Elektronische Geräte – In den Schweizer Wohnzimmern wird immer mehr gefilmt. Nicht nur Smartphones und Tablets besitzen eingebaute Kameras, sondern auch zahlreiche Fernseher. Wer seinem TV-Gerät keine Schranken setzt, könnte schon heute unter ständiger Überwachung stehen.

Der Spion in meiner Stube

Schöne neue Welt: Smart-TVs versprechen viele zusätzliche Dienste und bequeme Bedienung. Nur den wenigsten Käufern ist klar, dass sie dafür mit ihren Daten und ihrer Privatsphäre bezahlen. BILDER MICHAEL STAUB

George Orwell schrieb 1948 seinen Roman «1984», die beklemmende Vision eines Staates, der seine Bürger rund um die Uhr bespitzelt und unterdrückt. Ein zentrales Element der Überwachung sind die sogenannten Televisoren. Diese Fernseher bringen nicht nur Propagandasendungen in die gute Stube. Sie sind auch mit Kameras und Mikrofonen ausgestattet, die ständig auf Empfang sind. «Zum Glück ist es nur ein Buch!», lautete der Konsens bis vor etwa vier oder fünf Jahren. Damals wurden die ersten «Smart-TVs» lanciert. Die neuartigen Fernseher besassen Funktionen, die lange für Computer gedacht schienen: Netzwerkfähigkeit, Internetanschluss und Speicherkarten. Schon bald folgten «Komfortfunktionen» wie Sprach- oder Gestensteuerung und Skype.

MICHAEL STAUB
Journalist BR, Kriens

Grosse Brüder auf Empfang

Ausserhalb von Fachkreisen wurde lange Zeit kaum diskutiert, wie diese Funktionen überhaupt möglich sind. Eigentlich ist es klar: Eine Sprachsteuerung funktioniert nur, wenn das Gerät über ein Mikrofon permanent mithört. Und um Gesten zu erkennen und beispielsweise das Programm zu wechseln, muss eine Kamera auf Empfang sein. Wer sich also einen «Smart-TV» ins Wohnzimmer stellt, installiert im schlimmsten Fall freiwillig einen Televisor. Im Gegensatz zu Computern, Smartphones oder Tablets sind bei den Fernsehern die Sicherheitslöcher sehr zahlreich, gute Gegenmassnahmen dagegen kaum vorhanden. Es gibt zum Beispiel keine Virenscanner für Fernseher. Und beim Einrichten der Firewall, also der digitalen Brandwand zwischen dem Wohnzimmer und dem Internet, geraten selbst TV-Techniker an ihre Grenzen.

Fremde Augen und Ohren im eigenen Wohnzimmer sind aus verschiedenen Gründen höchst problematisch. Erstens geht es um den Schutz der Privatsphäre. Auch wer glaubt, er oder sie habe «nichts zu verbergen», erlebt durch solche Geräte einen massiven Eingriff und macht sich und seine Nächsten angreifbar. Zweitens können gehackte Geräte in sogenannte «Botnetze» eingespannt werden. Gekaperte Computer oder Fernseher werden sozusagen in Zombies verwandelt, die Spam-Mails versenden oder Websites durch orchestrierte Massenaufrufe lahmlegen. Und drittens gibt es bei Smart-TVs wie bei jedem Computer oder Smartphone die Zusammenführung von Daten (Datenaggregierung) zu beachten. Wie die Stiftung Warentest schon 2014 herausfand, lieferten die Geräte aller Marken umfangreiche Datenpakete an Hersteller, TV-Sender und/oder Google. Je mehr Daten aus unterschiedlichen Quellen (Computer, Smartphone, TV) aggregiert werden, desto lebensnaher wird der «digitale Doppelgänger» eines Menschen. Solche Daten einzusehen oder gar löschen zu lassen, ist heute faktisch unmöglich.

Die Einschläge kommen näher

Die beschriebenen Gefährdungen sind durchaus real. Das zeigt eine kurze Liste von Vorfällen aus den letzten zwei Jahren:

- **Gehackte Kamera.** Bereits 2015 demonstrierte der IT-Experte Benjamin Michéle in einer Sendung des ARD einen «Soforthack». Dazu drang er in das WLAN-Netzwerk einer Wohnung eines Paares ein und spielte eine Schadsoftware auf deren Fernseher auf. Damit erhielt Michéle in kürzester Zeit Zugriff auf die Kamera des Smart-TV. Ein Traum für Voyeure, Einbrecher und Erpresser.

- **Unfreiwilliger Sexfilm.** Ein britisches Paar wurde im Frühling 2016 beim Schäferstündchen auf dem Sofa unbemerkt gefilmt. Der Film landete im Internet auf einer einschlägigen Seite. Erst durch die Hinweise von Bekannten wurde dem Paar bewusst, dass offenbar sein Smart-TV unbemerkt gehackt und die Kamera gekapert worden war.

- **Samsung warnt vor eigenen Geräten.** Bereits 2014 bemängelte die Stiftung Warentest, dass Samsung mit Daten seiner Smart-TV-Kunden extrem lasch umgehe. 2016 wurde der Hersteller vor dem Landgericht Frankfurt verklagt, weil seine Sprachsteuerung unverschlüsselte Audiodaten über das Internet schickt. Inzwischen warnt Samsung seine eigenen Kunden: Auch «persönliche Informationen» würden aufgezeichnet und an Dritte weitergeleitet.

