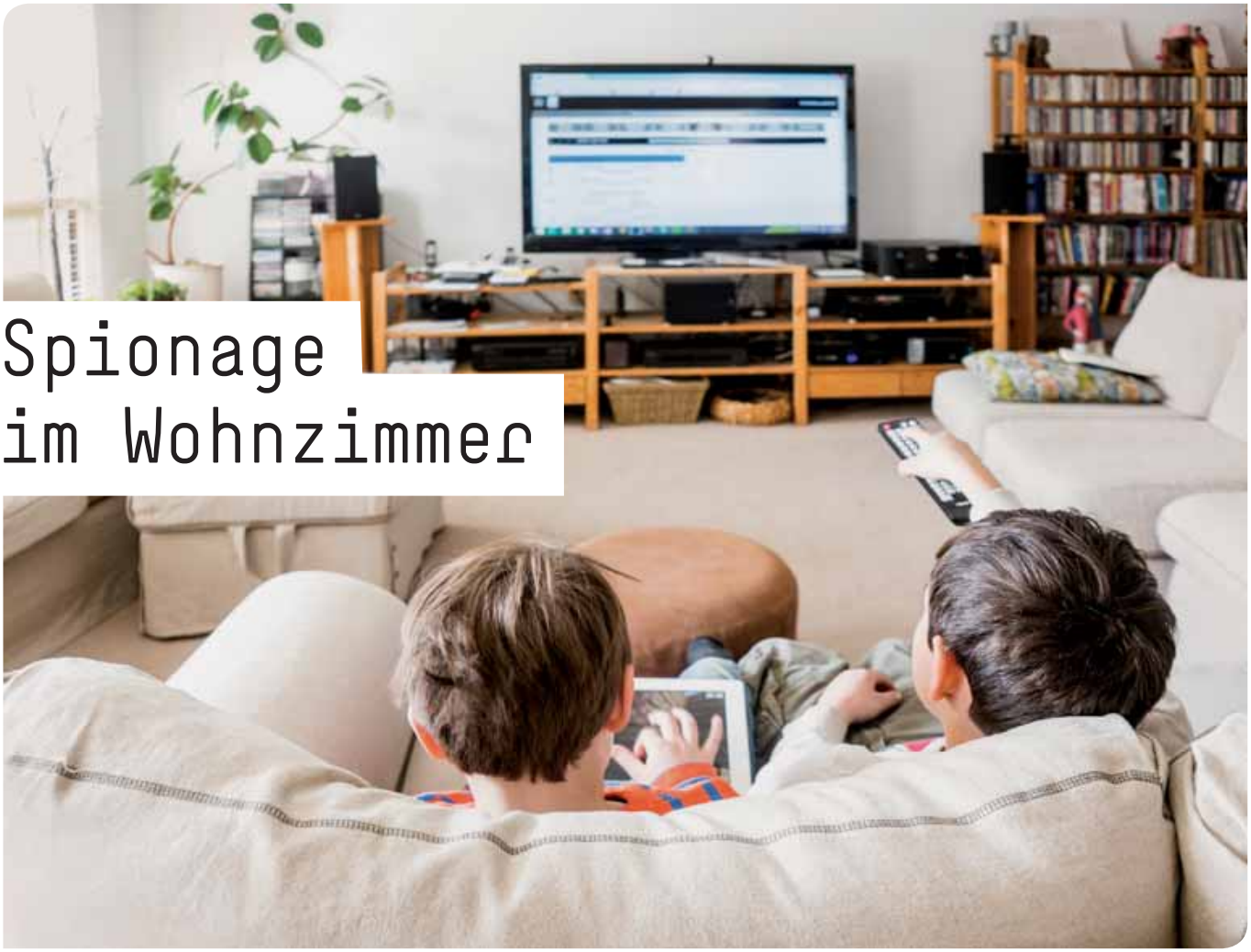

Smarte Fernseher sind mit dem Internet verbunden und verschicken Daten.
© *iStockphoto*

Spionage im Wohnzimmer

My home is my castle: Die eigenen vier Wände sind der Inbegriff von Privatheit und geschütztem Raum. Doch Smart-TVs, »intelligente« Haushaltsgeräte und Wearables sind mit dem Internet verbunden und senden unsere Daten in die Welt – oftmals ohne unser Wissen.

