Andreas Sachs

Smart-TVs im Fokus der Datenschutzaufsichtsbehörden

Das Internet hat viele Bereiche des Alltags bereits durchdrungen und wird von vielen Bürgern als nützlich und selbstverständlich angesehen. Es gibt allerdings noch einen Bereich, der sich lange gegen die Vernetzung „gewehrt" hat und als DAS Medium der Informationsbeschaffung angesehen wird oder zumindest wurde: der Fernseher.

Konvergenz der Medien

Durch maßgeblich zwei Faktoren hat sich dieser Sachverhalt mittlerweile grundlegend verändert. So besitzen heute die meisten Bürger einen Breitband-Internetanschluss (oder zumindest das, was mit viel Phantasie darunter verstanden werden kann). Gepaart mit einem Flatrate-Preismodell können beliebige Endgeräte dauerhaft mit dem Internet verbunden bleiben. Dies sind die Smartphones, die regelmäßig große Datenmengen mit den angebundenen Cloud-Speichern synchronisieren, die private Cloud zuhause, die einen Zugriff auf die letzten Urlaubsfotos von überall erlaubt oder die Spielekonsolen, die ohne Internetanbindung einen erheblichen Verlust des Spaßfaktors mit sich bringen. Was liegt also näher, als noch ein weiteres Endgerät mit wenigen Klicks über den WLAN-Anschluss des Haushaltes mit der großen weiten Welt zu verbinden. Der zweite Faktor sind die vielen kleinen Anwendungen, die Apps, die bereits die Smartphones so erfolgreich gemacht haben. Für jede Lebenslage, seien es Online-Banking, Shopping, Nachrichten, Soziale Netzwerke, Kochrezepte, Spiele, Liebeskummer, Bewertung von anderen Autofahrern, … gibt es mittlerweile kleine Helferlein. Manche davon sind derart erfolgreich geworden, dass diese eine millionenfache Verbreitung mit einem Stammkundenkreis gefunden haben. Was liegt also näher, als das Lieblingsspiel oder die soziale Kommunikation nicht mehr auf einem 5-Zoll-Mini-Display, sondern auf einem 40-Zoll-4K-Boliden mit Surround-Sound zu genießen.

Wer sich heute (oder in Bälde im Hinblick auf die Fußball-Europameisterschaft) ein neues Fernsehgerät kaufen möchte, wird feststellen, dass neben der Bildschirmdiagonale und der Bildqualität weitere Features zum Kauf genau eines bestimmten Geräts verführen sollen: Smart-TV, HbbTV, Spracherkennung, Skype, EPG, … Doch was versteckt sich hinter diesen Begriffen und was bedeutet dies bezüglich des Einsatzes eines technischen Gerätes, das bis jetzt für die anonyme Informationsbeschaffung (und gelegentlich für leichte Kost wie Gesangs- und Schönheitswettbewerbe oder Überlebenstrainings im Dschungel) stand.

Datenschutzaufsichtsbehörde

An dieser Stelle kommt nicht nur, aber auch der Begriff Datenschutz ins Spiel. Dieser ist heute sicherlich für jeden sehr geläufig, zumindest wenn die eigene Daten betroffen sind. Die einen verstehen darunter den Schutz des Rechts auf informationelle Selbstbestimmung, andere ein Relikt aus analogen Zeiten, weitere den ausschließlich technischen Schutz von Daten. Würde man die Frage nach dem Stellenwert für den Bürger stellen, dann könnte möglicherweise folgendes Dilemma festgestellt werden: Den Datenschutz finden viele sehr wichtig – irgendwie. Es soll keine Werbung zugestellt werden, der Staat soll keine Daten (z. B. das Einkommen, die Haushaltsgröße, …) erheben, die eigenen Daten sollen vor „Hackern" geschützt werden und wenn der eigene Name gegoogelt wird, sollen am besten keine Treffer erscheinen. Auf der anderen Seite soll es möglich sein, an allen tollen technischen Entwicklungen teilzuhaben – und das kostenlos (oder zumindest sehr günstig): Die Nachrichtenportale im Internet, die sozialen Medien, die Kommunikation mit Freunden und Familie, der Genuss von Musik und Filmen, … Klappt dies nicht so wie gewünscht, dann kann der Kontakt mit einer Behörde gesucht werden, die sich um den Datenschutz „kümmert". Nach ein wenig Recherche wird schnell klar, dass dieser offizielle Schritt zuerst ein bisschen komplizierter erscheint, da die Datenschutzaufsicht in Deutschland föderal geregelt ist. Dies bedeutet, dass jedes Bundesland eine eigene Datenschutzaufsichtsbehörde besitzt. Der Freistaat Bayern hat sich hier sogar für eine spezialisiertere Organisation entschieden und die Aufsichtsbehörde in einen öffentlichen Teil (für die Kontrolle des Staates) und einen nicht-öffentlichen Teil (für die Kontrolle der Wirtschaft) geteilt. So kompliziert wie sich das Konstrukt der Aufsichtsbehörden auf den ersten Blick anfühlt, ist es dann aber in der Praxis nicht. Sollte eine Behörde „nicht zuständig" sein, so wird beispielsweise eine Beschwerde unbürokratisch an die zuständige Aufsichtsbehörde weitergeleitet. Da den Datenschutzaufsichtsbehörden Begriffe wie E-Mail und PGP auch geläufig sind, geht dies (mitunter) auch recht zügig und sicher.

