Clever oder tumb?

Was Smart-TVs ins Internet übermitteln und wie leicht sie sich hacken lassen

Aktuelle TV-Geräte, wie wir sie in dieser Ausgabe testen, wollen mit dem Internet verbunden sein. Das ist einerseits ein Sicherheitsrisiko und birgt anderseits auch Gefahren für die Privatsphäre. Uns hat interessiert, wie viel die Geräte schwatzen, mit wem sie reden, worüber sie sprechen und welchen Einfluss man nehmen kann.

Von Peter Siering

Dass moderne TV-Geräte munter im lokalen Netzwerk und bis ins Internet hinaus plappern, ist kein Geheimnis. Vor vier Jahren haben wir uns angeschaut, was dabei vor sich geht [1]. Außerdem befassen sich diverse wissenschaftliche Veröffentlichungen mit der Frage [2]. Wir haben deshalb den Geräten aus unserem aktuellen Test auf Seite 82 genauer auf den Netzwerkverkehr geschaut und vergleichen die Ergebnisse mit den Erkenntnissen aus den vorgenannten Veröffentlichungen. Der Artikel ab Seite 78 zeigt, wie sie Ihrem Smart-Plappermäulchen einen Maulkorb verpassen. Auf Seite 90 stellen wir Alternativen zu den smarten Funktionen der TV-Geräte vor.

Viele Akteure

Für die Betrachtung des Netzwerkverkehrs eines TV-Geräts ist es hilfreich, die Akteure zu kennen: Da wären zunächst fest im Betriebssystem verdrahtete Funktionen, die das Gerät ins Netzwerk bringen und die unter anderem sicherstellen, dass es als Abspielziel für Mediendateien gefunden wird. Die Geräte schicken regelmäßig Pakete an alle ins lokale Netz. Auch umgekehrt lauschen die Geräte auf solche Ankündigungen und können deshalb ein NAS als Quelle für Mediendateien erkennen und das Durchsuchen nach abspielbarem Material anbieten. Solcher Netzwerkverkehr ist nur lokal sichtbar.

Hinzu kommen Funktionen, die über Apps realisiert werden. Die Hersteller bestücken die Geräte üppig und der Nutzer kann weitere nachinstallieren. Die meisten Apps sind auf einen bestimmten Dienst ausgerichtet, etwa Netflix, Amazon-Video, Maxdome, YouTube und die Mediatheken der Sendeanstalten. Die Apps nehmen übers Internet Kontakt zu den Servern der Dienstleister oder des Herstellers auf, ohne dass der Nutzer darauf Einfluss nehmen kann. Auf einigen Smart-TV-Plattformen erfährt er immerhin noch in den Detailinformationen, welche Rechte sich eine App herausnimmt – etwa, auf welche Informationen sie zugreifen darf.

Sehr zentral und Gegenstand vieler Untersuchungen sind die Extraangebote eines smarten TVs beim Fernsehen: Im Standard Hybrid Broadcast Broadband TV (HbbTV) ist festgeschrieben, wie sich per Rundfunk übertragene Programme um interaktive Inhalte ergänzen lassen. Letztlich überlagert dabei ein spezielles Webangebot das TV-Bild oder verdrängt es ganz. Die Sender nutzen das, um ihre Mediatheken zugänglich zu machen, Programminformationen anzubieten oder – im Fall der Shopping-Kanäle – sogar fürs Verkaufen. Hier findet rege Kommunikation übers Internet statt.

Obendrein bündeln die meisten Smart-TVs alle Funktionen in einer speziellen Oberfläche, die über den Home-Knopf der Fernbedienung erreichbar ist und bei Samsung beispielsweise „Smart Hub“ heißt. Sie lebt von bunten Bildern, die sie den jeweiligen Apps oder Funktionen entlockt. Oft nutzen die Hersteller Freiflächen auch, um für ihre eigenen Angebote zu werben oder die Werbung Dritter einzublenden. Man hat mitunter den Eindruck, auf dem Bildschirm sei ein Briefkasten explodiert, der in den letzten Wochen mit Werbezetteln vollgestopft worden ist.

