OUCH! | Oktober 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Jijzelf
- Wachtwoorden
- Updates
- Back-ups

Vier Stappen om Veilig te Blijven

Overzicht

Technologie neemt een steeds belangrijke plaats in ons leven en wordt alsmaar complexer. Op de hoogte blijven met de laatste beveiligingsadviezen kan soms verwarrend zijn. Het lijkt alsof er telkens nieuwe richtlijnen zijn over wat je moet doen en wat je niet moet doen. Toch zijn er een aantal fundamentele stappen die je altijd kan nemen om jezelf te beveiligen. Ongeacht de technologie die je gebruikt, raden we je aan om zeker deze vier stappen te volgen. Indien je meer wilt weten over een bepaalde stap, raadpleeg dan de 'Bronnen' sectie aan het einde van deze nieuwsbrief.

Gast redacteur

Ryan Johnson zorgt ervoor dat organisaties voorbereid zijn om te reageren op een onvermijdelijk datalek en geeft de cursus Advanced Network Forensics aan het SANS-instituut. Ryan is actief op Twitter als **@ForenicRJ**.

1. **Jezelf**: Het belangrijkste is dat je beseft dat enkel technologie niet voldoende is om jou volledig te beschermen. Aanvallers beseffen dat beveiligingstechnologie het makkelijkst kan omzeild worden door jou aan te vallen. Indien ze jouw wachtwoord, kredietkaart of persoonlijke gegevens 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 besmette website waarmee men jouw computer wil hacken. Op deze manier begint een CEO-fraude of ransomware aanval vaak. Ten slotte ben jijzelf de beste verdediging tegen aanvallers. Wees op jouw hoede. Door jouw gezond verstand te gebruiken zal je de meeste aanvallen kunnen herkennen en stoppen.

2. **Wachtwoorden**: De volgende stap om jezelf te beschermen is door sterke en unieke wachtwoorden te kiezen voor ieder toestel en account dat je bezit. Belangrijk hier is dat het wachtwoord sterk en uniek is. Een sterk wachtwoord betekent dat het niet makkelijk te raden is door hackers of door programma's. Ben je het beu om complexe wachtwoorden die te moeilijk zijn om te onthouden of in te geven? Probeer dan eens een wachtzin. In plaats van één woord, gebruik je een

Vier Stappen om Veilig te Blijven

reeks van woorden die je makkelijker onthoudt, zoals “Waar is mijn koffie?”. Hoe langer de wachtzin, hoe sterker. Een uniek wachtwoord betekent dat je ieder toestel en account van een verschillend wachtwoord voorziet. Indien er dan één wachtwoord wordt gelekt, zijn jouw andere accounts en toestellen veilig. Heb je moeite om alle sterke en unieke wachtwoorden te onthouden? Maak je dan geen zorgen, want dat kunnen we ook niet. Gebruik hiervoor een password manager, dit is een speciale toepassing voor jouw smartphone of computer die op een veilige manier al jouw wachtwoorden bewaart in een versleuteld formaat.

Door deze vier stappen toe te passen, bescherm je jezelf op een goede manier wanneer je de nieuwste technologieën gebruikt.

Ten slotte één van de belangrijkste dingen die je kan doen om jouw account te beschermen is het inschakelen van twee-staps-verificatie. Alleen een wachtwoord is niet meer genoeg om een account te beschermen, we hebben nood aan iets sterkers. Met twee-staps-verificatie gebruik je naast het wachtwoord, een extra stap, namelijk iets wat je bent (biometrie) of iets wat je hebt (zoals een code dat naar jouw smartphone wordt verstuurd of er op wordt gegenereerd). Schakel deze optie in op iedere account, zelfs op jouw password manager. Twee-staps-verificatie is de belangrijkste stap om jezelf te beschermen en is veel eenvoudiger als je denkt.

3. **Updates**: Zorg ervoor dat jouw computers, mobiele toestellen, apps en alle andere zaken die verbonden zijn met het Internet de laatste software versies bevatten. Cybercriminelen zijn continu op zoek naar nieuwe kwetsbaarheden in de software die jouw toestellen gebruiken. Wanneer ze kwetsbaarheden ontdekken, gebruiken ze speciale programma’s om jouw toestellen te hacken. Intussen, werken de fabrikanten van de door jou gebruikte technologie, hard om updates uit te brengen om deze kwetsbaarheden te verhelpen. Door deze updates te installeren op jouw computer en toestellen, maak je het moeilijker dat je wordt gehackt. Om bij te blijven met de updates, schakel je best automatische updates in. Deze regel geldt voor iedere technologie dat verbonden is met een netwerk, zoals Smart TV’s, babyfoons, de router thuis, spelconsoles of op een dag zelfs jouw auto. Indien jouw besturingssysteem of toestellen oud zijn en niet meer worden ondersteund met security updates, dan kan je ze best vervangen door nieuwe die wel ondersteund zijn.

Vier Stappen om Veilig te Blijven

4. **Back-ups**: Vroeg of laat, hoe voorzichtig je ook bent, kan je gehackt worden. In dit geval is jouw enige optie jou er van te verzekeren dat jouw computer of toestel geen malware meer bevat. De aanvaller zal jou zelfs verhinderd hebben om persoonlijke bestanden,foto's en andere informatie te raadplegen op het gehackte 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. We raden ook aan om back-ups offline of in de Cloud te bewaren om ze te beschermen tegen cyberaanvallers.

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)

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

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