Rechtliche Regelungen für Smart-TVs

Wenn eine Datenschutzaufsichtsbehörde sich einer Aufgabenstellung (z. B. Beschwerde oder Beratungsanfrage) annimmt, dann geschieht dies nicht auf beliebiger Basis oder Sichtweise, sondern immer auf Grundlage von Gesetzen. Diese regeln (mehr oder weniger spezifisch) die Art und Weise, ob und wie die Verarbeitung personenbezogener Daten erfolgen darf. In Deutschland gilt diesbezüglich der Grundsatz „Verbot mit Er-

laubnisvorbehalt", was bedeutet, dass personenbezogene Daten entweder auf Basis eines konkreten Paragraphen eines Datenschutzgesetzes (hauptsächlich Bundesdatenschutzgesetz und Telemediengesetz) verarbeitet werden oder, indem der Bürger um Erlaubnis für diese Verarbeitung gebeten wird. Die Regelungen unterscheiden auch zwischen dem Verhältnis zweier „Verantwortlicher Stellen", z. B. Unternehmen, untereinander (wie dies beispielsweise beim Outsourcing an einen Cloud-Anbieter zum Tragen kommt) einerseits und dem Verhältnis zwischen dem Bürger (auch als Betroffener bezeichnet) und einer Verantwortlichen Stelle, z. B. einem Smart-TV-Hersteller, andererseits.

Nutzungsbedingungen

Soll nun ein (neues) Smart-TV angeschafft werden, dann stellt sich auch die Frage, inwiefern eine Verarbeitung personenbezogener Daten stattfindet und wie diese im ersten Schritt auch rechtlich geregelt wird. Mittel der Wahl ist bei Smart-TVs ein zivilrechtlicher Vertrag, auch Allgemeine Geschäftsbedingungen genannt, der auch eine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten darstellen kann. Bei diesem sollte Transparenz das oberste Gebot sein, da dies die Grundlage dafür ist, eine Entscheidung über die Nutzung eines Smart-TV zu treffen. Dass dies in der Praxis nicht zwangsläufig zutrifft, ist auch den Datenschutzaufsichtsbehörden bekannt. Auch stellte sich die grundsätzliche Frage nach den rechtlichen Anforderungen eines Smart-TV in Deutschland. Deshalb haben sich die Datenschutzaufsichtsbehörden in Deutschland, die in ihrem Bundesland einen Hersteller von Smart-TVs (oder eine Niederlassung) haben, entschieden, ein Prüfprojekt zu starten, das zwei aufeinander aufbauende Ziele hatte: Zuerst sollten aktuelle Smart-TVs technisch besser verstanden werden. Darauf aufbauend sollten dann technische und rechtliche Anforderungen an Smart-TVs formuliert werden, die auf Basis der deutschen Datenschutzgesetze eine Richtschnur und eine rote Linie für einen beanstandungsfreien Einsatz von Smart-TVs in Deutschland darstellen sollen.

Das Prüfprojekt

Unter Federführung des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) wurde ein technisches Prüflabor aufgebaut (bzw. das bestehende Labor an die Smart-TV Prüfung angepasst) und eine Prüfmethodik entwickelt, um vergleichbare Ergebnisse bei mehreren Smart-TVs zu erhalten.