Traumloser Schlaf

Angesichts der Anzahl der Akteure und angesichts der Tatsache, dass sich viele Apps nicht entfernen lassen, fällt es enorm schwer, den entstandenen Netzwerkverkehr konkret einer Quelle zuzuordnen. Letztlich gelingt das nur, indem man durch Bedienung einzelne Akteure reizt und beobachtet, was an der Netzwerkschnittstelle passiert. Nicht immer gelangt man so an gesicherte Erkenntnisse (gleich mehr dazu im Kontext der Experimente mit HbbTV) – um die zu erlangen, dürften die Hersteller die Geräte nicht vernageln, sondern müssten sie für solche Untersuchungen öffnen.

Wir haben in mehreren Betriebsphasen die Netzwerkaktivität der Geräte verglichen: bei der Ersteinrichtung, beim Fernsehen und im Standby. Die quantitative Auswertung hat die Enterprise Ausgabe des Netzwerkanalyse-Tools ntopng erleichtert, die uns der Hersteller freundlicherweise für diese Zwecke zur Verfü-

HbbTV überlagert das TV-Bild mit speziell präparierten Webseiten; das TV-Gerät führt dabei unter anderem enthaltenen JavaScript-Code aus.

gung gestellt hat; diese Ausgabe von ntopng zeichnet langfristig Daten in einer Datenbank auf und erlaubt eine spätere Auswertung. Parallel haben wir den Netzwerkverkehr mit Wireshark komplett aufgezeichnet, um im Nachhinein Details nachspüren zu können.

Bei der Ersteinrichtung fällt Panasonic positiv auf: Das Gerät stellt per DNS gerade mal Namensanfragen für neun verschiedene Server, LG und Hisense bringen es auf 18. Die Android-basierten Geräte von Philips und Sony fragen über 40 Namen an. Samsung interessiert sich für fast 60. Die Anzahl der Anfragen steht in direkter Relation zu den Servern, mit denen sich die Geräte während der Installation unterhalten. Darunter sind tendenziell harmlose, etwa Zeitserver, aber auch viele fragwürdige.

Fragwürdig, weil wir allen Geräten während der Installation die Zustimmung zu irgendwelcher Datenübertragung verweigert haben. Lediglich bei Philips und Sony mussten wir Googles Bedingungen zustimmen, sonst ging es gar nicht weiter; entsprechend greifen die auch auf Google-Server zu. Viele Fernseher riefen noch während des Einrichtens HbbTV-Angebote ab. Oft finden sich Content-Provider wie Netflix und Maxdome in den Listen. Auch Facebook und Microsoft tauchen auf. Die größte Plaudertasche ist, was den DNS-Anfragen nach bereits zu erwarten war, Samsung.

Falsche Fährten

Sieht man sich die Verteilung des gesamtem Netzwerkverkehrs über eine längere Zeit an, so tauchen sehr häufig Amazon, Google und Microsoft auf. Wenn man das im Detail betrachtet, so wird schnell klar: Hier geht es nicht um die Dienste dieser Firmen, sondern um deren Cloud-Server, die andere Unternehmen buchen können, um nicht selbst die Infrastruktur betreiben zu müssen. Das Gleiche gilt für Content

Wenn die unscheinbare Einblendung im Bild erscheint, hat das TV-Gerät bereits mit den Servern der ARD-Kontakt gehabt.

Delivery Networks wie Akamai. Beim Auswerten und womöglich Blockieren von Zugriffen kann man hier also schnell auf eine falsche Fährte geraten; am besten hält man sich dafür an die initial angefragten DNS-Namen.

Die quantitative Auswertung von TV-Schauen und Standby gibt ein ähnliches Bild ab: LG, Panasonic und Hisense sind schweigsam und kommunizieren selten. Philips redet dann und wann mit Google und Netflix, Sony schwatzt häufiger auch mit eigenen Servern. Samsung plappert ständig vor allem mit Servern der eigenen Home-Base – verglichen mit dem sparsamsten Redner anhand der Paketzahl um einem Faktor 50 mehr. Im Standby verstummen LG, Hisense, Philips und Samsung. Panasonic annonciert eingebaute Server-Dienste und Sony schwatzt in reduzierter Frequenz weiter.

