Smarte Spielzeuge auf dem Gabentisch?
Bitte nur mit Sicherheits-Check vorab

Jedes Jahr sind Eltern auf der Suche nach dem ultimativen, besonderen Geschenk und die Spielwarenindustrie bietet ihnen im Bereich des Digitalen eine große Auswahl an Tablets, Lern-Computern und Smart Toys. Wer einem jungen Menschen zu Weihnachten ein mit dem Internet verbundenes „intelligentes" Spielzeug schenken möchte, sollte auf versteckte und schwerwiegende Sicherheitsrisiken achten, die bei manchen Gadgets quasi im Kauf inbegriffen sind.

Längst nicht jedes internetfähige Spielzeug sollte bedenkenlos auf dem Gabentisch liegen. Denn im Zusammenhang mit dem Internet of Things (IoT), zu dem auch smarte Spielzeuge gehören, gibt es seit Jahren immer wieder größere Sicherheitsprobleme. Das bestätigt auch die Bundesnetzagentur. Viele dieser Produkte werden auf Softwareebene übereilt zusammengeschustert, was dazu führt, dass sowohl die Sicherheit des Geräts als auch die der Online-Konten miserabel ist. Und nur wenige werden für Schwachstellen gepatcht.

Eltern, Großeltern oder Freunde sollten sich daher vor dem Kauf smarter Spielzeuge ein paar Fragen stellen, um zur Bescherung eine böse Überraschung zu vermeiden:

- Welche Daten werden vom Hersteller erhoben und wie werden sie weiterverarbeitet?
- Wie lauten die Datenschutzbestimmungen für das Spielzeug und für die zugehörigen Apps?
- Welche Zugriffsrechte sind für das Spielzeug und die zugehörigen Apps vorgesehen?
- Lassen sich Kameras oder Mikrofone abschalten?
- Ist die Internetverbindung konstant oder kann sie getrennt werden?
- Wie sieht es mit einem Passwortschutz aus, ist dieser vorhanden und kann dieser geändert werden?
- Gibt es Updates für das Produkt, welche nicht nur das Spielerlebnis, sondern auch die Sicherheit verbessern?

Die Einschätzung von Michael Veit, Security-Experte bei Sophos: „Unser erster Rat ist, bei Spielzeugen in Verbindung mit einer App oder einem Online-Dienst die Geschäftsbedingungen sehr genau zu prüfen, um herauszufinden, ob es sich um eine Mogelpackung handelt. Wer ein vernetztes Spielzeug kauft, kann nicht wissen, wie sicher es ist, weder bei der lokalen Anwendung noch bei der Übertragung der gesammelten Daten an entfernte Server. Wenn es von Anfang an nicht gut gesichert ist, gibt es keine Garantie, dass Probleme irgendwann erkannt und behoben werden. Unser zweiter Rat ist, vor dem Kauf eine Internet-Suche nach dem Spielzeug und seinem Hersteller durchzuführen, um bekannte Probleme zu ermitteln."

Für eine verantwortungsvolle Nutzung sollten die Schenkenden einige Tipps für den Umgang mit intelligentem Spielzeug beachten:

- Verwenden Sie solche Spielzeuge nur in einer vertrauenswürdigen Umgebung, zum Beispiel zu Hause. Damit kann verhindert werden, dass persönliche Informationen von Unbefugten abgefangen werden.
- Verbinden Sie internetfähige Spielzeuge nur mit einem passwortgeschützten WLAN und zudem nur dann, wenn eine Online-Verbindung für die Nutzung unbedingt notwendig ist.

- Viele Spielzeuge benötigen zwar Internet, jedoch nicht den Zugang zu sensiblen Daten. Sie in das Gastnetz einzubinden, reicht in den meisten Fällen aus und verhindert den unkontrollierten Zugriff auf private Daten.
- Achten Sie darauf, falls vorhanden, einen Zugriffsschutz zu aktivieren, um den Missbrauch von Daten zu verhindern, wenn das Spielzeug in fremde Hände gerät.
- Wenn das Spielzeug mit einer App oder Benutzeroberfläche ausgestattet ist, ändern Sie wenn möglich den Benutzernamen und setzen Sie ein sicheres Passwort (bestehend aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen)
- Nicht zuletzt sollten Sie regelmäßig prüfen, ob Updates für das Spielzeug verfügbar sind und diese installieren.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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