PRAXIS INFO

Vernetztes Spielzeug

Tipps für mehr Sicherheit im digitalen Kinderzimmer

April 2020

JUGEND SCHUTZ.NET

Auch ins Kinderzimmer hat die Digitalisierung längst Einzug gehalten – in Form verschiedenster Spielzeuge und Kuscheltiere, die mit dem Internet verbunden sind. Die Faszination, die diese Smart Toys auf Kinder ausüben, ist verständlich. Jedoch sind nicht alle vernetzen Spielkameraden so unscheinbar, wie sie aussehen: Immer wieder gerät vermeintlich harmloses Kinderspielzeug in die öffentliche Kritik, wie beispielsweise die kulleräugige Puppe Cayla, die von der Bundesnetzagentur schließlich als unzulässiges Spionagegerät verboten wurde. Es ist wichtig, mögliche Risiken zu kennen und Spielzeug sowie damit verbundene mobile Geräte möglichst sicher einzustellen.

Was sind Smart Toys?

Bei Smart Toys handelt es sich häufig um Spielzeug mit Sensoren oder einer Künstlichen Intelligenz (KI). Mithilfe von Kamera oder Bewegungssensoren können sie ihre Umgebung wahrnehmen und reagieren. Manche der Spielzeuge besitzen eine Funkschnittstelle. Dadurch lassen sich Daten übertragen, beispielsweise mittels Bluetooth oder über WLAN. Viele der Spielzeuge sind mit einer zugehörigen App gekoppelt und werden darüber gesteuert.

Smart Toys können Kinder auch beim Lernen unterstützen. Beispielsweise, indem sie das Weltall in einer virtuellen Realität erfahren und so Planeten kennenlernen. Oder, indem Kinder spielerisch physikalische Experimente durchführen, während eine App ihnen die Hintergründe erklärt. Einige Spielzeuge sind pädagogisch eingebettet und so auch für den Einsatz im Unterricht geeignet.

Beispiele für vernetztes Spielzeug

Hier finden sich einige Beispiele dafür, was sich alles unter dem Begriff Smart Toys zusammenfassen lässt:

- Bücher mit begleitender App
- Spielzeuge, die über eine App gesteuert werden (z.B. Spielzeugauto, Raumschiff)
- Teddybären oder Puppen mit (personalisierter) Sprachausgabe, teilweise mit Aufnahmefunktion
- Programmierbare Roboter
- Erweiterung klassischer Brettspiele durch Apps
- Spielzeug mit Sensoren, das z.B. auf Licht, Wärme oder Lautstärke reagieren und interagieren kann

Mögliche Risiken von Smart Toys

Ungeeignete Werbung und Kostenfallen

Ist das Spielzeug über eine App mit dem Internet verbunden, können Kinder in Kostenfallen tappen oder mit ungeeigneter Werbung konfrontiert werden. Direkte Kaufaufforderungen, Sonderangebote und Zeitlimits können Druck auf Kinder ausüben und sie zum Geldausgeben verleiten. Hinzu kommt: Der tatsächliche Gegenwert hinter In-App-Käufen lässt sich durch die verwirrende Preisgestaltung häufig nicht erfassen.

Mangelnde Datensicherheit

Kinder brauchen aufgrund ihrer Unerfahrenheit besonderen Schutz hinsichtlich ihrer personenbezogenen Daten, da sie sich der Risiken und Folgen bei Veröffentlichung und Verarbeitung weniger bewusst sind. Für die Nutzung der Spielzeuge allerdings werden teilweise persönliche Angaben verlangt. So sind z.B. Fotos, Adressen oder Gesprächsaufzeichnungen erforderlich.

Auch unbemerkt können persönliche Daten direkt oder über die Nutzung einer App gesammelt und an den Hersteller oder Analysedienste übertragen werden. Besonders jüngeren Kindern fehlt häufig das Bewusstsein dafür, dass ihr Spielzeug so etwas kann, weil es ihnen noch an technischem Verständnis mangelt. Stattdessen betrachten sie das vernetzte Kuscheltier als Freund und vertrauen ihm Privates an. Mittels sensibler Kinderdaten könnte ein Persönlichkeitsprofil des Kindes erstellt werden, das dann an Dritte weitergegeben und z.B. für Werbungzwecke genutzt werden kann.

Doch selbst, wenn das nicht aktiv passiert: Bei mangelnden Sicherheitsvorkehrungen des Anbieters können Daten trotzdem schnell in falsche Hände geraten.

Informationen und Hilfe

- jugendschutz.net testet und bewertet Spielzeug auf Risiken für Kinder unter www.klick-tipps.net/eltern/spielzeug.
- Infos und Tipps für Eltern und pädagogische Fachkräfte bietet die Broschüre des Bundesfamilienministeriums „Smart Home. Clever vernetzt".
- Bei Verdacht auf Verstöße im Bereich des Jugendschutzes können Sie über die Hotline unter www.jugendschutz.net/hotline/ melden.
- Bei Verdacht auf Verstöße im Bereich des Datenschutzes wenden Sie sich an die zuständige Datenschutzbehörde (www.bfdi.bund.de).
- Bei Verdacht auf Verstöße im Bereich des Verbraucherschutzes wenden Sie sich an die Verbraucherzentrale, z.B. unter www.vzbv.de.

