Die Geister, die man ruft.
IoT-Risiken zu Hause. 8 Tipps wie man sicher bleibt.

Es spukt im Haunted House: Sophos-Studie zählt mehr als 70.000 Zugriffsversuche auf sein virtuelles Smart Home sowie über 68.000 offene Web-Schnittstellen zu Smart-Home-Geräten. Deutschland liegt mit 6.576 offenen Web-GUIs weltweit auf Platz zwei. Sophos gibt 8 Tipps für eine bessere Sicherheit des Smart Home

Wiesbaden, 25. Oktober 2017 – Gerade zu Halloween ist es ja durchaus möglich, dass das traute Heim von dem einen oder anderen Spuk und frech fordernden Quälgeistern heimgesucht wird. Aber während man letztere gut mit süßen oder sauren Bonbons bestechen kann, gibt es andere Spuk-Spezies, die unsichtbar und wirklich gruselig sind: Hacking-Attacken auf das eigene Smart Home beispielsweise.

Zur Geister-Hochkonjunktur rund um Halloween präsentiert Sophos daher gemeinsam mit dem Spezialisten für industrielle Automatisierung, Koramis, weitere Ergebnisse des Forschungsprojekts „Haunted House“, dessen Abschlussbericht im November 2017 veröffentlicht wird. Aktuelle Zwischenzahlen zeigen mehr als 70.000 Zugriffsversuche von 24.089 einzelnen IPS auf das virtuelle Haus. Hiermit wird deutlich: Das Haunted House ist kein einmaliges Geisterphänomen sondern eine dauerhafte Gefahr für private Smart Homes – sofern diese nicht fachgerecht eingerichtet sind. Und dies ist nur die eine Seite des Spuks:

Die Geister, die man ruft
Parallel zu den Zugriffsversuchen auf das „Haunted House“ erforscht das Projekt mithilfe von Suchmaschinen wie Shodan oder Cenys auch, wie viele Smart Home Komponenten mehr oder weniger einfach über das Internet zugänglich sind. Ein im Oktober hierfür gestarteter Scan fand bis heute mehr als 68.000 offene Web-Schnittstellen von bekannten Smart-Home-Komponenten, die vor allem in Privathaushalten eingesetzt werden. Darunter drahtlose Fensterkontakte, Rauchmelder, automatische Türschließanlagen oder Kamerasysteme. Alle gefundenen Geräte waren über das Internet leicht zugänglich. Die Ergebnisse wurden mithilfe einer „Heatmap“ visualisiert, die zeigt, dass sich die IoT-Technologie in Städten und urbanen Zentren wie Berlin, Hamburg, Köln, Frankfurt oder München konzentriert, während sie in ländlichen Gebieten weniger verbreitet ist.

"Diese Ergebnisse zeigen wie wichtig es ist, bei der Installation und Einrichtung eines Smart Homes vorsichtig zu sein", sagt Michael Veit, IT-Sicherheitsexperte bei Sophos. "Ansonsten ist die Chance hoch, dass zu Halloween nicht nur Bonbon-heischende Geister an der Tür klingeln, sondern echte Cyber-Gangster im Smart-Home-Netzwerk nach Geld und Daten suchen."

8 Tipps für ein Spuk-freies Smart Home:

1. **My Home(network) is my Castle:** Niemals das Heimnetz mit anderen teilen!
2. **IoT-Geräte möglichst raus aus dem Heimnetzwerk**: Ein Beispiel: wenn hauptsächlich über Kabel oder Antenne empfangen wird, kommt das Fernsehgerät auch ohne WLAN aus.
3. **Separates Netzwerk für IoT-Geräte**: Wenn der WLAN-Router verschiedene Netzwerke (Segmentierung) erstellen kann, sollte ein spezielles Netzwerk für IoT-Geräte aufgebaut werden, das den Zugriff auf andere Bereiche des Netzwerks unterbindet.
4. **„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.

5. **Verwendung einer sicheren VPN-Technologie**: Statt einer ungesicherten Port-Weiterleitung eines Routers für den Fernzugriff auf die IoT-Geräte aus dem Internet ist es besser, eine sichere VPN-Technologie für Smartphones oder Mac / PC zu verwenden.
6. **Software Updates**: Es sollte immer die aktuelle AV-Software auf allen PCs, Macs und Android-Smartphones installiert sein. Kostenlose Tools wie Sophos Home oder Sophos Mobile Security sind auf der Sophos Website verfügbar.
7. **Mehr Sicherheit durch neueste Firmware**: Nicht nur PCs, Laptops oder Smartphones, auch jedes IoT-Gerät muss mit der aktuellsten Firmware für einen sicheren Betrieb ausgerüstet sein. Der Aufwand lohnt sich in Bezug auf Sicherheit und Privatsphäre.
8. **Google ist dein Freund**: Es ist sinnvoll vor dem Kauf nach potenziellen Sicherheitslücken der IoT-Geräte zu suchen, die man verwenden möchte. Eine Google-Suche gibt einen schnellen und guten Überblick, wenn das Produkt der Wahl bereits im Fokus von Hackern steht oder gar gehackt wurde.

Also auch für Smart-Home-Besitzer gilt (nicht nur) zu Halloween: Süßes oder Saures – man hat es selbst in der Hand.

Links:

- Sophos XG Firewall Home Edition Firewall: https://www.sophos.com/de-de/products/free-tools/sophos-xg-firewall-home-edition.aspx
- Sophos Home: https://home.sophos.com/de-de
- Sophos Mobile Security: https://www.sophos.com/de-de/products/free-tools/sophos-mobile-security-free-edition.aspx

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