Alexa, wer war der Mörder?

Wiesbaden, 23. Februar 2017 – Das Internet der Dinge (IoT) ist definitiv in unseren Haushalten angekommen und irgendwie fühlt man sich schon fast wie auf der Brücke vom Raumschiff Enterprise. Coole Gadgets steuern vieles per Stimme, wofür wir normalerweise ein paar Schritte wie beispielsweise zum Lichtschalter oder zur Stereoanlage tun müssten – alles ganz einfach per Sprachbefehl oder Frage.
Damit diese beeindruckenden persönlichen Assistenten funktionieren benötigen sie das Internet und das nicht nur, um Musik abzuspielen oder eine Antwort zu geben. Sie nehmen alle Befehle auf und speichern diese. Erst so können Hersteller von Echo/Alexa, Siri, Cortana oder Google Home die Qualität der sprachlichen Interaktion weiter verbessern und den Geräten noch mehr Beeindruckendes beibringen.

In einem jüngeren Fall in USA wollte sich die Polizei derartiger Sprachaufnahmen einer Anwenderin zunutze machen. In Zusammenhang mit einem Mord verlangte die Polizei sämtliche Sprachaufnahmen des Amazon Echo-Geräts in der Hoffnung, Hinweise zur Aufklärung der Tat zu erhalten. Doch Amazon hat sich an den Datenschutz gehalten und geweigert, die entsprechenden Sprachaufzeichnungen herauszugeben. Dieser Fall zeigt, dass bestimmte Einrichtungen ein valides Interesse an derartig gespeicherten Informationen haben. Es ist aber auch leicht vorstellbar, dass Cyber-Kriminelle eine lohnende Einnahmequelle durch Erpressung daraus entwickeln könnten.

Hundertprozentige Privatsphäre ausgeschlossen
Anwender, die solche Technologien zuhause oder im Büro einsetzen, dürfen nicht mit einer hundertprozentigen Privatsphäre rechnen. Aber es gibt ein paar Dinge, auf die Benutzer achten sollten, um zumindest etwas mehr Sicherheit zu erhalten:

1. Wenn Echo nicht genutzt wird, sollte die Stummtaste aktiviert sein. Die Stummschaltung befindet sich direkt am Gerät. Das "immer hörende" Mikrofon wird somit abgeschaltet, bis es wieder aktiviert wird.
2. Man sollte Echo nicht mit sensiblen Accounts verbinden. Es gab bereits einige Fälle in denen die Verkettung von mehreren Accounts zu unschönen Überraschungen oder Tränen geführt haben. Ein Kontrollverlust wie beispielsweise bei Bestellungen ist schnell geschehen.
3. Alte Aufnahmen sollten gelöscht werden. Bei Echo beispielsweise können auf dem Amazon-Konto unter "Manage my Device" über ein praktisches Dashboard einzelne Abfragen oder der gesamten Suchverlauf gelöscht werden.
4. Google-Settings sollten restriktiv eingestellt sein. Wer Google Home verwendet, kennt das immense Datensammelverhalten des Unternehmens. Aber immerhin bietet Google auf der Webseite diverse Einstellmöglichkeiten an, um Berechtigungen zu erlauben oder zu entziehen. Darüber hinaus verfügt auch Home über eine Mute-Taste.

„Systeme wie Amazon Echo/Alexa oder Google Home sind faszinierend und werden sich in unserer technisch affinen Welt sehr schnell verbreiten. So angenehm und interessant sie unser Leben auch gestalten, die Nutzer sollten unbedingt auf Sicherheit und Privatsphäre achten. Hier ist jeder einzelne Nutzer gefragt, aktiv darüber nachzudenken, welche Informationen er preis gibt und welche nicht“, sagt Michael Veit, Security-Experte bei Sophos.

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. 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