Wasch- und Saug-Alarm – Kurioses aus der IoT-Welt

Das Internet der Dinge ist phantastisch und bietet Anwendern ungeahnte Möglichkeiten. Manche Funktionen sind fragwürdig und nicht selten entstehen für den Anwender Security-Probleme.

Wiesbaden, 1. August 2017 – Man könnte meinen, dass das Internet of Things (IoT) gerade im privaten Umfeld aufgrund von Unwissenheit oder Sorglosigkeit zur Security-Gefahr werden kann, aber weit gefehlt. Auch im Business Umfeld zeigt sich das IoT immer wieder von seiner schlechtesten Seite. Folgend drei kuriose Beispiele, wie IoT nicht sein sollte:

Waschstraße mit Eigenleben
Wer heute mit seinem Auto in eine Waschstraße fährt, kann sein nasses Wunder erleben. Analysten verzeichnen eine steigende Anzahl an Waschstraßen, die an das Internet angeschlossen sind. Grund für die Anbindung sind Konfigurationsmöglichkeiten für die Waschprogramme und Alarme im Falle eines Fehlers. Das Fatale an der Sache: genau wie zahlreiche andere IoT-Geräte sind auch viele Waschstraßen nur mit dem Standardpasswort mit dem Server verbunden. Steckt man in einer verrückt gewordenen Waschstraße fest, die völlig andere Waschprogramme fährt oder einen nicht mehr heraus lässt, ist ein Hacker-Angriff durchaus wahrscheinlich.

Security Alarm mit alarmierender Security
Der Sinn einer Alarmanlage ist eindeutig: die Sicherheit von Räumen oder Gebäuden zu erhöhen. Doch weit gefehlt. Analysten fanden Alarmsysteme, die zwar das Gebäude absichern und im Ernstfall auch Alarm schlagen und den Eigentümer umgehend über Einbruchsversuche per Mail oder App benachrichtigen. Aber: dafür sollen laut manchen Herstellern bestimmte Ports in das Internet geöffnet werden. Die Kommunikation über das Internet erfolgt weitgehend ungeschützt. Eine Einbruchsgefahr verhindern, indem man eine nächste schafft - ein Schildbürgerstreich.

Der Spion im eigenen Haus
Was wäre unser Leben ohne die vielen kleinen Helferlein im Haus, so auch neuerdings der Staubsaugroboter. Heikel daran ist, dass Staubsaugroboter nun auch mit dem Internet verbunden sind – manche auch über Spracheingabesysteme. Einige Hersteller sammeln völlig ungeniert große Mengen an Daten über das traute Heim, darunter die Abmessungen der Räume oder wo im Raum Dinge stehen. Gerüchten zufolge könnten Hersteller von Staubsaugrobotern Kontakt mit den großen drei Internetgiganten aufgenommen haben, um die gesammelten Daten gemeinsam zu „nutzen“. Also nicht wundern, wenn einem beim nächsten Surfen im Internet eine Schrankwand empfohlen wird – unter dem Motto „Könnte bei Ihnen zwischen Fenster und Sofa stehen.“

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