Das Internet der Dinge ist kein Kindergeburtstag – Vier Tipps von Sophos zu Anschaffung und Haltung eines Cloudpets

Hunderttausende Sprachnachrichten von Eltern und Kindern standen ungeschützt im Netz - diese Information sorgte vor Kurzem für große Aufregung. Ein Paradebeispiel für fehlendes Sicherheitsbewusstsein beim Trendthema Internet der Dinge. Damit sich alle Familienmitglieder mit einem Cloudpet sicher fühlen können, gibt Sophos Anschaffungs- und Haltungstipps.

Wiesbaden, 30. März 2017. Der Siegeszug des Internet of Things scheint unaufhaltbar – ebenso wie die nachschwappende Sicherheitslückenwelle. Der Grund dafür ist die immer noch stiefmütterliche Behandlung bei der Absicherung der kleinen Minicomputer. Der Trend macht vor keiner Branche halt und sorgte in den letzten Tagen vor allem bei Kinderspielzeug für Aufregung. Nachdem die Bundesnetzagentur vor kurzem die mit dem Internet verbundene Puppe Cayla vom deutschen Markt genommen hatte, stehen nun die „Cloudpets“ im Fokus. Nach verschiedenen Berichten standen mehrere Hunderttausend Accounts ungeschützt im Netz und ließen Hacker so zum Beispiel ohne Probleme auf die von der Puppe aufgenommen Sprachnachrichten von Eltern und Nachwuchs zugreifen.

Hier haben wir nun ein weiteres, perfektes Bespiel, was beim Internet der Dinge alles schief gehen kann – in diesem Fall, weil die Backend-Systeme, mit denen die Spielzeuge verknüpft sind, nicht ausreichend oder vielleicht sogar gar nicht geschützt waren. Im Fall Cloudpets ist das besonders enttäuschend, da es quasi zum Nulltarif möglich gewesen wäre, die Datenbanken mit einem vernünftigen Passwort zu schützen. Solange die Hersteller von IoT-Geräten Sicherheit und damit die Privatsphäre der Anwender nicht ernst nehmen, muss man davon ausgehen, dass solch feindliche Übernahmen kein Einzelfall bleiben.

Doch auch als Anwender muss man die IoT-Welle nicht völlig unbedarft „mitsurfen“ und sollte sich über einige Fakten bewusst sein. Für die Preise, die beispielsweise IoT-fähige Spielzeuge kosten, ist es unmöglich, ausreichend Computing-Power zu integrieren, um das Gerät unabhängig interagieren zu lassen. Die Folge ist die ständige Verbindung mit dem Internet und das Hin- und Herschicken von Daten jeglicher Art, um Herauszufinden, was die Stimme aus dem Off denn nun eventuell gesagt hat.

Das Bewusstsein für konstante Überwachung dieser Art ist schon bei Erwachsenen oftmals schwach ausgeprägt und bei Kindern nochmals weniger vorhanden.
Hier gilt es, verantwortungsvoll zu handeln und jegliches Onlinestellen neuer Geräte gründlich zu überdenken. Das Motto sollte lauten: „Wenn es Zweifel gibt, lieber lassen!“

Und wenn es dann doch das neueste Gadget sein soll, bitte folgendes beachten:

1. Halten Sie Ihr Online-Netzwerk exklusiv
Verbinden Sie keine Geräte mit Ihrem Online-Netzwerk, wenn es nicht nötig ist. So muss der TV zum Beispiel nicht übers WLAN laufen, wenn dort sowieso nur Fernsehen via Kabel oder Antenne geguckt wird.

2. Gastnetzwerk für IoT-Geräte einrichten
Falls Ihr WiFi-Router es ermöglicht, verschiedene Netzwerke einzurichten, sollten Sie ein „Gastnetzwerk“ für Ihre IoT-Geräte einrichten und damit den Zugang zum regulären Netzwerk verwehren.

3. Aktualisieren Sie auch die IoT-Software
Nicht nur ihr PC oder Laptop, auch IoT-Geräte müssen aktuelle Versionen laufen haben, um möglichst sicher zu sein. Das kann teilweise zeitaufwändig sein, lohnt sich aber dennoch in Hinblick auf die Sicherheit Ihrer Privatsphäre.

4. Vor dem Kauf: Google-Suche zu Hackerinfos
Last but not least lohnt sich auch eine schnelle Google-Suche, wenn Sie sich ein neues IoT-Gerät anschaffen wollen. Hier erhält man einen guten Überblick, ob das Produkt der Wahl eventuell schon im Fokus der Hacker steht oder sogar bereits gehackt wurde.

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