Außerdem haben wir uns mit dem Werkzeug mitmproy angesehen, ob die Geräte anfällig für Angriffe eines „Man in the Middle“ sind, der sich in den HTTP- und HTTPS-Verkehr einschleicht und die Inhalte sichtbar macht. Im Fall des verschlüsselten HTTPS schiebt er den TV-Geräten ein selbstsigniertes Zertifikat unter. Die Webbrowser aller TV-Geräte haben das „falsche“ Zertifikat erkannt und den Verbindungsaufbau zu einem SSL-gesicherten Angebot als manipuliert gebrandmarkt oder den Zugriff gleich verweigert. In keinem Gerät war es möglich, per Browser die CA der selbstsignierten Zertifikate zu importieren.

In einem weiteren Schritt haben wir untersucht, ob die Geräte bei der Update-Prüfung bemerken, dass sie über den mitmproxy ein selbstsigniertes Zertifikat untergeschoben bekommen. Nur Sony und Samsung zeigten einen allgemeinen Hinweis an, dass bei der Update-Prüfung etwas schiefgelaufen sei – sie lassen sich nicht von einer Fake-Site Updates unterschieben. Philips, Hisense und Panasonic vermitteln den Eindruck, dass keine Updates erhältlich seien, trotz HTTPS-Verbindung nahmen sie aber am unpassenden Zertifikat keinen sichtbaren Anstoß – womöglich würden sie ein Fake-Update akzeptieren. LG verwendet offenbar HTTP für die Update-Prüfung und konnte entsprechend keine Manipulation erkennen.

Der mitmproxy diente uns zudem dazu, die HbbTV-Kommunikation mitzulesen. Die läuft interessanterweise nach wie vor fast vollständig unverschlüsselt. Lediglich das ZDF liefert Bilder seines Programmführers über einen SSL-gesicherten Server aus. HbbTV als über das TV-Bild gelegtes Webangebot verwendet zur Kommunikation fast ausschließlich HTTP. Und nicht nur das: Im Datenstrom finden sich die auch in Webangeboten typischen Daten, die ein Nachverfolgen des Nutzers erlauben, etwa per Cookie, per Zählpixel und sonstiger Merkmale.

Verkappter Browser

Die TV-Geräte führen ausgelieferten JavaScript-Code wie ein Browser aus, was den Betreibern erhebliche Möglichkeiten einräumt. Die beginnen schon deutlich, bevor der Nutzer mit dem Angebot er Sender interagiert: Sobald er auf einen Kanal wechselt, ruft sein TV-Gerät im HbbTV-Angebot des Senders eine URL auf, die im DVB-Datenstrom übermittelt worden ist. Noch mal: Dieser Abruf geschieht ohne Zutun. Sie erkennen ihn daran, dass im TV-Bild der Hinweis erscheint, dass Sie weitere Informationen über das Betätigen des roten Knopfes erhalten (oft kombiniert mit etwas Werbung).

Von nun an hat der TV-Sender den Nutzer am Haken: Bei einigen Sendern (ARD und RTL) konnten wir beobachten, dass sie anschließend das TV-Gerät regelmäßig wieder das HbbTV-Angebot aufrufen ließen oder beim Programmwechsel

Smart-TV-Datenverkehr bei Erstinstallation

	Hisense	LG	Pansonic	Philips	Samsung	Sony
DNS-Abfragen (Namen / gesamt)	18 / 143	9 / 23	9 / 17	42 / 561	57 / 1404	49 / 450
Top ASN	Amazon, Google	Amazon, Akamai, Infonline	Amazon, Akamai, NTT, Microsoft, Google, Netflix	Amazon, Google, Akamai, Rackspace, Myloc	Amazon, Akamai, Microsoft, Facebook, Leaseweb	Amazon, Google, Akamai, Vanoppen
Top Länder	US	DE, IE, US	FR, IE, NL, US	DE, GB, IE, NL, US	DE, IE, NL, US	IE, NL, US
Daten (senden / empfangen in KByte)	105 / 630	135 / 367	382 / 2031	1300 / 10600	202 / 1200	941 / 4920

