Ministerium für Ernährung, Ländlichen Raum und
Verbraucherschutz Baden-Württemberg

ALGORITHMEN

#seiunberechenbar ...und schütze Deine Kinder

PantherMedia / doble.dphoto

Mit Freundinnen und Freunden über Messenger schreiben, Computerspiele spielen, Videos auf YouTube oder TikTok anschauen, Fotos machen und online hochladen oder mit vernetztem Spielzeug spielen – Kinder und Jugendliche, aber auch die Eltern, sind immer mehr digital unterwegs. Längst zählen sie zu attraktiven Datenquellen für Unternehmen, die mit Algorithmen verarbeitet werden. Doch gerade die Privatsphäre von Kindern und Jugendlichen ist besonders schützenswert. Wir zeigen an ausgewählten Beispielen, was Eltern tun können, damit ihre Kinder im Netz unberechenbar bleiben.

Kinderfotos in den Sozialen Medien

Das Familienglück mit anderen in sogenannten Sozialen Medien (z. B. Facebook, Instagram) oder Messengern (z. B. WhatsApp, Telegram, Signal) zu teilen, hat für viele Erwachsene wie auch für Kinder einen großen Reiz. Schnell sind die schönsten Fotos vom letzten Kindergeburtstag oder Urlaub innerhalb einer Chat-Gruppe oder im persönlichen Social-Media-Profil hochgeladen, sodass sie andere

sehen und kommentieren können. Dabei werden häufig Fotos mit Kindern ausgewählt. Hierbei ist besondere Vorsicht geboten, denn wie die Erwachsenen, haben Kinder ein Recht am eigenen Bild. Kinder können jedoch die Folgen schlecht abschätzen.

Was kann mit Fotos passieren, die unachtsam im Netz geteilt wurden? Möglich ist, dass aus den privaten Fotos Daten über persönliche Vorlieben und Hobbies gesammelt werden, die beispielsweise für Werbetreibende interessant sein können. Oder die Fotos landen in einer Datenbank zur Gesichtserkennung: Wie Fingerabdrücke können auch Gesichter herangezogen werden, um Personen zu identifizieren, algorithmenbasierte Gesichtserkennungssoftware zu verbessern und so die Nutzer in allen Phasen des Lebens gläserner zu machen – mit allen Folgen.

Was also tun, um sich und Kinder vor unerwünschter Nutzung von persönlichen Fotos zu schützen?

- Kinder sollten auf Fotos, die veröffentlicht werden, grundsätzlich nicht direkt erkennbar sein.
- Werden Fotos über das Smartphone aufgenommen und hochgeladen, sollte die Ortsbestimmung via GPS deaktiviert sein. Über das sogenannte Geotagging kann ansonsten sichtbar werden, wo genau das Foto aufgenommen wurde.
- Verzichten Sie, wenn möglich, auf das Speichern von Fotos in einem Online-Speicher („Cloud"). Die eigene (externe) Festplatte ist ein Speicherort, der mehr Sicherheit bietet.
- Achten Sie darauf, dass Ihr Profil in Sozialen Medien nur für einen engen Kreis von Freunden und Bekannten sichtbar ist.

Smartes Spielzeug

Sprechende Dinosaurier, Spielzeug-Roboter, interaktive Bilderbücher oder Kinder-Smartwatches – die Welt der vernetzten, intelligenten Spielzeuge ist groß und faszinierend für Kinder. Erwachsene sollten die verschiedenen Arten von intelligenten Spielgeräten und deren Gefahren kennen, denn schnell können unbedarft eingekaufte oder verschenkte, vernetzte Spielzeuge zu einem unsichtbaren Spion im Kinderzimmer werden. Die Verbraucherzentrale unterscheidet in diesem Zusammenhang vier Problemartikel: Spielfiguren mit Spracherkennung, die in begrenztem Maße mit dem Kind kommunizieren können; ferngesteuertes Spielzeug (z. B. Autos, Helikopter, Drohnen), das sich mit einer App steuern lässt; Roboter-Spielzeug und elektronisches Lernspielzeug (z. B. Kindertablets).

Mit Mikrofon und Kamera ausgestattete, funkfähige Spielgeräte können ihre Umgebung abhören bzw. ausspionieren oder Standortdaten sammeln. Durch ungesicherte Bluetooth-Verbindungen können dann theoretisch auch fremde Personen mit dem Kind Kontakt aufnehmen. Als Sendeanlage eingestufte Spielzeuge wurden in der Vergangenheit zwar von der Bundesnetzagentur verboten, trotzdem gibt es genügend Spielzeuge auf dem Markt, die Daten weitergeben. Algorithmen kommen im Zusammenhang mit dem Sammeln von Daten für Marketingzwecke ins Spiel. Zeichnen Spielgeräte Daten auf, werden diese häufig auf Servern außerhalb der EU gespeichert. Die Hersteller können dann Dritten Zugriff auf die gesammelten Daten gewähren, die sich wiederum zur Profilbildung der Kinder und für personalisierte Werbung nutzen lassen. Schlimmstenfalls geraten die Daten in die Hände von Kriminellen. Um die Privatsphäre der Kinder vollständig zu schützen und Datenmissbrauch zu verhindern, raten Datenschützer und Medienpädagogen klar davon ab, vernetztes Spielzeug zu verwenden. Sobald sich sogenannte Smart Toys mit dem Internet verbinden, ist davon auszugehen,

dass auch Daten übertragen werden. Wer seinen Kindern das Spielen mit vernetztem Spielzeug trotzdem nicht verwehren will, kann folgende Tipps beachten:

