**Persbericht**

**Sophos-onderzoek onthult IoT-risico’s; België staat op 15e plek wereldwijd**

* *Onderzoek wijst uit: meer dan 70.000 toegangspogingen tot smart homes*
* *Scannen naar smart home devices bevat meer dan 68.000 open web GUI's*
* *869 open web-GUI’s voor België; goed voor een 15e stek wereldwijd*

**Brussel, 26 oktober 2017 – Samen met Koramis heeft Sophos 'Project Haunted House' gelanceerd. De resultaten van het onderzoek worden pas in november aanstaande gepubliceerd, maar de eerste tussentijdse cijfers hieruit hebben aangetoond dat meer dan 70.000 toegangspogingen van 24.089 individuele IPS’s naar virtuele huizen hebben plaatsgevonden. België komt er met 869 open web interfaces vanaf met een wereldwijde top-15 notering. De Verenigde Staten voeren de lijst aan, Duitsland staat op een tweede plek, gevolgd door Canada op drie. Een duidelijke tendens is zichtbaar: het ‘Haunted House’ is geen Halloween-aangelegenheid maar een waar gevaar voor smart homes.**

Om deze cijfers te versterken en de classificatie in de grootste context mogelijk te maken, bevat het project ook actieve internetscans voor smart home devices via zoekmachines zoals Shodan of Censys. Een scan die in oktober begon, resulteerde in meer dan 68.000 open webinterfaces van gerenommeerde ‘smart home’ componenten, die voornamelijk worden gebruikt in particuliere woningen. Denk daarbij aan draadloze raamcontacten, rookmelders, automatische deuropenings- of vergrendelingssystemen én camerasystemen. Al deze apparaten bleken gemakkelijk toegankelijk via het internet. De visualisatie via *heat maps* geeft aan dat de IoT-technologie zich in steden en stedelijke centra afspeelt, met een sterke concentratie in de randstad. Op het platteland is dit minder van toepassing.

"Deze aantallen benadrukken het belang van beveiliging bij het bouwen van je smart home", zegt Tim Stamer, Marketing Manager Benelux. "Anders is er kans dat cybercriminelen die op zoek zijn naar je geld en data makkelijk kunnen binnendringen. "

Acht tips voor een veilig smart home (en niet een Haunted House):

1. **Houd thuisnetwerken voor eigen gebruik** - Deel het niet met anderen.
2. **Sluit geen IoT-apparaten aan op het thuisnetwerk als dat niet nodig is** - De tv mag bijvoorbeeld niet worden aangesloten op de Wifi wanneer er voornamelijk tv via kabel of antenne wordt gekeken.
3. **Maak een apart netwerk voor IoT-apparaten** - Als de WiFi-router meerdere netwerken kan aanmaken, zorg dan voor een speciaal netwerk voor alle IoT-apparaten waarmee de toegang tot het ‘reguliere’ netwerk niet meer nodig is.
4. **Maak verschillende afgesloten netwerken op verschillende Wifi-netwerken** - Het is zelfs beter verschillende afgesloten netwerkgebieden te creëren voor Home Office, entertainmentelektronica, gebouw- en beveiligingstechniek en het gastnetwerk - alle met verschillende Wifi. Dit kan door een firewall worden geactiveerd die alleen de communicatie mogelijk maakt die nodig is om de componenten te gebruiken, maar niet voor de infiltratie van een besmetting van een I0T-apparaat naar een andere.
5. **Gebruik beveiligde VPN-technologie** - Gebruik geen onbeveiligde poorten op de router om toegang te krijgen tot IoT-apparaten van het internet. Gebruik in plaats daarvan een beveiligde VPN-technologie op de smartphone of Mac / PC.
6. **Houd software up to date** - Installeer de antivirussoftware op alle pc’s, Macs en Android-smartphones.
7. **Beveilig alles met de nieuwste firmware** - Niet alleen pc, laptop of smartphones, maar ieder IoT-apparaat dient met de meest actuele firmware zo veilig mogelijk te draaien. Tijdrovend maar de moeite waard.
8. **Google is je vriend** - Google naar mogelijke veiligheidsgaten van IoT-apparatuur. Dit geeft een goed overzicht van IoT-producten die hackers op het oog hebben (of die al een keer zijn gehackt).

**Connect with Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/+sophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com/).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Sandra Van Hauwaert, Square Egg, [Sandra@square-egg.be](mailto:Sandra@square-egg.be), 0497251816