In der Vergangenheit gab es immer wieder Meldungen dieser Art: So konnten Angreifer bei Vtech durch Sicherheitsprobleme beispielsweise Porträtfotos von Kindern und Eltern sowie Chatprotokolle abgreifen.[1] Vom Kuscheltier-Hersteller CloudPet gelangten Kriminelle an sensible Sprachnachrichten zwischen Eltern und Kindern und verlangten für deren Herausgabe Lösegeld.[2]

Riskanter Kontakt mit Fremden

Über ungesicherte (Bluetooth-)Verbindungen können Fremde z.B. bei sprechenden Kuscheltieren schlimmstenfalls direkten Kontakt mit dem Kind aufnehmen, sich dessen Vertrauen erschleichen, die Wohnung ausspionieren oder gar eine Bedrohung für das Kind selbst darstellen. Als Folge sind Übergriffe im realen Leben potentiell möglich. Aus dem gleichen Grund können auch eine unverschlüsselte Übertragung von Standortdaten oder integrierte Kommunikationsmöglichkeiten mit Fremden problematisch sein.

Konfrontation mit ungeeigneten Inhalten

Bei Systemen, die auf automatisierte Spracherkennung und Informationen aus dem Internet zurückgreifen, ist nicht auszuschließen, dass Kinder mit ungeeigneten Inhalten konfrontiert werden. Ein jüngstes Beispiel ist der Microsoft-Chatbot „Tay", der Kommunikation mit künstlicher Intelligenz ermöglichen sollte. Twitter-User konnten jedoch das Programm binnen kürzester Zeit zum Rassisten „umprogrammieren". Microsoft zog das Programm infolge dessen zurück[3]. Auch durch Interaktionsmöglichkeiten innerhalb einer App, wie z.B. einen Chat mit anderen Nutzern oder die Möglichkeit, zu kommentieren und Links zu posten, können Kinder auf ungeeignete Inhalte stoßen.

[1] golem.de/news/kinderspielzeug-vtech-zahlt-650-000-dollar-strafe-fuer-datenschutzverstoesse-1801-132086.html
[2] heise.de/security/meldung/Cloudpets-2-2-Millionen-Sprachdateien-von-Kinderspielzeug-offen-im-Netz-3637923.html
[3] https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch

Tipps für Eltern und pädagogische Fachkräfte

Vor dem Kauf

- ☐ Ist das Spielzeug benutzerfreundlich und für Kinder geeignet? Erste Orientierung bieten Berichterstattung, Nutzerbewertungen oder Preise (z.B. TOMMI Kindersoftwarepreis).
- ☐ Lesen Sie die Informationen auf der Verpackung oder der Website des Herstellers. Werden Sie als Erwachsener eingebunden? Was verspricht der Anbieter zur Sicherheit?
- ☐ Gibt es eine zugehörige App, lässt sich diese auch im Vorfeld ohne das Spielzeug installieren und testen. Achten Sie auch auf die verlangten Berechtigungen und informieren Sie sich, ob sie In-App-Käufe oder Werbung enthält.
- ☐ Lesen Sie die Datenschutzerklärung: Wie geht der Hersteller mit den Daten um? Wo stehen die Server – in Deutschland, in Europa oder im außereuropäischen Ausland? Haben Dritte Zugriff auf die Daten oder werden diese weitergegeben?
- ☐ Welche möglicherweise kritischen Sensoren (z.B. Kamera, Mikrofon) benutzt das Spielzeug? Wofür werden diese benötigt? Wird der Standort abgefragt?

Nach dem Kauf

- ☐ Probieren Sie das Spielzeug selbst aus und begleiten Sie Kinder bei der Nutzung.
- ☐ Sprechen Sie über mögliche Risiken und vereinbaren Sie gemeinsam Regeln, wie das Spielzeug genutzt werden darf. Auch für Eltern gilt: Vorbild sein und keine Daten des Kindes leichtfertig preisgeben. Pädagogische Fachkräfte sollten zusätzlich die Eltern einbeziehen.
- ☐ Spielzeuge und mobile Geräte möglichst sicher einstellen: Eine Anleitung zur Sicherung mobiler Geräte finden Sie unter www.klick-tipps.net/sicherheit. Kopplungskennwörter für Spielzeug und App sollten Sie wenn möglich ändern.
- ☐ Welche Berechtigungen verlangt die App? Braucht sie diese wirklich? Prüfen Sie, ob sich diese in den Einstellungen des mobilen Geräts ohne Einschränkungen entziehen lassen.
- ☐ Benötigte Funktionen wie z.B. Bluetooth, aber auch das Spielzeug selbst, sollten Sie nach Gebrauch wieder ausschalten. Falls möglich, verwenden Sie den Offline-Modus.
- ☐ Nutzen Sie Spielzeuge nicht als Überwachungstool für Kinder.

Weiterführende Informationen

www.jugendschutz.net

Meldemöglichkeiten

www.jugendschutz.net/hotline

Kindern und Jugendlichen ein gutes Aufwachsen mit Medien ermöglichen

jugendschutz.net ist das gemeinsame Kompetenzzentrum von Bund und Ländern für den Schutz von Kindern und Jugendlichen im Internet. Die Jugendministerien haben die Stelle 1997 gegründet und finanzieren sie seit 2003 gemeinsam mit den Landesmedienanstalten. Sie ist an die Kommission für Jugendmedienschutz (KJM) angebunden und unterstützt sie bei ihren Aufgaben. Die Arbeit von jugendschutz.net wird gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend im Rahmen der Initiative „Gutes Aufwachsen mit Medien“ des Kinder- und Jugendplans des Bundes (KJP).

Bundesministerium für Familie, Senioren, Frauen und Jugend

GUTES AUFWACHSEN MIT MEDIEN

kjm Kommission für Jugendmedienschutz

die medienanstalten

Kontakt
jugendschutz.net
Wallstraße 11, 55122 Mainz

Inhaltlich verantwortlich
Stefan Glaser
Wallstraße 11, 55122 Mainz

JUGEND SCHUTZ.NET