OUCH! | May 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Het Internet of Things (IoT)
- Problemen met IoT
- Jouw IoT-Toestellen Beschermen

Internet of Things (IoT)

Wat is het Internet Of Things (IoT)

Gast redacteur

James Lyne (**@jameslyne**) is de globale verantwoordelijke voor security onderzoek bij de security firma Sophos. Als zelfverklaarde 'massive geek' heeft hij technische vaardigheden in verschillende security domeinen. Hij is een gecertifieerde instructeur bij het SANS-instituut en is vaak hoofdspreker bij conferenties.

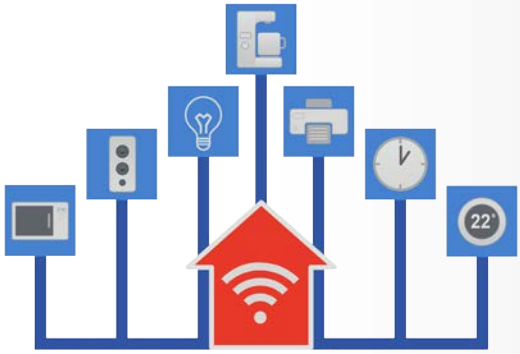
Vroeger was technologie relatief eenvoudig, je maakte verbinding met jouw computer met het Internet en gebruikte dit voor jouw dagelijkse activiteiten. Daarna evolueerde de technologie met mobiele toestellen die intrede deden in ons leven, zoals de smartphones en tablets. Deze toestellen zorgen ervoor dat je de kracht van een computer in jouw broekzak hebt. Hoewel deze toestellen meer mobiel zijn, hebben deze toestellen ook hun eigen beveiligingsuitdagingen. De nieuwste technologische evolutie is het Internet of Things. Met het Internet of Things, of afgekort IoT, worden alle dagelijkse toestellen verbonden met het Internet, toestellen als deurbellen, gloeilampen, speelpoppen en thermostaten. Deze verbonden toestellen kunnen ons leven vergemakkelijken –bijvoorbeeld automatisch het licht activeren wanneer jouw smartphone merkt dat je dichtbij huis bent. De IoT-markt evolueert zeer snel, iedere week komen er nieuwe toestellen bij. Toch hebben IoT-toestellen, net als mobiele toestellen, hun eigen specifieke security problemen. In deze nieuwsbrief helpen we jou deze risico's te begrijpen en wat je kan ondernemen om jouw IoT-toestellen te beveiligen, alsook jouw huis en jouw familie.

Problemen Met IoT

De kracht van IoT is dat de meeste van deze toestellen té eenvoudig zijn. Bijvoorbeeld, je steekt jouw koffiemachine in en deze zal vragen om te verbinden met jouw Wifi-netwerk thuis. Al deze eenvoud komt echter met een aantal problemen. Het grootste probleem is dat de bedrijven die de IoT-toestellen maken, geen ervaring hebben met security, hun expertise is het maken van huishoudtoestellen. Of misschien zijn het startups die zo efficiënt mogelijk een product ontwikkelen, op de snelst mogelijke manier, zoals op Kickstarter. Deze organisaties focussen op winst en niet op cyber security. Met als resultaat dat veel IoT-toestellen die je vandaag koopt, weinig tot geen beveiliging hebben. Bijvoorbeeld, sommigen bevatten standaard wachtwoorden die gekend zijn, misschien zelfs op het Internet zijn gepubliceerd en niet veranderd kunnen worden. Bij veel toestellen heb je geen mogelijkheid om ze in te stellen en ben je aangewezen met dat wat je hebt gekregen. Vaak

Internet of Things (IoT)

kan je de toestellen maar moeizaam updaten. Hierdoor zijn veel IoT-toestellen niet meer up-to-date en bevatten ze kwetsbaarheden die niet kunnen worden opgelost, waardoor ze permanent kwetsbaar zijn.



Weet welke IoT-toestellen er verbonden zijn met jouw netwerk, isoleer ze indien mogelijk en houd ze up-to-date en voorzie ze met sterke wachtzinnen.

Jouw IoT-toestellen Beschermen

Wat kan je doen? We willen dat je gebruik maakt van de kracht van IoT-toestellen op een veilige manier. Deze toestellen kunnen jouw leven vergemakkelijken, helpen geld te besparen en de fysieke beveiliging van jouw huis te verbeteren. Naarmate deze technologie meer ingeburgerd raakt, heb je geen enkele andere mogelijkheid meer dan IoT-toestellen te gebruiken. Hier zijn enkele stappen die je kan nemen om veilig om te gaan met IoT-toestellen.

- **Verbindt Enkel Wat Je Nodig Hebt**: De eenvoudigste manier om een IoT-toestel te beveiligen is door deze niet met het Internet te verbinden. Heb je het toestel niet online nodig, verbindt het dan niet met jouw Wifi-netwerk.
- **Afzonderlijk Wifi-Netwerk**: heb je jouw IoT-toestellen online nodig? Overweeg dan om een afzonderlijk Wifi-netwerk op te zetten. Veel Wifi access points hebben de mogelijkheid om een extra netwerk op te zetten, een zogenaamd guest netwerk. Een andere optie is om een extra Wifi access point te kopen die je enkel voor IoT-toestellen gebruikt. Hierdoor isoleer je de IoT-toestellen op een apart netwerk, waardoor ze niet kunnen worden gebruikt om computers of mobiele toestellen op jouw thuisnetwerk aan te vallen (die nog steeds het hoofddoelwit zijn voor cybercriminelen).
- **Update Wanneer Mogelijk**: Net als met jouw PC en mobiele toestellen, houd je IoT-toestellen up-to-date. Indien jouw IoT-toestel de mogelijkheid heeft om automatisch te updaten, schakel je dit best in.
- **Sterke Wachtwoorden**: Verander de wachtwoorden van jouw toestel in een unieke, sterke wachtzin die jij enkel kent. Kan je al jouw wachtwoorden niet onthouden? Overweeg dan om een wachtwoordkluis om ze op een veilige manier te bewaren.
- **Privacy instellingen**: indien je de privacy instellingen van jouw toestel kan configureren, beperk dan de hoeveelheid aan informatie die je deelt. Of schakel het delen van informatie gewoonweg uit.

Internet of Things (IoT)

- **Overweeg Vervanging**: Op een gegeven moment zal je jouw IoT-toestel willen vervangen omdat jouw toestel te veel kwetsbaarheden bevat die niet gemaakt kunnen worden of er zijn nieuwere toestellen die meer beveiliging hebben.

Er is geen simpele oplossing voor ieder toestel, het is handig om te kijken naar best practices en handleidingen over hoe je ze moet beveiligen. Jammer genoeg zijn de meeste IoT-toestellen ontworpen zonder de gedachte van beveiliging en veel leveranciers zijn karig met security informatie. Maar naarmate het cyberbewustzijn groeit, hopen we dat meer IoT-verkopers rekening houden met beveiliging en informatie geven over hoe je ze kan beveiligen en updaten.

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:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016

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