Hacken erwünscht: Smart-Home-Honeypot „Haunted House“

Langzeit-Hacking-Studie für das Internet der Dinge (IoT) im Smart Home geht mit Auftritten bei G20-Konferenz des BMWi und der CeBIT live

Wiesbaden, 2. März 2017 – Sophos startet gemeinsam mit Koramis, einem spezialisierten Unternehmen im Bereich Automation und Security, eine neue interaktive Studie rund um Hacking und Cyber-Gefahren im Umfeld des Internet der Dinge (IoT). Im Mittelpunkt steht ein Smart-Home-Modellhaus, in das handelsübliche Steuerungssysteme und IoT-Komponenten, beispielsweise für Licht, Heizung, Alarmanlagen oder Überwachungskameras, installiert sind. Wie heute bereits in vielen Privathaushalten aber auch Geschäftsgebäuden üblich, sind die einzelnen Smart-Komponenten über das Internet steuerbar. Im Modellaufbau „Haunted House“ werden die Art und Anzahl der Manipulationsversuche durch Hacker und Cyberkriminelle, die einzelne Komponenten im Haus zu übernehmen versuchen, überwacht und live sichtbar gemacht.

Das Haunted House ist erstmals am 16. und 17. März 2017 in Berlin auf der BMWi-Konferenz „Digitising Manufacturing in the G20“ live zu sehen; sowie im Anschluss auf der CeBIT 2017 am Sophos-Stand (Halle 6, Stand F18). Erfolgreiche Manipulationen finden in Echtzeit statt, indem beispielsweise am Modell ein Rollladen auf- oder das Licht angeht. Der Honeypot ist über mehrere Wochen online, am Ende des Projekts werden Art, Frequenz und soweit möglich die Herkunft der Angriffe ausgewertet. Parallel scannen die Experten das Internet nach tatsächlich verfügbaren Smart-Home-Komponenten und beziehen diese Ergebnisse in die Analyse ein. Die Ergebnisse dieser Untersuchung werden in einem White Paper zusammengetragen, das Aufschluss über die Qualität, Quantität und Aggressivität von Angreifern sowie mögliche physischen und personellen Gefahren gibt.

„In Kurztests einzelner handelsüblicher Smart-Home- und IoT-Business-Komponenten haben wir sehr schnell Manipulationsversuche über das Internet festgestellt. Wir gehen davon aus, dass ein ganzes Haus mit unterschiedlichsten Smart-Komponenten sehr schnell und häufig angegriffen wird. Damit wollen wir mit unserem Haunted House live veranschaulichen, welchen Gefahren sich sowohl Privatpersonen als auch Unternehmen mit ungeschützten IoT-Geräten aussetzen“, sagt Michael Veit, Security-Spezialist bei Sophos.

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 +49-172-4536839
sophos@tc-communications.de