Fitness-Tracker, Smart Watches, Smart Toys - LfDI MV warnt vor Datenschutzrisiken und IT-Sicherheitslücken im Kinderzimmer

Fitness-Tracker, Smart Watches, Fernseher, Kameras, Smart Toys und digitale Sprachassistenten: die uns umgebenen Geräte und Anwendungen bieten viele Vorteile, bergen jedoch auch bedeutende Risiken für die IT- Sicherheit und den Datenschutz.

Das Internet der Dinge (IoT), auch als smarte Geräte bekannt, bezeichnet eine vernetzte Welt intelligenter Geräte, die wie Computer funktionieren und miteinander kommunizieren. IoT-Systeme automatisieren alltägliche Prozesse, wie das Messen und Einstellen der Raumtemperatur oder Helligkeit, und senden dabei häufig Daten ins Internet. Beispiele für IoT-Systeme sind Fitness-Tracker, Smart Watches, Fernseher, Kameras, Smart Toys und digitale Sprachassistenten. Alle diese Geräte und Anwendungen, die zunehmend in unserem Alltag präsent sind, bieten viele Vorteile, bergen jedoch auch bedeutende Risiken für die IT-Sicherheit und den Datenschutz. So können sich Cyberkriminelle über ungesicherte Systeme einen Zugang zum Heimnetzwerk verschaffen, sensible Informationen wie Gesundheitsdaten abfangen oder die Kontrolle über die Geräte und deren Sensoren erlangen. Aktuelle Untersuchungen offenbaren, dass jeden Tag durchschnittlich zehn Angriffe auf jedes IoT Gerät erfolgen, welches mit dem Internet verbunden ist.

Eine Befragung im Rahmen des „Cybersicherheitmonitors (CyMon) 2024“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Thema Smarthome zeigt, dass die Sorglosigkeit gegenüber Cyberkriminalität bei der Nutzung von Smarthome -Geräten weit verbreitet ist. Aus Unkenntnis über die Gefährdungen, werden die Smarthome- Geräte oft unzureichend gesichert, was ein erhöhtes Risiko für Datenspionage und -missbrauch darstellt.

Auch so genannte Smart Toys, also vernetzte Spielzeuge wie der lernfähige Teddybär oder ein mit dem Smartphone steuerbares Auto, werden immer beliebter. Diese Spielzeuge können mit den Kindern interagieren und Lernprozesse fördern, indem sie Fragen beantworten oder sogar Lernschwierigkeiten erkennen. Gleichzeitig besteht die Gefahr, dass sie persönliche Daten sammeln und diese missbraucht werden. Zudem können Cyberkriminelle schlimmstenfalls über die Geräte auf die Kinder einwirken und sie bspw. dazu verleiten die Haustür zu öffnen. Bereits werksseitig getroffene Einstellungen, wie das Standardpasswort oder die gesetzten Berechtigungen, reichen in der Regel nicht aus, um die Sicherheit zu gewährleisten. Eltern sollten daher die Rechte und Zugriffsberechtigungen der Spielzeuge und der zugehörigen Apps prüfen, sichere Verbindungen und Passwörter nutzen. Bei Netzwerkverbindungen und Schnittstellen, wie Bluetooth oder Sensoren wie GPS, Kamera oder Mikrofone sollten nur bei Bedarf aktiviert sein. Weiterhin sind regelmäßige Updates zu installieren und auf Verschlüsselung sowie den Zugriffsschutz zu achten. Bei der Kaufentscheidung sollte ein entsprechender Support seitens des Herstellers in Bezug auf Sicherheitsfeatures und Updates sowie vielleicht auch der Sitz des Herstellers eine wichtige Rolle spielen.

Eltern tragen die Verantwortung, ihre Kinder vor möglichen Datenmissbräuchen und Sicherheitsrisiken zu schützen.

Quelle: PM des LfDI MV vom 26. Sept 2024