Ronald Eikenberg

Spion im Wohnzimmer

Privacy und Sicherheit bei Internet-fähigen TVs

Moderne Fernseher bringen das Internet nicht nur in die Stube, sie nutzen es auch selbst gerne. Wir haben analysiert, was eine Auswahl aktueller Smart-TVs ins Netz schickt. Dabei gab es unangenehme Überraschungen.

Neue Fernseher haben fast durchgängig eine WLAN- oder zumindest eine Ethernet-Schnittstelle. Darüber kann man das Gerät per App steuern oder auf Medienserver im Heimnetz zurückgreifen. Allerdings hievt man die Flimmerkiste damit auch ins Internet, wovon sie ungeniert Gebrauch macht: Wie selbstverständlich übermittelt sie unter anderem, welchen Sender man gerade schaut – und das nicht nur dem TV-Sender, sondern auch Werbefirmen. Der Hersteller bekommt ebenfalls ein Stück vom Datenkuchen ab. Bei einigen Geräten stießen wir darüber hinaus auf handfeste Sicherheitsprobleme.

Um uns einen Überblick zu verschaffen, welche Daten ins Netz fließen, stellten wir einen Querschnitt aktueller Smart-TVs in unserem Labor auf: je ein Modell von LG, Panasonic, Philips, Samsung und Toshiba. Die Geräte durften über unser Testnetz auf das Internet zugreifen, während wir dem Datenverkehr mit Analyse-Tools wie Wireshark zu Leibe rückten. Noch bevor wir Browser oder Apps starteten, kommunizierten die Fernsehgeräte bereits fleißig mit diversen Servern – vor allem beim Wechseln der Sender.

Was da beim Zappen unverschlüsselt durch die Leitung fließt, ist die erste Stufe des Datenangebots Hybrid Broadcast Broadband TV (HbbTV), über das Fernseher aus dem Internet Informationen zum laufenden Programm oder auch passende Werbung nachladen. Wo die Daten abgeholt werden, gibt der DVB-Datenstrom vor. So erhält der Fernseher zum Beispiel beim Einschalten von Pro7 den Befehl, mit seinem rudimentären Browser die URL http://hbbtv.prosieben.de/service/redbutton_p7.php abzurufen und transparent über das TV-Bild zu legen.

Der rote Knopf

Es handelt sich bei der Seite um den „Red Button“, der das HbbTV-Portal des Senders anpreist. Dazu wird ein Banner in der unteren rechten Bildschirmecke angezeigt. Der Fernseher lädt die Red-Button-Seite automatisch von einem Server der Sendeanstalt, sobald man den Sender anwählt. Dadurch bekommt der Sender mit, wann der vernetzte Zuschauer zuschaltet. Bei jedem Abruf der Red-Button-Seite übermittelt der Browser dem Webserver des Senders die IP-Adresse des heimischen Internet-Anschlusses sowie Informationen über das eingesetzte TV-Gerät.

Dass diese Zugriffsdaten tatsächlich ausgewertet werden, zeigt eine Präsentation der ProSiebenSat1-Tochter SevenOne Media: Demnach wurde etwa der Red Button von ProSieben im Dezember 2013 von 5 890 000 verschiedenen Geräten (Unique Devices) angezeigt. Das Unternehmen hat im Jahr 2013 einen Zuwachs von 270 Prozent registriert. Offensichtlich erfasst SevenOne nicht nur die

Gesamtzahl der Abrufe, sondern kann die Geräte auch voneinander unterscheiden. Dieses Wiedererkennungsmerkmal mussten wir im Datenverkehr nicht lange suchen: Viele Sender legen Cookies im Fernseher ab, um das Zuschauerverhalten zu tracken – darunter auch die Sender der Gruppe ProSiebenSat1.

Ein besonders verbreitetes Cookie heißt utma. Diesem Namen begegnet man auch in Cookie-Speichern auf PCs immer wieder. Es enthält unter anderem eine individuelle Identifizierungsnummer sowie den Zeitstempel des ersten Erstkontakts mit dem Server. Auch den Zeitpunkt der letzten Sitzung merkt sich das Cookie.