Bei Smart-TVs stellte sich zuerst die Frage, was denn technisch überhaupt geprüft werden soll und kann. Da es bei diesen keine standardisierten Plattformen gibt (auch wenn viele auf einem Linux-Kern aufbauen) und sie zusätzlich als geschlossene Systeme fungieren (ein Zugriff auf das Filesystem bzw. auf eine Shell ist nicht möglich – zumindest wenn keine Sicherheitslücke ausgenutzt werden kann), wurde entschieden, eine dynamische Analyse der Datenflüsse des Smart-TV bei dessen Nutzung durchzuführen. Dazu wird ein Endgerät mittels WLAN an einen Standard-PC angeschlossen, der als Router fungiert. Dies bedeutet, dass sämtliche Kommunikation des Smart-TV mit beliebigen Servern, die über das Internet-Protokoll IP abgewickelt wird, über die Netzwerkkarte dieses Rechners geht. Durch den Einsatz des Netzwerkanalysetools Wireshark kann so festgestellt werden,

- mit **welchen Servern** (Domainname oder IP-Adresse) **wann** kommuniziert wird, sowie
- **welche Daten** dabei übermittelt werden (sofern nicht verschlüsselt).

Kommuniziert ein Smart-TV verschlüsselt über das SSL/TLS-Protokoll mit einem Server, dann stellt dies ein Problem der technischen Prüftransparenz dar, da die Inhaltsdaten der Internetkommunikation verborgen sind. Dies ist zwar beim Einsatz der Betroffenen aus Gründen der Vertraulichkeit löblich (und auch notwendig), für einen Laboraufbau aber sehr hinderlich. Bei den Analysen wurde auch ein Web-Proxy (BurpSuite Pro) eingesetzt, der als Man-in-the-Middle die verschlüsselte HTTPS-Kommunikation „knacken" sollte – funktioniert hat dies allerdings bei den aktuellen Smart-TV-Geräten nicht (mehr), da diese wohl aus den Fehlern der Vergangenheit gelernt haben und die Überprüfung der Serverzertifikate nun korrekt implementieren. Da ein Smart-TV im Gegensatz zu einem Smartphone es nicht zulässt, dass eigene selbstsignierte SSL-Zertifikate installiert werden können, beschränkt dieser Sicherheitsmechanismus die Möglichkeiten eines Prüfers. Abbildung 1 zeigt das kleine Prüflabor beim BayLDA.

Abbildung 1: Prüflabor für Smart-TVs beim BayLDA

Die Datenschutzprüfung

Zur Durchführung der Prüfung wurden aktuelle Smart-TV-Geräte benötigt. Dazu wurden die Hersteller von Smart-TVs über die beabsichtigte Prüfung informiert und um ein aktuelles Leihgerät gebeten. Dieser Bitte sind alle 13 Unternehmen nachgekommen und haben auch das Angebot des BayLDA angenommen, bei der Durchführung der Prüfung anwesend zu sein. Die Hersteller wurden so ausgewählt, dass ca. 90 % Marktabdeckung (der Hersteller, nicht des Gerätemodells) erreicht wurden. Die Teilnahme von Vertretern der Hersteller hatte auch den Vorteil, dass bei der Prüfung auftretende Fragen teils schnell geklärt werden konnten sowie dass die transparente und unvoreingenommene Prüfung auch so an diese kommuniziert werden konnte.

Abbildung 2: Die ersten Testgeräte sind eingetroffen

Nachdem die ersten Testgeräte beim BayLDA eingetroffen waren (Abbildung 2) konnte die systematische Prüfung beginnen:

1. Ausgepackt und eingesteckt

Dieses Prüfszenario hatte die Transparenz der Informationen vor Nutzung eines Smart-TV im Fokus. Diese ist auch insofern wichtig, da auf Grund dieser eine Entscheidung über die Verwendung eines Gerätes getroffen werden soll(te). Die Ergebnisse waren allerdings ernüchternd, da nur knapp die Hälfte der Geräte nach Inbetriebnahme überhaupt eine Datenschutzerklärung anbot (Abbildung 3).

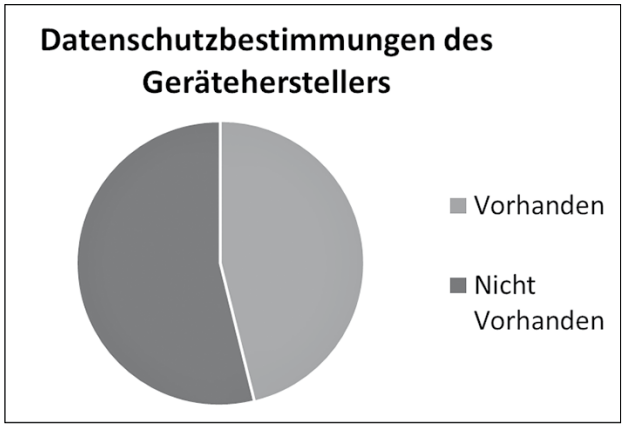

Abbildung 3: Kein Betrieb ohne Datenschutzerklärung!