- Am besten ist, das Spielzeug offline zu nutzen. Wenn online, dann über eine sichere, passwortgeschützte Internetverbindung, um unbefugten Zugriff Dritter zu verhindern.
- Kinder sollten das Spielgerät ausschalten, wenn sie nicht mehr damit spielen.
- Geben Sie so wenig persönliche Daten wie möglich preis (z. B. bei Anmeldevorgängen). Für Ihr Kind können Sie fiktive Angaben machen.
- Lesen Sie vorab die Datenschutzerklärung.
- Informieren Sie sich über die Zugriffsrechte des Spielzeugs oder der dazugehörigen App, wenn sich das Spielzeug mit anderen Geräten verbinden lässt (z. B. Smartphone, Tablet, PC). Je weniger Zugriffsrechte gewährt werden, umso besser für den Schutz der Daten.
- Sind Updates für das Spielzeug vorhanden, sollten diese installiert werden, um Datenschutzlücken vorzubeugen. Vor dem Kauf sollte abschätzbar sein, wie lang voraussichtlich Updates angeboten werden.
- Funkfähige Spielzeuge, die Ton und/oder Bild unbemerkt aufnehmen und diese Daten weitersenden können, sind in Deutschland verboten. Achten Sie bei Einkäufen im Internet darauf, keine solchen Spielzeuge zu erwerben und vergewissern Sie sich der Seriosität des Anbieters bzw. Herstellers.

In-Game-Käufe / In-App-Käufe

In-Game-Käufe bezeichnen den Erwerb von virtuellen Leistungen oder Gütern verschiedenster Art innerhalb von Computerspielen – bei Spiele-Apps, nennt man sie In-App-Käufe. Das Angebot solcher Kaufmöglichkeiten nimmt immer mehr zu, da sie mittlerweile ein lukratives Geschäftsmodell für die Spieleindustrie sind.

Dabei kann das eigentliche Hauptspiel zunächst kostenfrei sein, was häufig bei Browser-Games und Spiele-Apps der Fall ist. An einem gewissen Punkt während des Spiels kommen aber gezielt beispielsweise Erweiterungsmöglichkeiten, virtuelle Gegenstände und Figuren oder Spielwährungen mit kreativen Namen ins Spiel, die extra kosten (z. B. zusätzliche Charaktere, Schwierigkeitsstufen, Spielmissionen oder Spezialfähigkeiten, verkürzte Wartezeiten). Besonders die sogenannten Loot-Boxen (Beutekisten) – deren Inhalt vorher unbekannt ist – sind für Kinder verlockend und haben einen kritisch zu sehenden Glücksspiel-Charakter. In der Regel steuern Algorithmen u. a. die Lootbox-Mechanismen so, dass die Spieler möglichst lange an das Spiel gebunden werden.

Um die Angebote zu bezahlen, gibt es verschiedene Möglichkeiten. Ein großes Problem ist, dass häufig zu Beginn des Spiels bzw. nach dem Herunterladen der App einmalig die Kreditkartendaten eingegeben werden müssen und somit Tür und Tor für regelmäßige Bezahlvorgänge geöffnet werden. Dann ist es nicht nur für Kinder schwer, die Übersicht über getätigte Käufe und Rechnungsbeträge zu behalten. Bei Browser-Games kommen häufig Premium-Dienste zum Einsatz, über die mittels einer SMS oder einem kostenpflichtigen Anruf die Zahlung getätigt wird, die dann von der Prepaid-Karte oder mit der nächsten Telefonrechnung abgebucht wird. Eine andere Möglichkeit zum Bezahlen bieten so genannte Scratch-Karten (Rubbelkarten), die am Kiosk, im Supermarkt oder in Tankstellen verkauft werden. Der frei

gerubbelte Code kann dann im Spiel für In-Game-Käufe eingegeben werden. So können auch Minderjährige auf eigene Faust mit ihrem Taschengeld bezahlen.

Die Auseinandersetzung mit den Wirkmechanismen und Bezahlmethoden von In-Game-Käufen lohnt sich, um bösen Überraschungen vorzubeugen. Hier ein paar Tipps:

- Es ist sinnvoll, das Prinzip der In-Game-Käufe und die Gefahren ausführlich mit Kindern und Jugendlichen zu besprechen.
- Bei Mobilfunkanbietern kann über eine Drittanbietersperre verhindert werden, dass über die Telefonrechnung Geld abgebucht wird.
- Bei Handys und Tablets lassen sich In-App-Käufe über die Einstellungen deaktivieren.
- Für Geräte, auf die Minderjährige Zugriff haben, kann ein Passwortschutz für jeden Kauf eingerichtet werden. Das ist beispielsweise bei Spielekonsolen mit Hilfe eines Gastzugangs bzw. -profils möglich
- Haben Kinder die Erlaubnis, In-Game-Käufe zu tätigen, sollten Sie vorher zusammen mit den Kindern Höchstgrenzen festlegen.

Link dieser Seite:

https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/kinder