Teilen macht Freude

Nicht nur die Sender bekommen das Einschalten mit; die meisten Red-Button-Seiten laden auch automatisch Inhalte von fremden Servern nach. Dabei fiel vor allem immer wieder ein alter Bekannter auf: Google Analytics. Nahezu alle wichtigen Privatsender und sogar der öffentlich-rechtliche Sender arte lassen die Abrufe der Red-Button-Seite vom externen Datensammler tracken – und somit faktisch auch das Einschalten des Senders. Die übertragenen Daten erlauben umfassende Rückschlüsse auf die Fernsehgewohnheiten des Zuschauers – und somit auch auf seine persönlichen Interessen. Wann wird der Fernseher für gewöhnlich eingeschaltet, welche Sender werden geschaut? Über welche Themen informiert sich der Nutzer? Ob man mit der Übertragung einverstanden ist, fragt keiner der Sender.

Technisch funktioniert das Tracking, indem die JavaScript-Datei http://www.google-analytics.com/ga.js in die Red-Button-Seite eingebettet wird. Daraus resultiert eine HTTP-Anfrage an Google, in dessen Header die URL der HbbTV-Seite steht. In diesem Moment hat Google bereits die externe IP-Adresse des Zuschauers und kann anhand der URL aus dem Header eindeutig auf den eingeschalteten Sender schließen. Ferner wird eine unsichtbare Grafik von der Adresse http://www.google-analytics.com/__utm.gif geladen. Darüber werden sogar die URL-Parameter des utma-Cookies an Google übertragen.

Wer glaubt, dass der Datenabfluss danach abebbt, liegt zumindest bei den ProSiebenSat1-Sendern falsch: Wir entdeckten im Datenstrom eine JavaScript-Datei namens hbbtvclient_longpolling.js, die dafür sorgt, dass der Fernseher nach dem Einschalten des Senders in regelmäßigen Abständen ein Lebenszeichen an den Sender schickt – selbst wenn der Red Button längst nicht mehr sichtbar ist. ProSiebenSat1 bekommt also nicht nur mit, wann man zuschaltet, sondern auch wie lange man hängen bleibt.

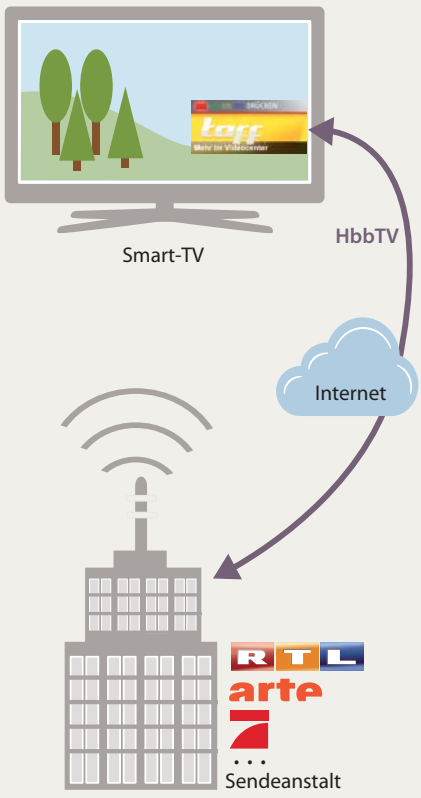
Rechtliches

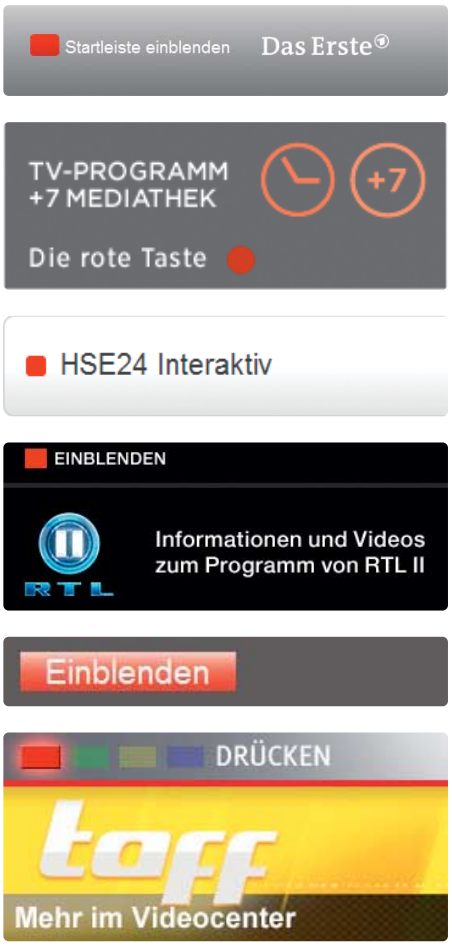
HbbTV ist inzwischen bei vielen neu gekauften Smart-TVs im Auslieferungszustand aktiv. Eine Aufklärung über die damit verbundenen Tracking-Maßnahmen erfolgt an keiner Stelle. Rechtlich ist schon die Verarbeitung der IP-Adressen höchst problematisch, da es sich nach Ansicht der meisten Juristen um personenbeziehbare Daten handelt, die den Vorschriften des Datenschutzes unterliegen. Eine Speicherung und Verarbeitung dieser Daten zu Tracking- oder Werbezwecken ist nur mit ausdrücklicher Einwilligung des Betroffenen erlaubt. Dieser muss zudem über die geplante Nutzung seiner Daten informiert werden. Fehlt es an einer solchen „aufgeklärten Einwilligung“, so ist die Speicherung und Verarbeitung von IP-Adressen nach Ansicht von Datenschutzbehörden klar rechtswidrig.