Weniger zurückhaltend war die Verteilung der Geräte, die noch vor Lesen der Datenschutzbestimmungen im Hintergrund eine Internetkommunikation mit dem Hersteller aufgenommen haben (Abbildung 4).

2. Ende des anonymen Fernsehens: HbbTV

Wird ein Smart-TV an das Internet angeschlossen, dann erscheint es noch so, als würde sich beim reinen Anschauen von Filmen und Sendungen nichts geändert haben. Das Smart-TV könnte als kontrollierte Nutzung von Apps oder der Mediathek verstanden werden. Dass dies nicht so ist, liegt auch an einer neueren technischen Entwicklung, die unter dem Namen „Hybrid Broadcast Broadband TV“ (HbbTV) standardisiert wurde. Dies stellt einen Paradigmenwechsel bei der Programmnutzung dar. War es bis jetzt so, dass das Fernsehprogramm als unidirektionaler Empfang des Rundfunksignals eine vollständig anonyme Nutzung zwangsläufig technisch mit sich brachte, ändert HbbTV dies nun vollständig. Es wird ein sogenannter Rückkanal zur Verfügung gestellt, über den das Fernsehgerät aktiv mit beliebigen Servern kommunizieren kann. Technisch ist dies so umgesetzt, dass neben dem Rundfunksignal digitale Zusatzinformationen übertragen werden, die auch eine URL beinhalten. Wie bei Webbrowsern üblich, kann damit auch der Smart-TV über das HbbTV-Protokoll eine Webseite laden, die spezielle Rahmenbedingungen für den Einsatz mit HbbTV umsetzen muss, ansonsten aber mit HTML5, CSS und JavaScript wie bei Webseiten bekannte Entwicklungen ermöglicht. Eine davon ist der Einsatz von Tracking-Verfahren, die es z. B. durch den Einsatz von Cookies ermöglichen, das Nutzungsverhalten eines konkreten Smart-TV zu ermitteln. Dabei greifen wie bei Browsern zwar auch Schutzmechanismen wie die Same-Origin-Policy, die einen Zugriff auf Cookies fremder Domänen unterbinden. Bei den Tests wurde aber trotzdem ein senderübergreifendes Tracking (innerhalb einer Senderkette) festgestellt, bei dem periodisch (ca. jede Minute) ein Aufruf an den Tracking-Server erfolgte und damit die Verweildauer auf einem Sender (zu einer Uhrzeit) sowie der Wechsel zu einem anderen Sender (der Sendergruppe) festgestellt werden konnte. Möglich machen dies wie sonst im Web auch die sogenannten Third-Party-Cookies – nur bei Smart-TVs können diese meist nicht gelöscht werden.

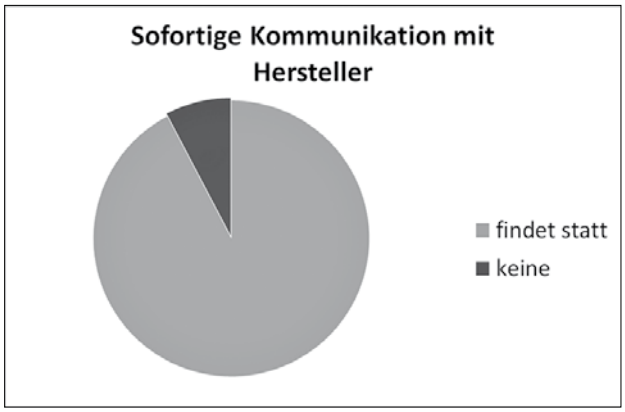

Abbildung 4: T. V. nach Hause telefonieren …

Wer jetzt der Meinung sein sollte, dies dürfte doch nicht zulässig sein, dem darf die Kurzantwort sehr häufiger und sehr juristischer Diskussionen zu diesem Thema gegeben werden: Es ist unklar. Es gibt das eine Argument, das sagt, dass ein Smart-TV nichts anderes als einen mit dem Internet verbundenen PC darstellt (der auch noch TV kann). Unter dieser Prämisse wären dann die gleichen rechtlichen Anforderungen wie beim Tracking von Webseiten zu stellen. Dies würde bedeuten, dass über den Einsatz von Trackingverfahren informiert werden sowie eine Widerspruchsmöglichkeit vorhanden sein muss. Dass letztere technisch auch bei Webseiten meist nicht funktioniert, da nach einem sogenannten Opt-out weiterhin HTTP-Requests an den Tracking-Anbieter (mit einem kleinen Opt-out-Flag) gehen, sei nur am Rande erwähnt. Das andere Argument sagt, dass ein Anschluss eines Smart-TV, der ja nicht nur HbbTV kann, nicht unmittelbar mit einem PC gleichzusetzen ist. So ist es vorstellbar, dass (per WLAN) nur auf die lokale Filmdatenbank zugegriffen oder ausschließlich YouTube als „smarte“ Applikation verwendet werden soll. In diesem Fall wäre vor dem Aufbau eines internetbasierten Rückkanals, der auch immer IP-Adressen be-

inhaltet, um Erlaubnis zu fragen. Bei der Analyse von zehn Sendern (fünf privat, fünf öffentlich-rechtlich) wurde festgestellt, dass immerhin acht auch eine Datenschutzerklärung hatten, die über den Einsatz von Tracking-Verfahren informierte. Sieben der zehn analysierten Sender setzen Tracking-Verfahren schon ein, bevor die speziellen Möglichkeiten einer HbbTV-Seite (durch Drücken des „Red Buttons" auf der Fernbedienung) überhaupt genutzt werden. Die Zielsetzung der Trackingverfahren ist offensichtlich: Zum einen soll das Einschaltverhalten ermittelt werden – damit gehören die Gfk-Panels, die eine Basis für die Verteilung der Werbeeinnahmen darstellen, bald der Vergangenheit an. Zum anderen ermöglicht HbbTV die Einblendung individueller Werbung auf Basis der Nutzung des Smart-TV. So können passend zur Kochsendung geeignete Weine oder zur Sendung über Bandscheibenvorfälle passende Reha-Maßnahmen beworben werden. Schützen wird sich der Normalanwender davor kaum können, ist doch die Technik intransparent und die geeignete Konfiguration einer Gateway-Firewall im eigenen Hausnetz doch eher etwas für Technik-Enthusiasten.

Ob HbbTV in dieser Form weiterbetrieben werden kann, hängt von der weiteren rechtlichen Bewertung der komplizierten Rahmenbedingungen sowie der Zurückhaltung des Tracking-Verhaltens von Seiten der Fernsehsender ab, die bei einem exzessiven Einsatz einen Vollzug von Seiten der Aufsichtsbehörden geradezu erzwingen würden.

3. Apps bei Smart-TV

Wie bei Smartphones und Tablets gibt es auch bei Smart-TVs Apps, die genutzt, oder moderner ausgedrückt, für ein besseres Nutzererlebnis verwendet werden können. Diese kommen (noch) nicht von Google oder Apple Stores, sondern sind von der Basis so vielfältig wie die technischen Plattformen, auf denen Smart-TVs betrieben werden. Entsprechend unterscheidet sich die Anzahl der Apps, die von wenigen vorinstallierten bis zu Hunderten von Anwendungen reichen. Heruntergeladen werden diese über das Smart-TV-Gerät, aber nicht zwingend vom Smart-TV-Hersteller. So gibt es einen Akteur „App-Store-Betreiber", der eine eigene verantwortliche Stelle sein kann und in Eigenmächtigkeit Apps für den Download bereitstellt sowie evtl. auch eine Registrierung der Nutzer durchführt.

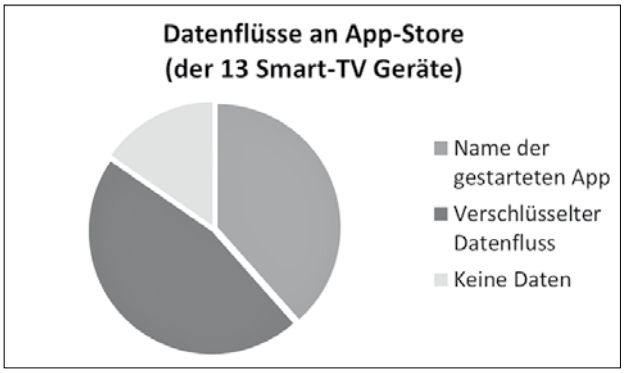

Abbildung 5: Datenschutz verletzt: der App-Store hört mit

Technisch sind die meisten Apps als Web-App umgesetzt (obwohl bei manchen Plattformen auch native Apps möglich sind). Der Start erfolgt dann durch den Aufruf einer der installierten App zugeordneten URL. Mit dieser findet eine Kommunikation mit dem App-Hersteller, der selbst für den Datenschutz bei seiner App verantwortlich ist, statt. In der Prüfung wurde allerdings bei knapp der Hälfte der Testgeräte festgestellt, dass auch an den App-Store der Start einer App, verbunden mit einer geräte- oder installationseindeutigen ID, übermittelt wurde (Abbildung 5). Damit werden Profile der App-Nutzungen erhoben, die anhand des App-Namens, der Häufigkeit und des Zeitpunkts durchaus nicht uninteressante Aussagen ableiten lassen, beispielsweise die Nutzungshäufigkeit von YouTube oder eines Spieles mit wilden Vögeln.

4. USB-Medien

Smart-TV-Geräte bieten auch umfangreiche Möglichkeiten der Medienwiedergabe aus USB-Datenträgern an. Dies können heruntergeladene Videodateien, MP3-Sammlungen oder die letzten Urlaubsfotos sein. Dazu wird das USB-Medium in einen Slot am Gerät gesteckt, und die Verarbeitung erfolgt lokal am Gerät. Umso überraschender war es, dass bei vier Geräten beim Einstecken und Nutzen der lokalen Mediendateien Datenflüsse stattfanden (Abbildung 6).

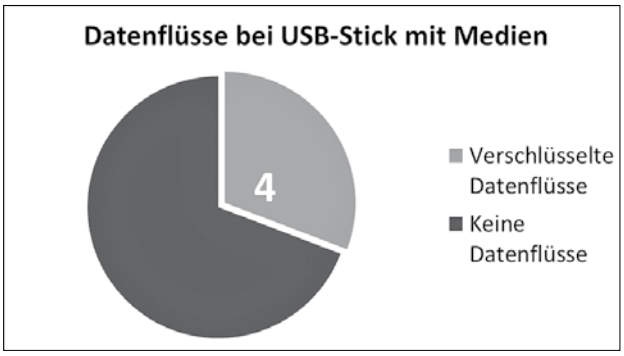

Abbildung 6: Smart-TV beim Ausplaudern erwischt …

Da diese allerdings mit HTTPS verschlüsselt und Man-In-the-Middle-Methoden mangels Möglichkeit einer Einspielung von eigenen Test-Serverzertifikaten nicht möglich waren, konnten nur heuristische Prüfverfahren angewandt werden, um den Inhalt der Übermittlungen zu erhellen. In der Prüfung wurden beispielsweise viele Grafikdateien mit sehr langen Dateinamen auf einem USB-Stick erzeugt und die Größe der verschlüsselten Datenpakete mit der Größe verglichen, wenn die gleiche Anzahl Dateien mit sehr kurzen Dateinamen auf einem Stick enthalten war. Selbiges wurde mit unterschiedlich großen Mediendateien durchgeführt. Indizien dafür, dass Dateinamen und Inhalte der USB-Medien das Smart-TV verlassen haben, wurden nicht gefunden, da die Größe der verschlüsselten Pakete gleich groß war. Bei einem Hersteller (der übrigens seinen Sitz nicht in Bayern hatte) wurden mit einem mobilen Prüflabor bei dessen Firmensitz die Tests wiederholt – allerdings hatten wir dort das echte Server-Zertifikat erhalten (und nach der Prüfung wieder gelöscht). Damit war es uns möglich, einen Einblick in die HTTPS-Verbindungen zu nehmen (leicht zu machen mit der Burp-Suite). Festgestellt haben wir in diesem Fall, dass statistische Nutzungsdaten des Medienplayers (z. B. Stick ein, Foto ausgewählt, Video ausgewählt), nicht aber Dateinamen oder Inhalte übertragen wurden.

5. Aufnahmen von Fernsehsendungen

Fast alle Smart-TVs haben die Möglichkeit, Fernsehsendungen auf internen oder externen Festplatten aufzuzeichnen. Wie bei den USB-Medien würde man hier nicht zwingend Datenflüsse an Dritte erwarten. Bei sieben Geräten fanden diese dennoch statt, wobei fast alle davon ebenfalls HTTPS-verschlüsselt erfolgten.

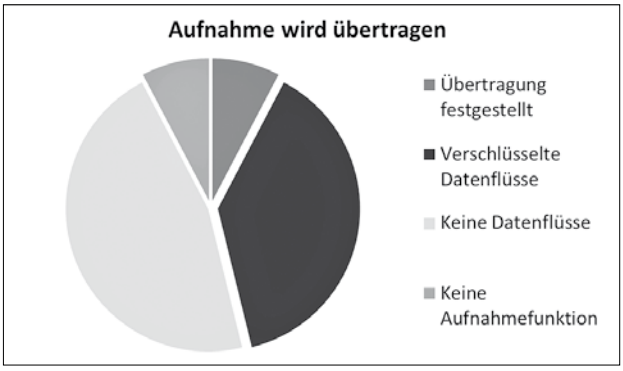

Abbildung 7: Auch Mitschnitt und Wiedergabe kommen ans Licht

Anders als bei den USB-Medien ist in diesen detektivische Spurensuche schwierig, da die Größe der verschlüsselten Datenpakete keinen Rückschluss darüber ableiten lässt, ob die aktuelle Sendung enthalten ist. Bei dem einen Hersteller, bei dem wir mittels des mobilen Prüflabors einen Einblick in die verschlüsselte HTTPS-Verbindung nehmen konnten, wurde festgestellt, dass sowohl die Aufnahme (Sender, Zeitpunkt) als auch die Wiedergabe gepaart mit einer eindeutigen ID an den Hersteller übertragen wurde (Abbildung 7).

Security

Datenschutz ist der Schutz des Persönlichkeitsrechts eines sogenannten Betroffenen – also auch eines Smart-TV-Nutzers. Dazu gehört neben der Frage, ob und welche Daten überhaupt an Hersteller, Fernsehsender, App-Store-Betreiber, … übermittelt werden dürfen, auch, ob die Sicherheit im Sinne von *Security* ausreichend ist. Bei Smart-TVs ist dieses Themenfeld sehr abhängig vom Hersteller, der Modellversion und natürlich vom aktuellen Softwarestand der Firmware. Systematische Tests der Sicherheit waren aus Ressourcengründen im Rahmen des Smart-TV-Prüfprojekts nicht möglich. Aufgefallen sind allerdings doch einige Punkte:

- Die HTTPS-Verschlüsselung ist bei den aktuellen Geräten zumindest insofern korrekt implementiert, als die Server-Zertifikate auf die Gültigkeit (bezüglich des Ausstellers) überprüft werden. Die Konfiguration der HTTPS-Endpunkte an den Servern ließ allerdings teils zu wünschen übrig. So war Perfect Forward Secrecy (PFS) nicht immer vorhanden. Sogar SSL3 kam teilweise zum Einsatz.

- Bei Portscans an die Smart-TVs waren einige Ports vorhanden und offen, deren Funktion nicht ganz klar war. Bei einigen waren hier Debug-/Test-Zugänge vorhanden, auf die auch bei Produktivversionen innerhalb des lokalen Netzes zugegriffen werden kann. Inwiefern hier Risiken vorhanden sind, wäre noch zu klären.

- Die HbbTV-Seiten, die automatisch und auch ohne aktive Nutzung eines Betroffenen von den Fernsehsendern auf den Smart-TV geladen werden, basieren im Großen und Ganzen auf HTML5, CSS und JavaScript. Würde ein Angreifer eine solche Seite übernehmen, dann hätte dieser Zugriff auf das Smart-TV mit den Schnittstellen, die der HbbTV-Standard definiert. Während ein Ausschalten eines Smart-TV aus der Ferne beim Endspiel der Fußball-Europameisterschaft nur sehr ärgerlich wäre (für manche auch mehr als das), wird es sehr kritisch, wenn über proprietäre Schnittstellen auf diese Weise auf die Kamera und das Mikrophon zugegriffen wird. Dass dies unter realistischen Rahmenbedingungen schon heute möglich ist, wurde im Rahmen einer Reportage über Smart-TVs sogar schon im Fernseher gezeigt *(http://www.swr.de/marktcheck/smart-tv-spione/-/id=100834/did=15300884/nid=100834/1ncw4pz/)*.

- Dass Softwaresysteme Schwachstellen enthalten, lässt sich (zumindest praktisch) nicht verhindern. Deswegen kommt der Einspielung von Sicherheitsupdates eine zentrale Rolle zu. Da dies vom Smart-TV-Hersteller gemacht werden muss, besteht die Gefahr, dass – ähnlich wie bei „alten" Android-Smartphones – Sicherheitslücken nicht immer geschlossen werden können.

