Medienmiteilung

Smart Toys: Eltern müssen Risiken kennen und Verantwortung übernehmen

Experte Mirko Ross erklärt Eltern, worauf sie unbedingt achten sollten

Stuttgart, 18.12.19. Sprechende Puppen und appgesteuerte Autos liegen voll im Trend. Aber sie können weit mehr als Kinder begeistern. Denn über Smart Toys lassen sich Daten ausspionieren, Werbebotschaften einspielen oder im schlimmsten Fall: Kontakt zum Kind herstellen. Mirko Ross, Experte für Cybersicherheit, appelliert an die Eltern, Verantwortung zu übernehmen und sich aktiv um die Sicherheit von interaktivem Spielzeug zu kümmern !

Auf dem Wunschzettel vieler Kinder stehen zu Weihnachten Smart Toys ganz oben. Das singende Hundebaby und der sprechende Teddybär versprechen großen Spaß. Den Eltern ist allerdings oft nicht bewusst, dass durch die Anbindung von Spielzeug ans Internet ein erhebliches Sicherheitsrisiko mit teils verheerenden Folgen entstehen kann. Gelingt es Cyberkriminellen, ein IoT-Gerät zu übernehmen, ist dies oftmals ein Einfallstor in weitere Geräte und Dienste.

„Man darf sich von der Spielzeugoptik dieser Dinge nicht einlullen lassen“, warnt Mirko Ross, renommierter Experte und Aktivist für Cybersicherheit im Internet of Things. „Eine sprechende Puppe ist nichts anderes als ein kleiner Computer mit Firmware, Schnittstellen und der Fähigkeit, Daten zu verarbeiten und zu speichern. Wenn man bei der Koppelung mit dem Internet nicht sorgfältig auf die Sicherheit achtet, kann das IT-Innenleben der Puppe von Dritten ausgelesen oder manipuliert werden. Das müssen Eltern auf dem Schirm haben und entsprechend verantwortungsvoll handeln.“

Die erste Frage hinsichtlich der Sicherheit stellt sich beim Kauf des Spielzeugs. Der Hersteller sollte bestimmte sicherheitsrelevante Vorgaben erfüllen. Dazu gehört zum Beispiel die Möglichkeit, Funkverbindungen wie Bluetooth und Wifi mit einem Passwort zu verschlüsseln und die regelmäßige Aktualisierung der Software durch Updates. Billige No-Name-Produkte haben in der Regel solche Sicherheitsfeatures nicht. Deshalb rät Mirko Ross, lieber etwas mehr Geld in die Hand zu nehmen und Smart Toys nur von renommierten Markenherstellern zu kaufen.

Wenn das Spielzeug ausgepackt ist, müssen sich zunächst die Eltern damit beschäftigen.
Aus Marketinggründen machen viele Hersteller die Inbetriebnahme der Geräte so einfach wie möglich. Oft ist das Spielzeug deshalb bereits mit einem Standardpasswort ausgestattet und kann damit sofort online gehen. Diese Passworte können sich Angreifer ohne Probleme beschaffen. Deshalb ist es unumgänglich, Zeit und Geduld zu investieren, um das Gerät vor dem Spieleinsatz nach den Angaben des Herstellers sorgfältig zu konfigurieren. Dazu gehört auch, es mit einem sicheren Passwort zu versehen.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Ein sicheres Passwort muss aus einer zufälligen Kombination von Buchstaben, Ziffern und Sonderzeichen erstellt werden und mindestens 16 Zeichen lang sein. Auf keinen Fall darf man naheliegende und damit unsichere Passworte wie „Puppe“, „Teddybär“ oder den Vornamen des Kindes verwenden.

Wird das Gerät über einen Router mit dem Internet verbunden, ist es sinnvoll, die Einstellungen so zu wählen, dass gängige Ports z.B. für Fernwartungszugriffe geschlossen werden und somit unerreichbar für schnüffelnde Scanner und Angreifer sind. Schließlich sollte man klären, ob das Spielzeug automatisch vom Hersteller mit Updates versorgt wird oder ob man Updates selbst herunterladen muss – und das dann auch tun!

Ist ein sorgfältig konfiguriertes Smart Toy tatsächlich sicher? Dazu Mirko Ross: „Solange der Hersteller nicht für Schäden haften muss, die durch unsichere Geräte verursacht werden, werden sich die Risiken im Internet der Dinge nicht wesentlich reduzieren lassen. Denn als Laie kann man nicht einschätzen, welche sicherheitsrelevanten Schwachstellen eine Software hat und deshalb keine entsprechenden Maßnahmen treffen. Auch beim Thema Datenschutz gibt es viele Fragezeichen. Wenn ich zum Beispiel eine App herunterlade und dort als Vater meine persönlichen Daten und die des Kindes eingebe, hätte ich große Bedenken, ob der Hersteller verantwortlich mit den Daten umgeht. In der Vergangenheit wurden entsprechende Daten leider sehr oft unverschlüsselt in Cloud-Servern außerhalb Europas gespeichert und verarbeitet. Im Zweifelsfall würde ich ein solches Produkt lieber zurückgeben. Die Frage ist dann nur, wie erkläre ich das meinem Kind...“

Abdruck honorarfrei, Beleg (Print, Scan) oder Link erbeten.

Mirko Ross ist iX-Autor und Gründer sowie CEO des Start-ups asvin und der digital worx GmbH. Für die Sicherheit im IoT engagiert er sich als Mitglied der Expertengruppe für Sicherheit im Internet der Dinge der Europäischen Agentur für Netzwerk- und Informationssicherheit ENISA. Darüber hinaus ist er Mitglied des Internet Of Things Council, einem weltweiten IoT-Think-Tank, und Projektkoordinator im eHealth-Forschungsprojekt MITASSIST.

Image

Kontakt
seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: +49 7181 / 26 29 376
E: medien@seidel-kommunikation.de