Diese Auffassung teilt auch der Datenschutzexperte Prof. Dr. Nikolaus Forgó vom Institut für Rechtsinformatik der Leibniz-Uni Hannover, den wir über unsere Beobachtungen informierten. „Bereits die Erhebung der Daten ist ein klarer Rechtsbruch. Dass die Daten auch noch an Google weitergegeben werden, ist nur noch das Sahnehäubchen obendrauf“. Nach Einschätzung des Datenschutzbeauftragten des Landes Schleswig-Holstein, Dr. Thilo Weichert, ist das Tracking „ganz klar ein Eingriff in das Recht auf infor-

Datendienst HbbTV

Beim Zuschalten erhält der Fernseher über den DVB-Datenstrom den Befehl, eine Webseite vom Server der Sendeanstalt abzurufen.





Die Red-Button-Einblendung fordert den Zuschauer auf, die rote Taste auf der Fernbedienung zu drücken.

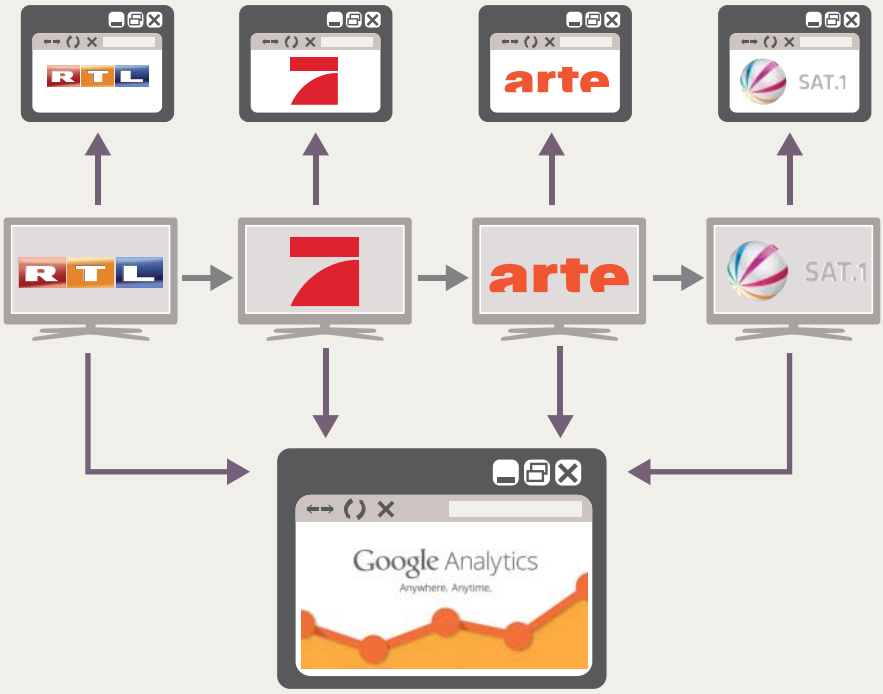
Stream Content

```
GET /launchbar/index.html HTTP/1.1
Host: cdn.digitaltext.rtl.de
User-Agent: HbbTV/1.1.1 (;Samsung;SmartTV2013;T-MST12DEUC-1111.1;;) WebKit
Accept: text/html,application/xhtml+xml,application/xml,application/vnd.hbbtv.xhtml
+xml,application/ce-html+xml,application/vnd.oipf.xhtml+xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Cookie: user_id_report=03DE2886FBF8A54932892F8747892FEF4FCD;
__utma=50207732.1228140272.1386842940.1386842940.1386842940.1;
__utmb=50207732.6.9.1386842958763; __utmc=50207732;
__utmz=50207732.1386842940.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
```

„Hallo, hier bin ich – und ich habe Kekse mitgebracht.“ – Das Smart-TV meldet unser Zuschalten an RTL.

