. We raden aan om dit in te schakelen waar

Vijf stappen om veilig te blijven

mogelijk. Het versleutelen van data-in-beweging betekent het versleutelen van data dat wordt verzonden van jouw computer of toestel naar anderen. Zoals bijvoorbeeld tijdens het online bankieren. Een simpele manier om te zien of encryptie is ingeschakeld tijdens het surfen, is door te letten op het adres van de website. Begint het adres met “https” of bevat het adres een icoon van een gesloten slotje, dan is er sprake van encryptie.

5. **Back-ups**: Vroeg of laat, ongeacht hoe zorgvuldig je ook bent, zal één van jouw toestellen of accounts worden gecompromitteerd. In dit geval, is jouw enige optie je ervan te verzekeren dat jouw computer of mobiele toestel geen malware meer bevat. Dit kan je doen door een volledige wipe en een nieuwe installatie. De aanvaller kan jou zelfs verhinderd hebben om persoonlijke bestanden te raadplegen als foto’s en andere gegevens op het gecompromitteerd systeem. De enige uitweg is om jouw persoonlijke informatie te herstellen van een back-up. Zorg ervoor dat je regelmatig back-ups maakt van belangrijke informatie en test ook of je de gegevens kunt herstellen. De meeste besturingssystemen en mobiele toestellen ondersteunen automatische back-ups.

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.

Nederlandse Editie

Cegeka is een full-service ICT-bedrijf: u kan bij ons terecht voor advies, detachering, softwareontwikkeling, bouw van websites, on-site en remote beheer van ICT-infrastructuur en outsourcing. Voor meer informatie: http://www.cegeka.com of volg ons op Twitter via @cegeka.

Bronnen (Engels)

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Keeping Your Tablet Secure:	http://www.securingthehuman.org/ouch/2013#december2013
Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Backups:	http://www.securingthehuman.org/ouch/2013#september2013

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de Creative Commons BY-NC-ND 4.0 license. Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en voor vertalingen.

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus