Medienmitteilung Stuttgart 13.12.2019

„Hier spricht der Nikolaus“: Überwachungskamera im Kinderzimmer gehackt – Wie können Eltern ihre Kinder vor Angriffen durch Hacker schützen?

Mirko Ross, Experte für Cybersicherheit, gibt im Interview die besten Tipps

Eltern auf der ganzen Welt sind schockiert: Wie das Fachmagazin WIRED gestern berichtete, wurde die achtjährige Tochter einer Familie in Memphis, Tennes- see, von einem Fremden über eine Überwachungskamera des Herstellers Ring im Kinderzimmer belästigt. Der Hacker meldete sich mit den Worten „Ich bin der Nikolaus“ und gab dem Mädchen dann Anweisungen, ihr Zimmer zu verwüsten und das Fernsehgerät kaputt zu machen.

Frage: Herr Ross, ist solch ein Hackerangriff auch in unseren Kinderzimmern denkbar?

Mirko Ross: Leider ja, denn Hackerangriffe auf Geräte, die mit dem Internet verbunden sind, kommen überall auf der Welt vor, dagegen kann uns weder der Netzbetreiber noch der Gesetzgeber wirklich schützen.

Frage: Wie ist es möglich, dass ein Hacker zu einem Kind Kontakt aufnimmt?

Mirko Ross: Viele Verbraucher sind schnell damit überfordert, smarte Produkte so sicher zu betreiben, dass kein Hacker von außen zugreifen kann. Solche Zugriffe sind z.B. über so genannte Smart Toys ziemlich einfach, wenn diese nicht ordentlich gesi- chert sind. Smart Toys sind Spielsachen wie Puppen oder Teddybären, die mit Mikrofo- nen und teilweise mit Kameras ausgestattet sind und per Smartphone oder Router mit dem Internet verbunden werden. Durch die Internetanbindung können sie interaktiv mit den Kindern kommunizieren. Sofern ein solches Spielzeug bzw. Gerät nicht durch ein sicheres Passwort geschützt wird, ist es für einen Hacker ein Kinderspiel, das Gerät

zu kapern. Damit ist es möglich, Daten auszuspionieren, Werbebotschaften einzuspielen, das Kind zu filmen oder auch schlimmstenfalls direkt mit ihm zu sprechen.

Frage: Was kann ich als Vater oder Mutter tun, um mein Kind vor Angriffen zu schützen?

Mirko Ross: Eltern müssen sich zunächst einmal der Gefahren bewusst sein. Das bedeutet schon beim Kauf: Finger weg von billigen No-name-Produkten. Besser ist es, Smart Toys nur von renommierten Markenherstellern zu kaufen. Wenn ich mir nicht sicher sein kann, was ich da kaufe, würde ich persönlich im Zweifelsfall lieber darauf verzichten.

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

Frage: Ist ein solches Markenprodukt dann tatsächlich sicher?

Mirko Ross: Darauf würde ich nicht vertrauen. Die Industrie will die Inbetriebnahme der Geräte so einfach wie möglich machen. Oft ist das Spielzeug deshalb bereits vom Hersteller mit einem Standardpasswort ausgestattet und kann damit sofort online gehen. Diese Passworte können sich Angreifer ohne Probleme beschaffen. Deshalb muss man sich auf jeden Fall die Zeit nehmen und das Gerät zunächst nach den Angaben des Herstellers selber konfigurieren. Dazu gehört auch, es mit einem eigenen Passwort zu versehen. Ein sicheres Passwort sollte 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. Darüber hinaus sollte jemand, der sich gut mit Routern auskennt, dafür sorgen, dass das Gerät nicht von außen und damit für Angreifer sichtbar ist. Ein dritter wichtiger Punkt sind Software-Updates: Man sollte herausfinden, ob das Spielzeug automatisch mit Updates versorgt wird oder ob man die Updates selbst herunterladen muss – und das dann auch tun!

Herr Ross, wir danken für das Gespräch!

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 Informati- onssicherheit ENISA. Darüber hinaus ist er Mitglied des Internet Of Things Council, einem weltweiten IoT-Think-Tank, und Projektkoordinator im eHealth-Forschungsprojekt MITASSIST.

Bild:

Portrait Mirko Ross, CEO asvin GmbH

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

Kontakt:

seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (bei Stuttgart)
T: +40 (0)7181 / 26 29 376
E: medien@seidel-kommunikation.de