HbbTV-Tracking durch Google Analytics

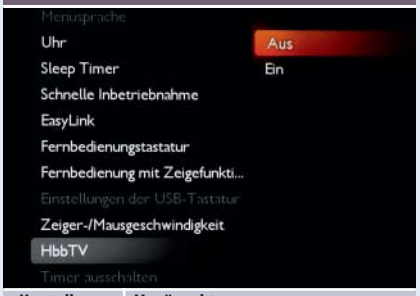
Während man durch die TV-Landschaft zappt, sendet der Fernseher immer wieder auch Datenpakete an Google.



Fernsehen ohne Zuschauer

Um die Datenpetze HbbTV abzuschalten, muss man tief im Menü des Fernsehers wühlen. Der folgenden Tabelle können Sie entnehmen, wo Sie den entsprechenden Menüpunkt bei den Smart-TVs der meistverbreiteten Hersteller finden.

HbbTV deaktivieren



Hersteller	Menüpunkt
LG	Option / HbbTV
Panasonic	Setup / Datenservice Anwendung / Service
Philips	allgemeine Einstellungen / HbbTV[1]
Samsung	System / Datendienst
Sony	Einstellungen / digitale Einstellungen / interaktive Anwendungseinrichtung
Toshiba	Optionen / Hybrid TV Standard

[1] erst nach einem Neustart aktiv

mationelle Selbstbestimmung (Grundrecht auf Datenschutz) als Konkretisierung des allgemeinen Persönlichkeitsrechts“.

Auch der niedersächsische Datenschutzbeauftragte Joachim Wahlbrink steht HbbTV höchst kritisch gegenüber: „Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche, anonyme Empfang von Rundfunkprogrammen auf dem Spiel“, so Wahlbrink.

ProSiebenSat1 erklärte gegenüber c’t, die Auslieferung des Red Button werde getrackt, um zu ermitteln, „wann die HbbTV-Angebote genutzt werden und wie die Wachstumsraten sind“. Dass man dadurch darauf schließen kann, wann die TV-Nation einschaltet, darauf geht die Sendergruppe trotz expliziter Nachfrage nicht ein. RTL zeigte sich auskunftsfreudiger. Das Unternehmen räumte ein, dass man zwar nicht gezielt das Zuschalten erfasse, jedoch geschehe „das Starten des HbbTV-Dienstes auf vielen Geräten automatisch beim Einschalten des Senders“, und wird folglich auch von der HbbTV-Nutzungsstatistik erfasst. Eine Messung der Verweildauer findet bei RTL nach eigenen Angaben nicht statt, was sich mit unseren Beobachtungen deckt.

Beide Sendergruppen erklärten, die IP-Adressen der Nutzer lediglich in gekürzter Form weiterzugeben. RTL bezieht sich damit explizit auf die IP-Adressen-Anonymisierung von Google Analytics, bei der die IPs in Europa verkürzt werden sollen, ehe sie den Kontinent verlassen. Angesprochen auf die Cookies erklärte RTL, dass sie „auf den Geräten für maximal 24 Monate gespeichert werden, soweit das Gerät dies zulässt“. Man arbeite derzeit „an einer einheitlichen Lösung zur Abstellmöglichkeit für Cookies“. ProSiebenSat1 äußerte sich nicht zur Lebenszeit der Cookies, will aber immerhin daran arbeiten, seine Messungen ohne externe Hilfe durchzuführen. Ob die Sendergruppen ihre Vorsätze in die Tat umsetzen, werden wir zu einem späteren Zeitpunkt überprüfen.

Arte, der einzige öffentlich-rechtliche Sender mit Google Analytics beantwortete unsere Presseanfrage nicht. Zur Kenntnis genommen hat sie der Sender aber offenbar: Wenige Tage nach der Anfrage verbannte arte den Google-Dienst von seinem HbbTV-Portal.

Bild: SevenOne Media

ProSiebenSat1 gewährt potenziellen Werbekunden einen Einblick in seinen Datenfundus.

Nach Hause telefonieren

Auch bei den weiteren Smart-TV-Funktionen ist Tracking allgegenwärtig. Die Hersteller bekommen schon das Aufrufen des Smart-

TV-Menüs mit. Alle von uns analysierten Geräte pflegen einen regen Austausch mit dem Mutterschiff. Welchen Zweck die Datenpakete der Smart-TVs an die Server der Hersteller erfüllen, konnten wir oft nicht einmal nach intensiver Recherche ergründen. Man muss dem Hersteller also blind vertrauen, dass er es mit der Datensammelei nicht übertreibt.

