OUCH! | Augustus 2018

OUCH!

SANS SECURITY AWARENESS

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

Slimme Thuisproducten

Wat zijn Slimme Thuisproducten?

Aanvankelijk beschikten slechts een paar van uw apparaten thuis over een internetverbinding, zoals uw laptop, smartphone of gameconsole. Vandaag de dag echter maken steeds meer apparaten verbinding met het internet, van uw gloeilampen en luidsprekers tot uw tv, uw deur of zelfs uw auto. Binnenkort kan bijna elk apparaat in uw huis worden aangesloten op het internet. Deze verbonden apparaten worden vaak aangeduid met de naam “internet of things” (IoT) of “Slimme Thuisproducten”. Deze verbonden apparaten brengen veel gemak, maar zij brengen ook unieke gevaren met zich mee.

Wat is het probleem?

Met meer apparaten die zijn aangesloten op het netwerk van uw huis, kan er ook meer misgaan. Hackers kunnen uw apparaten programmeren om andere apparaten aan te vallen, leveranciers kunnen uitgebreide informatie over uw activiteiten verzamelen en bovendien kunnen uw apparaten geïnfecteerd raken en u buitensluiten. Veel van de bedrijven die deze apparaten maken hebben geen ervaring met cybersecurity en zien beveiliging als een kostenpost. Als gevolg hiervan hebben veel van de apparaten die u koopt weinig tot geen beveiliging ingebouwd. Sommige apparaten zijn bijvoorbeeld voorzien van een standaardwachtwoord dat algemeen bekend is of u kunt het apparaat niet updaten of configureren.

Hoe kan ik mezelf beschermen

Welnu, wat kun je doen? We willen absoluut dat je aangesloten apparaten veilig en beveiligd kan benutten. Deze apparaten bieden fantastische functies die je leven eenvoudiger maken. Bovendien, als de technologie groeit, heb je misschien geen andere keuze dan slimme producten te gebruiken. Hier zijn de belangrijkste stappen die je kunt nemen om jezelf te beschermen.

Sluit alleen datgene aan wat je nodig hebt: De eenvoudigste manier om een apparaat te beveiligen is het niet te verbinden met het internet. Als je je apparaat niet online nodig hebt, sluit het dan niet aan op je Wi-Fi-netwerk. Is het werkelijk nodig dat je broodrooster meldingen stuurt naar je telefoon?

Weten wat je hebt verbonden: Welke apparaten heb je op je thuisnetwerk aangesloten? Twijfel je of kan je je het niet meer herinneren? Schakel je draadloze netwerk uit en kijk wat er niet meer werkt. Het zal misschien niet alles opvangen, maar je zult verbaasd zijn hoeveel apparaten je bent vergeten.

Blijf op de hoogte: Net als je computer en mobiele apparaten is het van cruciaal belang om al je apparaten up-to-date te houden. Als je toestel de optie heeft om automatisch bij te werken, schakel die dan in.

Wachtwoorden: Wijzig de wachtwoorden op je apparaten in een unieke, sterke wachtwoordzin die alleen jij kent. Waarschijnlijk hoef je ze maar één keer in te voeren. Kun je je niet meer al je passphrases herinneren? Maak je geen zorgen, wij ook niet. Overweeg het gebruik van een password manager om ze allemaal veilig op te slaan.

Privacy Opties: Als je op je toestel privacyopties kunt configureren, beperk dan de hoeveelheid informatie die wordt verzameld of gedeeld. Een van de opties is het eenvoudig uitschakelen van de mogelijkheden voor het delen van informatie.

Leverancier: Koop al jouw apparaten bij een bedrijf dat je kent en vertrouwt. Zoek producten die de veiligheid ondersteunen, zoals automatische updates, het wijzigen van het standaardwachtwoord en het wijzigen van privacyinstellingen.

Altijd luisteren: Als een apparaat uw stemcommando's kan uitvoeren, luistert het voortdurend. Uw Alexa- en Google Home-apparaten kunnen bijvoorbeeld gevoelige gesprekken opnemen. Houd daar rekening mee wanneer je bepaalt waar je de apparaten in je huis plaatst en bekijk de privacyopties.

Gastennetwerk: Overweeg om gebruik te maken van een gescheiden "Guest" WiFi-netwerk voor de Slimme Thuisproducten in plaats van het primaire WiFi-netwerk dat je gebruikt voor je computers en mobiele apparaten. Op deze manier blijven computers of mobiele apparaten op het hoofdnetwerk veilig als er een Slim Product is geïnfecteerd.

Er is geen enkele reden om bang te zijn voor nieuwe technologieën, maar we moeten wel beseffen welke risico's ze met zich meebrengen. Met deze paar eenvoudige stappen kun je helpen bij het creëren van een veel veiliger Smart Home.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Robert M. Lee *(@RobertMLee) is een SANS-gecertificeerde instructeur en tevens auteur van FOR578 - Cyber Threat Intelligence en ICS515 - ICS Active Defense and Incident Response. Robert is ook CEO en oprichter van het industriële cyberbeveiligingsbedrijf Dragos.*

Bronnen

Passphrases:	https://www.sans.org/u/GEB
Password Managers:	https://www.sans.org/u/GEG
Securing Your Home Network:	https://www.sans.org/u/GEL