Text: Janine van Ackeren

Forum Privatheit

Wie kann man die Privatheit schützen? Mit dieser Frage setzen sich nationale und internationale Experten im Forum Privatheit auseinander. Koordiniert wird das vom Bundesministerium für Bildung und Forschung geförderte Projekt durch das ISI. Partner sind das Fraunhofer-Institut für Sichere Informationstechnologie SIT, verschiedene Universitäten und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

www.forum-privatheit.de

Ab in die Jogginghose, dann auf die Couch und einen gemütlichen Fernsehabend mit der Familie oder Freunden verbringen. Zuhause fühlen wir uns sicher und unbeobachtet. Was man hier macht, sagt und tut, bleibt in den eigenen vier Wänden. Ob das auch in Zukunft noch so gilt, ist nicht sicher. Denn nach Meinung verschiedener Wissenschaftler ist unsere Privatsphäre bedroht, sogar im heimischen Wohnzimmer.

Smarte Fernseher sind Computer

»In Zeiten des Smart-TVs ist ein Fernseher nicht länger nur ein TV-Gerät, sondern ein versteckter Computer, der Daten an internationale Unternehmen sendet. Schon beim gewöhnlichen Fernsehen erheben sie Nutzungs- und Verhaltensdaten und ermöglichen über Foto-, Audio- und Videoaufnahmen sogar eine persönliche Identifikation«, erklärt Dr. Michael Friedewald, Geschäftsfeldleiter am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Im White Paper »Das versteckte Internet« skizzieren die Expertinnen und Experten des Forschungsverbunds »Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt« (siehe Kasten) problematische Aspekte smarter Technologien. Das Paper soll der breiten Bevölkerung bewusst machen, wie viele Daten ohne das Wissen des Betroffenen an Dritte gesendet werden. Die Experten konzentrierten sich dabei auf die drei Anwendungsbereiche Smart TV, intelligente Autos sowie neue Endgeräte wie Smart Watches, die direkt am Körper getragen werden.

»Smart-TVs sind Fernseher, die mit Computer-Prozessoren ausgestattet wurden. Über diese bieten die Hersteller zahlreiche Services an – teilweise finanzieren sie diese über die Nutzerdaten quer – auch wenn dies meist mit den besten Absichten geschieht«, ergänzt Friedewald. »Innerhalb weniger Jahre wird nahezu jeder Haushalt ein solches vermeintliches Spionagegerät im Wohnzimmer stehen haben.« Den Nutzern allerdings ist meist nicht bewusst, dass sie mit dem Anschaltknopf des Fernsehers weitaus mehr einschalten als das reine Massenmedium. Und noch weniger können sie nachvollziehen, wie viele Daten wo, wann und zu welchem Zweck erhoben und genutzt werden – und zu wem diese persönlichen Informationen fließen. Auf den ersten Blick mag der Gedanke an Spionage via Fernseher absurd erscheinen. Taucht man jedoch etwas tiefer in die Materie ein, zeichnet sich ein anderes Bild: Möchte der Nutzer bestimmte Anwendungen im Fernseher nutzen, muss er sich dafür registrieren. Auch das Smart-TV selbst meldet sich mit einer IP-Adresse im Netz an. Dann können die Nutzer wie mit einer Art übergroßem Smartphone nach Belieben Apps herunterladen, Emails lesen, Einkäufe tätigen. Die Daten, die der Fernseher sammelt, könnten einerseits bei Sendeanstalten landen, um die Einschaltquoten genauer zu erfassen. Problematischer ist: Die Daten können auch zu Google als Anbieter der Android-Plattform, anderen Anbietern der Softwareplattform sowie zum Hersteller des Fernsehgeräts gelangen. »Die Gerätehersteller sitzen vielfach in Asien. Sie wissen teilweise nicht, welche Datenschutzkultur hierzulande besteht – da ist man ohne Absicht schnell in einer Grauzone«, bestätigt Friedewald. Sind die Daten erst einmal übertragen, lässt sich kaum noch nachvollziehen, was mit ihnen geschieht.

