SOPHOS

Wie gefährlich sind sprechende Spielzeuge?

Immer mehr Spielzeuge sind für die Kommunikation mit ihren kleinen Besitzern ausgelegt. Sie verfügen über eine Spracherkennung und sie sind lernfähig. Um diese Funktionen erfüllen zu können, benötigt das Kuscheltier aber eine Internetverbindung. Sophos klärt über die Risiken auf.

Sprechende Spielzeuge sind bei großen und kleinen Kindern beliebt. Klassiker von früher, wie Mikado und Mensch ärgere dich nicht – jetzt im Hello Kitty Design – sind zwar noch immer angesagt, aber elektronisches Spielzeug hat seinen festen Platz im Regal und auch der Osterhase wird neben den Schokoladeneiern einige der neuesten elektronische Spielereien verstecken. Viele der neuen Spielzeugmodelle benötigen einen Internetzugang.

Einige sind für sehr junge Kinder konzipiert, wie beispielsweise die smarte Ente namens Edwin. Edwin ist eines der lernenden Spielzeuge. Es ist mit einer App verbunden und begleitet das Kind durch Spiele, singt Kinderlieder oder misst die Temperatur des Badewassers. Für Kinder, die bereits sprechen können, gibt es Spielzeuge, die mit ihnen eine Konversation führen. Ein WLAN-fähiger Teddybär mit einem Mikrofon und integrierten Lautsprechern ermöglicht Eltern, mit ihren Kindern von unterwegs über ihr Smartphone zu plaudern.

Der Smart Toy Bär verwendet maschinelles Lernen und Spracherkennung, der Zugang erfolgt über eine WLAN-Verbindung. Das Spielzeug erinnert sich beispielsweise an die Lieblingsspiele des Kindes, es antwortet wenn es angesprochen wird, erzählt Witze und hilft dem Kind laut Hersteller auch bei seiner sozialen und emotionalen Entwicklung. Eigentlich ganz cool, allerdings kann mit einem sprechenden Bär mit Internetverbindung und auch viel schief gehen.

Sicherheitsforscher haben bei einem Smart-Toy Bär von Fisher Price Sicherheitsmängel entdeckt, über die der Name des Kindes, Geschlecht, Geburtsdatum und andere persönliche Daten in fremde Hände gelangen können.

Eine weiteres internetfähiges Spielzeug, das bei Groß und Klein für Furore sorgt, ist das sprachgesteuerte „Barbie Dream-House“, ein Smart-Home für die schon länger plauderfähige „Hello Barbie“, das im Herbst auf den deutschen Markt kommen soll. Die Haustechnik, inklusive eingebautem Aufzug, wird per Sprachsteuerung bewegt und auch Backofen und Dusche reagieren auf Kommando. Ein technischer Traum in Pink. Auch das Barbie-Modell hat eine WLAN-Verbindung, die sich mit dem Server des Herstellers Mattel verbindet wenn die Spracherkennung arbeitet und eine von 8000 Zeilen vorprogrammierter Antworten gibt. Bereits im Dezember entdeckten Sicherheitsforscher vielfache Sicherheitsmängel in der „Hello Barbie“, inklusive dem POODLE bug, den Angreifer nutzen können, um Barbies Kommunikation über das Internet abzugreifen.

Es gibt derzeit keine Hinweise darauf, dass diese Sicherheitsmängel von Hackern bereits verwendet wurden. Das Speichern von Kinderdaten in Spielzeugfirmen gibt dennoch Anlass zur Sorge. Im November 2015 drangen Hacker in das Datennetz der Marke VTech ein und stahlen Millionen von persönlichen Datensätzen von VTechs Kid Connect-Kunden. Dieser Dienst ermöglicht es Eltern, mit ihren Kindern über eine App auf deren Tablet zu kommunizieren. Zu den gestohlenen Daten gehörten E-Mail-Adressen, Namen und Passwörter von über vier Millionen Usern. Angreifer könnten darüber Bilder von Eltern und Kindern, Chat-Logs und Audioaufnahmen der Kinderstimmen abgreifen.

„Eltern denken immer und bei all ihren Entscheidungen an die Sicherheit ihrer Kinder und nun hat sich ein weiteres Gefahrenfeld aufgetan“, erklärt Chester Wisniewski, Senior Security Advisor bei Sophos. „Eltern müssen sich fragen, ob ein Plausch mit einem Teddybären es wert ist, die persönlichen Daten dafür einer Gefahr auszusetzen.“

Und natürlich gilt es nicht nur Spielzeuge abzusichern, sondern auch die klassischen, ans Internet angeschlossenen Geräte wie PC oder Smartphone. Hierbei hilft die für Privatnutzer kostenlose Lösung Sophos Home. Hinweise dazu, wie Eltern die Nutzung von Smart Toys sicherer machen können, finden Sie hier: http://sophosblog.de/mehr-sicherheit-im-internet-der-dinge/

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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de