„Bonjour, Madame!“– wenn Hacker die eigene Webcam übernehmen. Das gruselige Fundstück der Woche.

Die mit dem Internet verbundene Kamera einer Niederländerin fing plötzlich an, mit ihr zu sprechen. Geschockt nahm sie den Dialog mit dem Hacker auf und veröffentlichte ihn. Damit sich dieser Schreckmoment nicht wiederholt, gibt Sophos drei bewährte IoT-Tipps.

Wiesbaden, 17. Oktober 2017. „Bonjour Madame!“ – geschockt beschreibt die Gefühlslage von Rilana H. vielleicht am besten, als ihre WiFi-fähige Kamera sie aus dem Nichts heraus beim Hausputz begrüßt. Ein Hacker hatte die Kontrolle über das IoT-Gerät übernommen, das die Niederländerin vor ein paar Monaten bei einer lokalen Discounterkette günstig erstanden hatte. Sie packte die Kamera in die Box zurück, erzählte ihrer Freundin am Abend davon und wollte den Spieß umdrehen: sie stellte die Kamera wieder auf, mit Blick auf die Wand gerichtet, und filmte mit ihrem Handy, wie der Hacker erneut Kontakt aufnahm. Den Dialog veröffentlichte sie vor Kurzem auf Facebook.

Einmal mehr stellt sich bei solchen Geschichten die Frage, ob sie real oder ein Hoax sind. Aber unser Instinkt deutet an, dass es so gewesen sein könnte. Es wäre schließlich nicht das erste Mal, dass eine nicht gesicherte Webcam sich selbständig umschaut. Es existiert eine große Fundgrube an einfach aufzuspürenden und sehr schwach gesicherten Kameras, die Hacker für ihre Zwecke nutzen können. Auf bestimmten Webseiten haben Cyber-Plünderer eine Vielzahl an Feeds zur Auswahl, die von Geräten raubkopiert wurden. Bereits 2014 berichtete Sophos auf seinem Blog „Naked Security“ über eine Seite, die Feeds von Babyüberwachungsmonitoren in Kinderzimmern und von Sicherheitswebcams anbot. Hier konnte man live in Schlafzimmer, Büro, Geschäfte, Restaurants, Fitness-Studios und Schwimmbäder schauen.

Shodan – die Suchmaschine für IoT – nutzen die Cyberkriminellen dabei geschickt für sich: sie suchen gezielt nach mit dem Netz verbundenen Geräten aller Art inklusive deren angreifbarer Kameras. Shodan stellt dabei erst kürzlich verbundene Geräte an die Spitze der Suchergebnisse. Vielleicht war so auch die Kamera der Niederländerin nur das erste erreichbare Ziel der Hackersuche.

Sophos rät für die Verwendung von Webcams oder anderen internetfähigen Geräten und gadgets deshalb auf folgende drei Schritte zu achten:

1. Kameras oder andere IoT-Geräte sollten mit einem Passwort geschützt werden können.

2. IoT-Geräte sind bekannt dafür, dass im Auslieferungszustand ein sehr einfaches Standardpasswort eingerichtet ist. Das Standardpasswort zu verwenden, ist wie kein Passwort zu verwenden. Lieber schnell durch ein gutes ändern. Letztendlich ist es wie beim herkömmlichen Einbruch: bekommt der Dieb die Tür nicht innerhalb kürzester Zeit auf, lässt er es und geht zur nächsten. Diese erste Hürde sollte man ihm deshalb so schwer wie möglich machen.

3. Darüber hinaus sollte sich jeder Anwender genau überlegen, was er von seiner Privatsphäre im Internet Preis geben möchte und was die Konsequenzen sein

könnten. Wer weiß, was sich der Hacker alles hätte anschauen können, hätte er zur Niederländerin nicht aktiv Kontakt aufgenommen.

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