OUCH! | April 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Ik Ben Gehackt, Wat Nu?

Overzicht

Hoe veilig je ook omspringt met technologie, vroeg of laat is er de kans dat je gehackt of gecompromitteerd wordt. In deze nieuwsbrief leer je hoe je kan bepalen of jouw computer of mobiel toestel is gehackt en wat je dan moet doen. Hoe sneller je bepaalt dat er iets niet pluis is en hoe sneller je reageert, hoe beter je de schade beperkt die een cyberaanvaller kan veroorzaken.

Gast redacteur

Samantha Davison (**@sam_e_davison**) is de Security awareness en opleiding programma manager bij Uber en leidt medewerkers op in 350 verschillende steden over de hele wereld.

Indicaties Dat Je Gehackt Bent

Het is lastig om te bepalen dat je gehackt bent want vaak is er geen eenduidige manier waarop je dit kan vaststellen. Hackers laten vaak sporen achter, die men indicaties noemt. Hoe meer indicaties er op jouw systeem aanwezig zijn, hoe groter de kans dat je bent gehackt.

- Jouw antivirusprogramma geeft een waarschuwing dat jouw systeem besmet is, zeker als het niet mogelijk is om de schadelijke bestanden te verwijderen of in quarantaine te plaatsen.
- De startpagina van jouw browser is plots gewijzigd en de browser brengt je naar websites waar je niet om hebt gevraagd.
- Er zijn nieuwe gebruikersaccounts op jouw computer of toestel die je niet hebt aangemaakt of er zijn nieuwe programma's actief die je niet hebt geïnstalleerd.
- Jouw computer of de toepassingen crashen constant, er zijn iconen van onbekende toepassingen of vreemde pop-up vensters duiken op.
- Een programma vraagt om jouw autorisatie om wijzigen te doen aan jouw systeem, toch ben je niet iets aan het installeren of aan het updaten.
- Jouw wachtwoord werkt niet meer als je probeert aan te melden in jouw systeem of online gebruikersaccount, zelfs als je zeker bent dat jouw wachtwoord correct is.
- Vrienden vragen je waarom je hen SPAM e-mails stuurt waarvan je zeker weet dat je die niet hebt verstuurd.
- Jouw mobiel toestel verstuurt SMS-berichten naar betaalnummers.

Ik Ben Gehackt, Wat Nu?

- Er is plots een hoog data-of batterijverbruik op jouw mobiel toestel.

Hoe reageren

Als je denkt dat jouw computer of toestel gehackt is, is het belangrijk om snel te reageren. Hoe sneller je reageert, hoe beter. Indien de computer of toestel van jouw werkgever is, los je het probleem beter niet zelf op. Hierdoor kan je mogelijk bewijsmateriaal verwijderen die men in een onderzoek nodig heeft. Rapporteer daarom dit incident meteen aan jouw werkgever, door contact te nemen met jouw helpdesk, security team of leidinggevende. Kan je de organisatie niet bereiken, of ben je bezorgd, haal dan jouw toestel van het netwerk, zet het in slaap- of vliegmodus. Zelfs als je niet zeker weet of je wel bent gehackt, is het beter om dit te rapporteren. Indien het gaat om een persoonlijke computer of toestel, kan je deze stappen nemen:

Vroeg of laat zal jouw computer of toestel worden gecompromitteerd, hoe sneller je een incident kan detecteren en er op reageert, hoe beter.

- **Wijzig Jouw Wachtwoorden**: dit omvat niet alleen de wachtwoorden op jouw toestellen, maar ook jouw online wachtwoorden. Gebruik hiervoor best een andere computer, waarvan je weet dat deze veilig is om de wachtwoorden te wijzigen.
- **Antivirus**: indien jouw antivirus een melding geeft over een besmet bestand, kan je de stappen volgen die het aanbeveelt. Dit is vaak het in quarantaine plaatsen van het bestand, het bestand schoonmaken of verwijderen. De meeste antivirusprogramma's bevatten links met meer informatie over de besmetting. Als je twijfelt, plaats dan het bestand in quarantaine. Indien dit niet mogelijk is, verwijder het dan.
- **Nieuwe installatie**: Indien je de besmetting niet kan repareren of indien je zeker wilt zijn dat het systeem volledig veilig is, biedt een nieuwe installatie de veiligste keuze. Voor computers dien je de stappen te volgen van de leverancier. In veel gevallen dien je hier de ingebouwde tools te gebruiken om het besturingssysteem terug te installeren. Indien deze tools er niet zijn of besmet zijn geraakt, contacteer dan jouw leverancier of raadpleeg de website voor meer informatie. Installeer het besturingssysteem niet opnieuw vanuit jouw back-ups, deze bevatten mogelijk dezelfde zwakke plekken die de hacker de oorspronkelijke toegang hebben gegeven. Back-ups dienen enkel te worden gebruikt om data te herstellen. Bij mobiele toestellen kan je best de stappen volgen van de leverancier of service provider, deze kan je vinden op hun website. In veel gevallen is dit simpelweg het toestel te herstellen naar de fabrieksinstellingen. Indien je niet vertrouwd bent met een nieuwe installatie, kan je ook

Ik Ben Gehackt, Wat Nu?

professionele hulp zoeken om je hiermee te helpen. Of als jouw computer of toestel té oud is, is het misschien beter en makkelijker om een nieuw toestel te kopen. Ten slotte, als je de installatie hebt uitgevoerd of een nieuw toestel hebt, zorg er dan voor dat automatische updates zijn ingeschakeld en de laatste updates zijn uitgevoerd.

- **Back-ups**: de belangrijkste stap die je kan nemen, is door je voor te bereiden door geregeld back-ups te nemen. Hoe vaker je back-ups neemt, hoe beter. Sommige back-up diensten zullen automatisch een back-up nemen voor nieuwe of gewijzigde bestanden. Ongeacht de back-upoplossing, dien je geregeld een test te doen of je de bestanden wel kunt herstellen. Hierdoor zal je zeker zijn dat je bestanden kunt herstellen indien je wordt gehackt.
- **Politiediensten**: voel je je bedreigt? Stap dan naar de politiediensten om melding te doen.

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)

Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Account Gehackt:	https://www.safeonweb.be/nl/tips/help-mijn-account-gehackt

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