Dieses Vertrauen dürfte bei Besitzern von LG-TVs nicht mehr sonderlich ausgeprägt sein: Geräte des Herstellers wurden Ende 2013 dabei ertappt, wie sie angeschlossene USB-Datenträger nach Mediendateien durchsuchten, um die Dateinamen an den Hersteller zu melden. Laut LG handelte es sich dabei um ein Versehen. Kurz nach unserer Anfrage veröffentlichte das Unternehmen eine neue Firmware-Version, die sich nicht mehr für die private Filmsammlung interessiert. Diese wird aber nicht automatisch installiert. Alle Geräte im Testfeld zeigen Werbung in der Smart-TV-Oberfläche an, die oftmals von den Servern externer Firmen nachgeladen wird. Panasonic blendet beim Einschalten sogar kurzzeitig Werbebanner in das laufende TV-Programm ein.

Schwachstelle HTTPS

Darüber hinaus haben wir mit den Geräten einige grundlegende Sicherheitschecks durchgeführt. Dabei erlebten wir erneut eine Überraschung: Drei der fünf Smart-TVs patzten schon bei der sicheren Datenübertragung via HTTPS. Wir konnten uns mit überschaubarem Aufwand in deren verschlüsselten Datenverkehr einklinken und fette Beute machen, darunter Zugangsdaten für Amazon (durch die Lovefilm-App) und Maxdome.

Die Modelle LG 42LN5758, Philips 65PFL9708S/12 und Samsung UE46F5370SS überprüfen nicht, ob SSL-Zertifikate von einem vertrauenswürdigen Herausgeber (CA) stammen. Wir haben den Smart-TVs selbst gemachte Zertifikate serviert, die von einer CA signiert wurden, die wir kurz zuvor ins Leben gerufen hatten. Die Testkandidaten können diese folglich gar nicht kennen und sollten ihr erst recht nicht vertrauen. Die fehlerhafte SSL-Implementierung zieht sich durch alle Anwendungsbereiche; Apps vertrauen zumeist darauf, dass die vorhandene Krypto-Infrastruktur funktioniert. Bei Philips und Samsung verlassen sich sogar die Browser darauf, weshalb wir mühelos in eine HTTPS-gesicherte Banking-Sitzung einsteigen konnten. Kurz gefasst: Wer mit diesen Geräten vertrauliche Daten verschickt, handelt leichtsinnig. Jeder, der sich zum Beispiel im gleichen Netzwerk befindet, kann die Daten im Klartext mitlesen.

LG, Philips und Samsung konnten das Sicherheitsproblem mit Hilfe der von uns zur Verfügung gestellten Informationen nachvollziehen. Der Fehler zieht sich jeweils durch die gesamte Produktpalette. Präzise Angaben darüber, welche Modelle verwundbar sind, konnte jedoch keines der Unternehmen machen. Die TV-Hersteller arbeiten nach eigenen Angaben an Firmware-Updates, die die Lücke schließen sollen.

Angriffe auf Smart-TVs sind übrigens keineswegs theoretischer Natur: Ist zum Beispiel der Router mit einem Datenschnüffel-Tool befallen, wie in c't 21/13 auf Seite 46 beschrieben, kommt der Angreifer auf diesem Weg auch an den Datenverkehr des TV. Wenn der Fernseher die ihm vorgesetzten SSL-Zertifikate nicht ausreichend überprüft, hat der kompromittierte Router den HTTPS-Traffic im Nu geknackt.