jeweils ermittelt mit ntopng vom Fabrikreset bis zur Anzeige des ersten regulären TV-Bilds; Geräte siehe Seite 82

erneut die URL ansprachen – ideal für die Sender, um zu sehen, wie lang ein Zuschauer verweilt. Die Programme der ARD, die ein gemeinsames HbbTV-Angebot nutzen, fielen besonders negativ auf: Wenn man per rotem Knopf tiefer einsteigt, übertragen sie jeden Tastendruck an den HbbTV-Server. Das sollte es den Betreibern erlauben, individuelle Benutzersessions nachzuspielen.

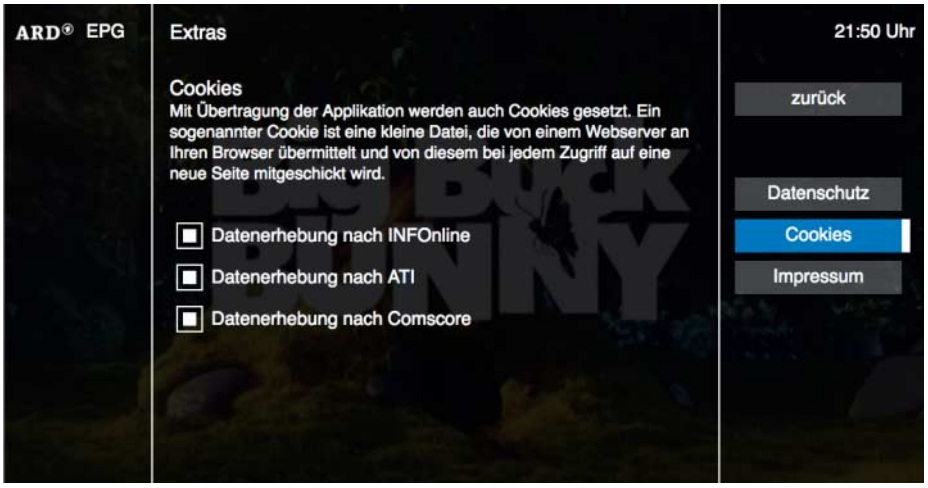
Die Standardmöglichkeiten, die Smart-TVs bieten, um sich der allzu engen Beobachtung durch die HbbTV-Angebote zu entziehen – nämlich eine Option zum „Nicht verfolgen" – hat keinen sichtbaren Einfluss gezeigt. Sie lässt bei HTTP-Anfragen an den HbbTV-Server den HTTP-Header „Do Not Track" (DNT) schicken. Wir haben bei dem obigen Verhalten allerdings keinen Unterschied mit und ohne diesen Wunsch sehen können. Hier setzen sich die Anstalten offenbar über den Wunsch der Nutzer hinweg.

Ein Blick mit nmap auf die auf den TV-Geräten erreichbaren Dienste per Netzwerkscan offenbarte eine Überraschung: Auf dem Panasonic-Gerät ist standardmäßig ein SMB-Server aktiv. Was auf den ersten Blick recht praktisch anmutet, ist brandgefährlich, weil das verwendete Samba knapp 10 Jahre alt ist, seit Jahren keine Sicherheitsupdates mehr erhält und obendrein nur SMBv1 spricht.

Auf allen Geräten waren einzelne Ports offen, ohne dass wir diesen Dienste zuordnen konnten – aus Sicherheitssicht ist das ein unnötiges Risiko. Selbst wenn die Hersteller die Ports vorgesehen haben, um etwa die Fernbedienung per App zu erlauben, sollte das abschaltbar sein. Leider lassen sich die Hersteller hier wenig in die Karten schauen: Samsung beispielsweise ändert gern mit Firmware-Updates die Funktionsweise solcher Schnittstellen, sodass freie Software zur Fernsteuerung auf die Nase fällt.