- **Erpressung via TV.** Bei PCs und Laptops ist das Problem der «Ransomware» schon lange bekannt: Sämtliche Daten werden verschlüsselt und nur gegen Bezahlung wieder freigegeben. Anfang 2017 zeigte der Softwareentwickler Darren Cauthon einen gehackten Smart-TV der Marke LG. Das Gerät war nicht mehr benutzbar, auf dem Bildschirm erschien eine fiktive Lösegeldforderung.

Der «Netflix»-Knopf deutet auf eine grosse Filmauswahl hin – und auf potenzielle Probleme mit dem Datenschutz und der Sicherheit.

Sicherheit aushandeln

Leider sind die unsicheren Smart-TVs keine Ausreisser im Gerätepark. Wie Roboterstaubsauger, fernbedienbare LED-Leuchten oder billige Türsprechanlagen gehören die angeblich schlauen Fernseher zum «Internet der Dinge» (Internet of Things, IoT). Man könne weder das IoT noch die wachsende Begeisterung aufhalten, fast alles Mögliche und Unmögliche ans Netz zu hängen, meint Hannes Lubich. Er ist Dozent für ICT System Management an der Fachhochschule Nordwestschweiz (FHNW). «Es gab schon früher disruptive Technologien, also Entwicklungen, die die Welt gleichsam auf den Kopf gestellt haben», sagt Lubich. Als Beispiel nennt er die Eisenbahn, die in ihren Anfängen nur etwa mit 20 Stundenkilometern fuhr. Ernsthafte Kritiker forderten, die Schienenwege einzuhausen, damit Betrachtern vom Anblick der «rasenden» Züge nicht schlecht wurde. Heute sind auf den SBB-Strecken Geschwindigkeiten von 160 Stundenkilometern durchaus normal.

Einen solchen Konsens auszuhandeln, dauerte früher drei bis vier Generationen. «So viel Zeit haben wir nicht mehr, und ein Moratorium für neue Technologien ist hier undenkbar», sagt Lubich. Jedoch habe man schon früher «erst mal das Neue hingestellt und gehofft, dass sich die Gesellschaft irgendwie daran angleicht.» Die Entwicklung zumindest partieller Schutzmechanismen für IoT-Geräte sei nur über «einen langen und zähen Prozess» zu erreichen. Letztlich sei Sicherheit eine Frage der Aushandlung, meint der IT-Experte: «Es wird weiterhin spektakuläre, ja haarsträubende Fälle geben. Daran merkt man, was die Gesellschaft hinzunehmen bereit ist und was nicht.»

Genau hinschauen

Wer diese Aushandlung des Erlaubten bei den TV-Geräten nicht einfach passiv hinnehmen will, hat schon heute einige Möglichkeiten:

- **Genau informieren.** Welche Funktionen besitzt das TV-Gerät, welche sind wirklich nötig? Wer «nur» Netflix nutzen will, braucht keine Gestensteuerung. Eine kurze Internetsuche nach «smart-tv datenschutz» kann beim Kaufentscheid hilfreich sein.

- **Spionen die Augen verbinden.** Keine Kamera muss ständig sendebereit sind. Ein Stück Klebeband, ein schöner Sticker oder ein Schieber sorgen für Privatsphäre (siehe Infobox).

- **Sorgfältig einrichten.** Die Datensammlerei und -weitergabe lässt sich zumindest teilweise verbieten. Die Einstellung ist meist für jeden (!) einzelnen Sender notwendig. Geduld und Hartnäckigkeit zahlen sich aus.

- **Alternativen prüfen.** Muss der Fernseher inklusive seiner vielen Sicherheitslücken direkt am Internet hängen? Oder kann der gewünschte Komfort auch mit einer Set-Top-Box erreicht werden? Dann bleibt der TV «dumm», was durchaus Vorteile bietet.

IST MEIN TV «SMART»?

Smart-TVs erkennt man an verschiedenen Merkmalen: Sie ermöglichen den Zugriff auf Online-Videotheken (z. B. SRF oder ZDF) oder Streamingdienste (Netflix). Die Geräte besitzen Anschlüsse für Netzwerkkabel oder eingebaute WLAN-Sender. Dadurch können sie auf Internetseiten zugreifen (beispielsweise für genaue Wetterprognosen) oder Kommunikationskanäle nutzen, die sonst mit Smartphone oder PC zugänglich sind (Skype, Twitter, E-Mail). Eingebaute Mikrofone sind unter Umständen schwer zu erkennen.

Kameras sind meist mittig am oberen Geräterand platziert. Sie können mit Aufklebern oder speziellen Schiebern abgedeckt werden, wie sie zum Beispiel die Schweizer Firma Soomz («stay out of my zoo») liefert. Das Abdecken von Kameralinsen sollte man in jedem Fall erwägen, auch bei Laptops, Tablets und Smartphones. Sogar James Comey, bis vor Kurzem Direktor des US-Geheimdienstes FBI, spricht sich mit Nachdruck für diese Massnahme aus: «Es gibt einige vernünftige Dinge, die man tun sollte, und dieses ist eines davon.» Gerade Laptop-Kameras können relativ leicht gehackt werden und ihre Benutzer unbemerkt filmen.

Abdeckungen für die Kameras von Fernsehern, Laptops oder Smartphones gibt es bei **www.soomz.io**