Grundsätzlich ist auch eine Infektion des TV möglich – schließlich werden die Smart-TV-Funktionen von kleinen Embedded-Rechnern bereitgestellt, in denen für gewöhnlich ein Unix-Kern werkelt. Entdeckt ein Angreifer darin Sicherheitslücken, kann er sich weitreichende Kontrolle über das System verschaffen. So gelang es dem Sicherheitsforscher SeungJin Lee bereits vor einem Jahr, einen Samsung-Fernseher in eine Videowanze zu verwandeln. Diese leitete den Video-Stream der eingebauten Kamera unbemerkt über das Netzwerk weiter – während das Gerät vermeintlich ausgeschaltet war.

```
1694 700.272958 192.168.178.187  46.137.14.197   HTTP   636 GET /?c=PRO7&seq=35&open=35&sid=431300 HTTP/1.1
1200 630.114412 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=34&open=34&sid=431300 HTTP/1.1
1071 559.978142 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=33&open=33&sid=431300 HTTP/1.1
 939 490.087151 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=32&open=32&sid=431300 HTTP/1.1
 808 420.138097 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=31&open=31&sid=431300 HTTP/1.1
 677 350.115075 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=30&open=30&sid=431300 HTTP/1.1
 555 280.018988 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=29&open=29&sid=431300 HTTP/1.1
 419 210.111771 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=28&open=28&sid=431300 HTTP/1.1
 284 140.011533 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=27&open=27&sid=431300 HTTP/1.1
 151 70.1033740 192.168.178.187  54.217.99.221   HTTP   636 GET /?c=PRO7&seq=26&open=26&sid=431300 HTTP/1.1
   5 0.01402400 192.168.178.187  54.217.138.199  HTTP   636 GET /?c=PRO7&seq=25&open=25&sid=431300 HTTP/1.1
```

Sind Sie noch da? Nach dem Einschalten der ProSiebenSat1-Sender kommuniziert der Fernseher im Minutentakt mit der Sendeanstalt.

Sendepause

Unsere Testergebnisse hinterlassen den Eindruck, dass die Themen Datenschutz und Sicherheit von den TV-Herstellern eher stiefmütterlich behandelt werden. Wer verhindern will, dass die Mattscheibe das persönliche Fernsehverhalten mit Gott und der Welt teilt, der muss HbbTV abschalten (siehe Kasten „Fernsehen ohne Zuschauer").

Wir haben unter **ct.de/hbbtv** eine Linkliste zusammengestellt, über die Sie bei Bedarf trotzdem auf die wichtigsten HbbTV-Senderportale zugreifen können. Legen Sie am besten ein Lesezeichen im Browser Ihres Smart-TV an. Damit können Sie zum Beispiel in den Mediatheken stöbern, ohne dass der Red Button Ihre Fernsehgewohnheiten verrät.

Wollen Sie dem TV das Internet gänzlich entziehen, aber weiterhin auf Dateifreigaben im heimischen Netzwerk zugreifen, können Sie die IP-Konfiguration des Geräts auf „manuell" ändern und als Gateway und DNS-Server die IP-Adresse 127.0.0.1 einstellen. Die häufig angebotene TV-Steuerung per App funktioniert dann weiterhin – etwa, wenn die Fernbedienung mal wieder in die Sofa-Ritze gerutscht ist. Falls Sie die Netzwerkfunktionen gar nicht nutzen, ziehen Sie am Besten den Netzwerkstecker und deaktivieren Sie die WLAN-Schnittstelle. (rei)

www.ct.de/1404078

Tracking-Cookie entschlüsselt

Schaltet man einen Sender ein, der HbbTV anbietet, werden oft Cookies von Google Analytics auf dem Fernseher gespeichert. Diese erkennt man an der Zeichenfolge utm, was für Urchin Tracking Module (UTM) steht. Besonders viel merkt sich dabei das Cookie utma, das nach dem folgenden Muster aufgebaut ist:

__utma=261068756.1386975058.1385751826.1389304570.1389540773.57

Eindeutige ID des HbbTV-Portals (z. B. 261068756 für Sat.1)	Zufällig generierte, dauerhafte Benutzer-ID	Zeitstempel des ersten Kontakts mit dem Portal (hier 29. 11. 2013, 20:03:46 Uhr)	Zeitstempel des Beginns der vorherigen Sitzung (hier 9. 1. 2014, 22:56:10 Uhr)	Zeitstempel des Beginns der aktuellen Sitzung (hier 12. 1. 2014, 16:32:53 Uhr)	Anzahl der bisherigen Sitzungen

HbbTV-Tracking der Sender

Sender	externer Trackingdienst	Cookies (eigene / fremde)
ARD-Gruppe[1]	–	✓ / –
arte	–[2,3]	–[3] / –
kabel eins	Google Analytics	✓ / –
n-tv	Google Analytics	✓ / –
Pro7	Google Analytics	✓ / –
RTL	Google Analytics	✓ / –
RTL 2	etracker, INFOnline	– / ✓
Sat.1	Google Analytics	✓ / –
Sixx	Google Analytics	✓ / –
VOX	Google Analytics	✓ / –
ZDF-Gruppe[1]	–	✓ / –

[1] Die Sender der Gruppe nutzen eine gemeinsame HbbTV-URL
[2] ursprünglich Google Analytics [3] nach unserer Anfrage entfernt