Wissen schafft

Die umfangreichste wissenschaftliche Untersuchung zu den Risiken von Smart-TVs ist die Doktorarbeit von Marco Ghiglieri vom Mai 2017. Sie fasst auch die Ergebnisse vieler zuvor veröffentlichter Arbeiten zusammen. Den Schwerpunkt bildet die Beobachtung des HbbTV-Verkehrs und eine Bewertung der Privacy-Risiken im zeitlichen Verlauf. So nahm von 2012 bis 2015 die Anzahl der TV-Sender mit HbbTV stark zu. So kommt die Arbeit zum Schluss, dass die Ambitionen der TV-Anstalten zunehmen, per HbbTV mehr über ihre Zuschauer herauszufinden – kein Wunder, können sie doch so bequem die Black Boxes ersetzen, mit denen bisher Zuschauerzahlen erfasst werden.



Besucher der HbbTV-Angebote der ARD-Familie können via Cookie Einfluss aufs Tracking nehmen. Standardmäßig sind alle Varianten aktiv.

Aus den Arbeiten ist der Prototyp einer Software entstanden, die etwa auf einem Raspberry Pi läuft und sich zwischen den HbbTV-Datenstrom des TV-Geräts und das Internet klemmt und erst auf expliziten Wunsch des Nutzers (via Einblendung auf dem TV-Gerät realisiert) Kontakt zu den HbbTV-Servern erlaubt. Leider ist diese Software auf den umgebauten Webseiten der TU-Darmstadt nicht mehr zu finden. Wir haben Kontakt zu Ghiglieri aufgenommen und er will sich bemühen, dass die Software wieder erhältlich ist. Er geht allerdings davon aus, dass sie aufgrund zunehmender SSL-Verschlüsselung von HbbTV nicht mehr wirksam ist – das indes deckt sich nicht mit unseren Beobachtungen.

Viele andere Punkte, die in den Veröffentlichungen kritisiert wurden, nämlich, dass die Smart-TV-Geräte bei der SSL-Validierung schlampen, konnten wir erfreulicherweise nicht mehr nachvollziehen. Die Hersteller haben ihre Hausaufgaben gemacht. Mit einer Ausnahme: LG scheint weiterhin beim Firmware-Update nachlässig zu sein, jedenfalls legt das der Vergleich der von uns in den Mitschnitten gesehenen Update-Methode mit der von Ghiglieri dokumentierten nahe.

Abgesang

Unterm Strich fällt vor allem Samsung negativ auf: Ohne Filter, wie im folgenden Artikel vorgestellt, sollte man diese Geräte nicht ans Internet lassen. Bei verschiedenen Modellen der Baureihe konnten wir abweichende Verhaltensweisen beobachten: Ein Gerät schickte permanent Bilder in die Samsung-Cloud, um sie zu skalieren, ein anderes griff im Minutentakt auf die HbbTV-Angebote von ARD und ZDF zu. Bei Samsung fehlt obendrein die Möglichkeit, gezielt HbbTV-Angebote einzelner Sender zu nutzen oder auszuklammern. Das heißt, bei aktivem HbbTV muss man bereit für den permanenten Aderlass von Daten sein. Das können die Smart-TVs von LG, Philips, Sony und Panasonic zumindest besser.

Ärgerlich bei allen Geräten ist, dass man stets eine Generalvollmacht für alle Akteure ausstellen soll. Welche Daten abseits von HbbTV wohin abfließen, bleibt oft unklar, auch weil viel verschlüsselt wird. Bei einigen Geräten konnten wir beobachten, dass sie regelmäßig Netflix ansteuerten, obwohl der Dienst weder konfiguriert noch die App gestartet war. Eine differenzierte Freigabe des Datenaustausches etwa mit Netflix bei einem Verbot für alle anderen Dienste ist nirgends vorgesehen. Hier könnten die Hersteller echt punkten. *(ps@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Spion im Wohnzimmer, Privacy und Sicherheit bei Internet-fähigen TVs, c't 4/2014, S. 78
[2] Marco Ghiglieri, Smart TV Privacy Risks and Protection Measures, TU-Darmstadt, http://tu-prints.ulb.tu-darmstadt.de/6187/1/Dissertation-MarcoGhiglieri_v2.pdf

Downloads, Studien: ***ct.de/yz8n***