- Die meisten Plattformen der Smart-TV-Geräte haben noch keine ausreichende Sicherheitsarchitektur. So gibt es Hersteller, bei denen alle Apps immer mit Root-Rechten laufen. Die Sicherheit soll über die korrekte Nutzung von APIs sichergestellt werden. Dass dies nur schlecht funktioniert, wird mittlerweile regelmäßig auf IT-Sicherheitskonferenzen dargestellt, bei denen Smart-TVs gehackt werden.

Andreas Sachs

Andreas Sachs ist Informatiker und leitet das technische Referat beim Bayerischen Landesamt für Datenschutzaufsicht in Ansbach. Zu seinen Aufgaben gehören die Beratung und Kontrolle von in Bayern ansässigen Unternehmen in den Bereichen IT-Sicherheit und technischem Datenschutz.

Wie geht es weiter?

Nach Durchführung der Prüfung der dreizehn Testgeräte wurden vom BayLDA technische Prüfberichte erstellt und an die beteiligten Datenschutzaufsichtsbehörden und die Hersteller versandt. Ziel war, wie bei anderen Datenschutzprüfungen auch, bei den technisch festgestellten Gegebenheiten (hier: Datenflüsse) ein gemeinsames Verständnis mit allen Beteiligten zu haben. Auf dieses kann dann eine rechtliche Bewertung aufgebaut werden. Dies hat auch stattgefunden und wurde in Form einer sogenannten Orientierungshilfe niedergeschrieben, in der die deutschen Datenschutzaufsichtsbehörden eine abgestimmte technische und/oder rechtliche Auffassung zu einem Themengebiet veröffentlichen. Die Orientierungshilfe „Datenschutzanforderungen an Smart-TV-Dienste“ kann unter *http://www.lda.bayern.de/de/orientierungshilfen.html* heruntergeladen werden. Diese wird von den Datenschutzaufsichtsbehörden für den aufsichtlichen Vollzug verwendet, sollte ein Smart-TV sich nicht an die deutschen Datenschutzgesetzte halten.

Fazit

Das anonyme Fernsehen wurde faktisch abgeschafft. Der Weg, den Smart-TV nicht mit dem Internet zu verbinden, bleibt natürlich bestehen, nur ist dann auch das „Smart“ nicht mehr nutzbar. Dies wird allerdings zukünftig nur für informierte Konsumenten, die für den Datenschutz auch bereit sind, Einschränkungen bei der Nutzung neuer Technologien auf sich zu nehmen, ein Weg sein. Experten für Netzwerkanalyse und Firewalls können auch zuhause die eigenen Systeme, samt Smart-TV, versuchen abzuschotten – ohne Garantie, ob dann die smarten Dienste auch weiterhin voll funktionsfähig sein werden. Es bleibt zu hoffen, dass die rechtlichen Instrumente (auch im Hinblick auf das neue Datenschutzgesetz, die EU-Datenschutzgrundverordnung, die ab Mitte 2018 gelten wird) ein exzessives Erheben von Nutzungsprofilen und deren Verarbeitung mit Big-Data-Methoden regeln können. Die Macht der Konsumenten bleibt natürlich erhalten – die Frage, ob Datenschutz für Hersteller von Smart-TVs ein Wettbewerbsvorteil sein kann, der möglicherweise auch höhere Kosten rechtfertigt und transparente Allgemeine Geschäftsbedingungen belohnt, wird die Zeit beantworten.

Sebastian Jekutsch

Fairere Computer

Dass IT-Produkte nicht fair produziert werden, etwa im Sinne des Fair Trade, hat viele Gründe, wie wir immer wieder in Artikeln aus der AG Faire Computer *des FIfF erfahren konnten. Dennoch ist zu beobachten: Sie werden immer etwas fairer. Im Beitrag zur FIfFKon 2015, der ausführlich bebildert und verlinkt im Blog* Faire Computer *zu finden ist, legen wir dar, wie dies tatsächlich geschieht: Durch investigative Aufdeckung von Unfairness, aufgrund derer negative Presseberichte folgen, reagieren die gebrandmarkten Unternehmen mit Korrekturmaßnahmen. Das Blog zeigt drei Beispiele aus Indonesien, Malaysia und der D.R. Kongo. Manchmal entstehen auch Pionierprojekte daraus, die [illegible] nchmal entstehen sogar Gesetze daraus, und dies ist ohne Zweifel*

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Der Beitrag ist zu finden unter *htt*

Sebastian Jekutsch

Sebastian Jekutsch recherchiert und informiert seit nun fünf Jahren über *sozialverträgliche IT-Produktion.* Er ist Sprecher der *AG Faire Computer* des FIfF und Initiator des *blog.faire-computer.de*.