Welch drastische Ausmaße dies haben kann, zeigt ein Beispiel: Einige TV-Geräte und Spielekonsolen werden bereits serienmäßig mit einer Kamera und Mikrofonen ausgeliefert. Sie machen die Fernbedienung überflüssig – es reichen Gesten oder eine Spracheingabe, um beispielsweise die Kanäle zu wechseln oder die Lautstärke zu ändern. Möchte man die Audio- oder Videofunktion nutzen, müssen diese ständig eingeschaltet sein. Aber was geschieht mit den Videos und Sprachaufnahmen? Würde man es merken, wenn sie in fremde Hände gelangen?

Smart-Watches haben Zugriff auf persönliche Daten

Der smarte Fernseher ist allerdings nur eines der Beispiele für die Entwicklung – ähnliche Probleme tauchen etwa beim »intelligenten« Kühlschrank und der schlauen Lichtsteuerung auf. Kurzum: bei Endgeräten, die heute in vielen Haushalten Einzug finden. Auch Smart-Watches und intelligente Fitness-Armbänder sind in punkto Datenschutz durchaus mit Vorsicht zu genießen: So könnten Krankenkassen über die individuellen Gewohnheiten des Nutzers zwar mit reduzierten Beiträgen locken, ebenso gut aber Fehlverhalten über die gesammelten Daten nachweisen und eine Kostenübernahme verweigern. Auch vernetzte Autos können Informationen über Fahrstil, Aufenthaltsort oder Fahrstrecke sammeln. Daraus lassen sich persönliche Merkmale und Gewohnheiten der Nutzer ableiten. »Die Zahl der Akteure, die potentiell auf personenbezogene Daten zugreifen können, erweitert sich jedenfalls immens«, gibt Friedewald zu bedenken.

Privatheit schützen

Das Problem an der Sache: Bislang mangelt es vielen Herstellern von Smart TVs, Wearables und vernetzten Autos an einer Datenschutzkultur. »Möchte man die Privatheit schützen, sind verschiedene Akteure gefragt: Industrie, Politik und natürlich auch die Nutzer«, sagt Friedewald. »Ein erster Ansatz besteht in der Transparenz: Der Nutzer muss wissen, welche Datentransfers im Hintergrund laufen und dies beeinflussen können.« Ähnlich wie bei einem Smartphone, bei dem etwa der Hinweis aufpoppt: »Die App XY möchte auf ihre Kontaktdaten zugreifen«. Der Anwender kann dem zustimmen oder aber den Zugriff verweigern. Bei neu gekauften Geräten sollten zunächst einmal alle Funktionen ausgeschaltet sein, die Informationen übermitteln. Möchte der Nutzer sie anwenden, muss er den Datentransfer bewusst freigeben. Man spricht bei solchen Voreinstellungen auch von »Privacy by Default«. Zudem sollte die Technik selbst sicherstellen, dass der Datenschutz eingehalten wird. Sprich: Die Privatheit des Nutzers sollte während der gesamten Entwicklungsphase im Fokus (Privacy by Design) stehen.

Auch die Politik ist in der Pflicht: Sie begegnet dem Problem mit der Datenschutzgrundverordnung. Diese liefert eine einheitliche gesetzliche Grundlage für den Datenschutz in Europa. Die Essenz: Egal wo ein Unternehmer sitzt, er muss den Datenschutz desjenigen Landes einhalten, in dem er seinen Dienst anbietet. Für Google beispielsweise hieße das: Das Unternehmen kann sich nicht mehr darauf berufen, in den USA zu sitzen. Bieten sie ihre Dienste in Deutschland an, gilt der deutsche Datenschutz. Bereits vor einigen Wochen hat der Europäische Gerichtshof das Safe-Harbor-Abkommen für ungültig erklärt, nach dem bislang personenbezogene Daten an Firmen in den USA übertragen werden konnten, da davon ausgegangen wurde, dass die USA gleichwertige Datenschutzstandards gewähren, wie sie auch innerhalb der EU herrschen. ■

Podcast online:
www.fraunhofer.de/audio

weiter.vorn

Das Fraunhofer-Magazin 1/16

Sicher digital wirtschaften

Kommunikation
Mobilfunk von Morgen

Nachhaltigkeit
Rohstoffquelle Elektroschrott

Life Sciences
Adern aus dem Drucker