Jeden Tag mindestens ein Eindringling im Haunted House – die wichtigsten Ergebnisse der Sophos IoT-Studie

Sophos hat die Ergebnisse seiner IoT-Security-Langzeitstudie „Haunted House“ in einem Whitepaper zusammengefasst. Das wichtigste vorab: kein Gerät wurde aktiv manipuliert, aber jeden Tag stieg die Anzahl der Angriffe

Wiesbaden, 28. November 2017 – Die Geräte der Zukunft werden smart sein: sie kommunizieren über das Internet mit der Außenwelt und sollen uns neben Spaß auch eine Erleichterung in unserem aufgabenorientierten Alltag geben. Doch während sich bereits die meisten Nutzer viele Gedanken über die Security für Computer oder mobile Geräte machen, ist dieses Bewusstsein bei Smart-Home-Komponenten noch nicht besonders ausgeprägt – dabei sind internetfähige IoT-Geräte (Internet of Things) nichts Anderes als kleine Computer im eigenen Netzwerk.

Das „Haunted House“ – die Simulation eines Smart Homes
Bislang aber gibt es kaum valide Daten über externe Zugriffe auf IoT-Geräte. Deswegen baute das von Sophos beauftrage Unternehmen Koramis eine Smart-Home-Infrastruktur als Honeypot auf, das „Haunted House“. Auf einer 4 x 2,5 Meter großen, einer Wohnung nachempfundenen Fläche wurden insgesamt 13 IoT-Geräte und -Steuerungssysteme unterschiedlicher Hersteller eingebaut, vernetzt und mit dem Internet verbunden – klassisch wie man es in immer mehr modernen Haushalten findet.

Drei Testphasen
In zwei der insgesamt drei Testphasen wurden die Art und Häufigkeit von Zugriffsversuchen auf die Komponenten im Haunted House aufgezeichnet. Die erste Phase erfolgte über sechs Wochen mit eigens vergebenen und sicheren Passwörtern. Die zweite Phase mit demselben Aufbau lief drei Wochen, allerdings mit den Standardeinstellungen der Hersteller – so wie man es häufig in privaten Haushalten installiert findet.
Für die Einordnung dieser Ergebnisse im einem größeren Kontext, wurden in einer dritten Phase aktive Internet-Scans nach typischen und offenen IoT-Komponenten mithilfe der IoT-Suchmaschinen SHODAN und Censys durchgeführt. Die Ergebnisse wurden in sogenannten Heatmaps für die deutschsprachige Region, Europa und weltweit dargestellt.

Die Ergebnisse: wenig überraschend aber besorgniserregend
Die Zugriffsversuche auf das Haunted House übertrafen die Erwartungen und waren hoch. Aus fast jedem Land der Welt wurde im Versuchszeitraum mindestens einmal versucht, ein IoT-Gerät im Haunted House anzusprechen – in der ersten Phase im Frühjahr 2017 ca. 1.500 tägliche Zugriffsversuche, in der zweiten Phase im Herbst 2017 rund 3.800.
Die Verteilung der Zugriffe aus den einzelnen Ländern unterscheidet sich dabei bei beiden Testphasen. Besetzen China und die USA in beiden Perioden die ersten beiden Plätze, verändert sich der Drittplatzierte stark: Mexiko liegt in der ersten Testphase auf drei, in der zweiten Phase schafft es das Land nicht mal unter die Top Ten. Brasilien (vormals fünf) nimmt seinen Platz ein. An Brasiliens Stelle positioniert sich neu Japan.
Auffallend: innerhalb dieses zweiten Testzeitraumes von drei Wochen konnten 27 Angriffe auf den Server eines Herstellers identifiziert werden. Im Ergebnis lässt sich also schließen, dass sich im Testzeitrum, bei dem mit Standardeinstellungen gearbeitet wurde, durchschnittlich mehr als ein ungebetener Gast pro Tag im Haunted House umgeschaut hat. An den Systemen wurden dabei von keinem Angreifer Veränderungen vorgenommen – obwohl dieses möglich gewesen wäre.

Bei den aktiven Internet-Scans wurden viele Internet-Gateways für IoT-Komponenten gefunden, mit steigender Tendenz. In der Region DACH lässt sich zwischen März und Mai mit 3,7 Prozent ein dauerhafter Anstieg offener Gateways verzeichnen. Hochgerechnet auf ein Jahr liegt der Wert bei linearer Fortschreibung bei 22,2 Prozent und bestätigt damit die prognostizierte Marktentwicklung von 25 Prozent für dien DACH-Bereich (www.statista.com). Weltweit stieg die Anzahl gefundener Gateways um die Rate 3,1 Prozent.

Die genaue Beschreibung der "Haunted House"-Studie samt ausführlicher Darstellung der Ergebnisse sind nun in einem Whitepaper veröffentlicht und steht zum Download unter: www.sophos-events.com/smarthome.

Wie kann man sich schützen?
„Zunächst einmal muss der Nutzer sich bewusst machen, dass viele IoT-Geräte kleine, netzfähige Computer sind, die sich von außen ansteuern lassen", so Michael Veit, IT-Security Experte bei Sophos. Will man also verhindern, dass Hacker sich Zugriff auf eigene Fotos und Dateien verschaffen oder die Rechenleistung des übernommenen Geräts für ein Bot-Netz nutzen, um großangelegte Cyberattacken auszuführen, sollte man ein paar Tipps beachten:

- My Home(network) is my Castle: Niemals das Heimnetz mit anderen teilen!
- Generell sollte man sich über eine einfach Suche im Internet darüber informieren, wie die Sicherheit der begehrten IoT-/Smart Home-Komponente einzuschätzen ist
- Die werksseitigen Passwörter sollten umgehend bei der Installation durch sichere Passwörter ersetzt werden
- Wenn verfügbar (und das ist eine Grundvoraussetzung für Security) sollte die Firmware immer auf den neuesten Stand aktualisiert werden
- IoT-Geräte möglichst raus aus dem Heimnetzwerk. Ein Beispiel: wenn hauptsächlich über Kabel oder Antenne empfangen wird, kommt das Fernsehgerät auch ohne WLAN aus.
- Im Heimnetz sollten wichtige von unwichtigen Komponenten getrennt und in unterschiedlichen Netzen konfiguriert werden, damit eventuell unsichere Komponenten keinen Zugriff auf sensible Daten haben
- „Sealed-Off"-Netzwerkbereiche auf verschiedenen WLANs: Noch sicherer ist es, verschiedene „Sealed-Off"-Netzwerkbereiche für Home Office, Unterhaltungselektronik, Gebäude- und Sicherheitstechnik oder das Gastnetzwerk mit jeweils unterschiedlichen WLANs zu erstellen. Dies kann durch eine Firewall ermöglicht werden, die ausschließlich jene Kommunikation erlaubt, die für die Verwendung der Komponenten erforderlich ist, und eine Infektion von einem IoT-Gerät zum anderen unterbindet. Die Sophos XG Firewall Home Edition Firewall steht kostenlos zum Download bereit.
- Verwendung einer sicheren VPN-Technologie: Statt für den Fernzugriff auf die IoT-Geräte aus dem Internet eine unsichere Port-Weiterleitung auf dem Router einzurichten, ist es besser, eine sichere VPN-Technologie auf dem Smartphone oder Mac / PC zu verwenden.
- Und natürlich sollten auch die „traditionellen" Geräte wie PC, Smartphone oder Laptop mit einem Antivirus-Programm geschützt sein. Kostenlose Versionen gibt es u.a. unter www.sophos.de/freetools

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de