



## Fernsehsender analysieren SmartTV-Besitzer

Darmstadt, 15.05.2013. Informatiker der TU Darmstadt haben gezeigt, dass Sendeanstalten das Nutzerverhalten ihrer Zuschauer mit internetfähigen TV-Geräten ohne deren Wissen auswerten können. Die Forscher stellten ihre am Center for Advanced Security Research Darmstadt (CASED) entstandene Arbeit heute in Bonn beim Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik vor.

Neue Fernsehgeräte, sogenannte Smart TVs, können Fernsehen und Internet verbinden. Viele öffentliche und private Sendeanstalten bieten Zuschauern so verschiedene interaktive Zusatzfunktionen. Möglich macht das unter anderem die neue Funktion Hybrid Broadcast Broadband TV (HbbTV), die beispielsweise Informationen zum laufenden Programm oder weitere Folgen einer Sendereihe aus der Mediathek zur Verfügung stellen kann. In Deutschland werden bis 2016 voraussichtlich über ein Drittel aller Haushalte einen HbbTV-fähigen Fernseher nutzen.

### Datenübertragung startet ohne Wissen der Nutzer

Die Nutzer dieser Geräte sehen in der Regel eine eingeblendete Information, dass der Sender Zusatzinformationen anbietet. Wer interessiert ist, kann diese über eine Taste auf der Fernbedienung abrufen. „Was die Nutzer nicht wissen können ist, dass der Fernseher bereits bei der Senderwahl mit dem Server der Sendeanstalt kommuniziert. Von vielen Sendern empfängt er mehrmals pro Minute Inhalte, überträgt aber auch Nutzungsdaten, ohne dass der Zuschauer HbbTV aktiv durch Drücken des Red Buttons nutzt“, erklärt Informatiker Marco Ghiglieri. Die so gewonnenen Informationen sind aus datenschutzrechtlicher Sicht durchaus als bedenklich einzustufen – insbesondere, da einige Sender die Daten auch Drittanbietern wie Google Analytics zur Verfügung stellen, die detaillierte Nutzeranalysen erzeugen. Diese könnten Sendern vor allem zur Ermittlung von regionalen Einschaltquoten und zur Übertragung personalisierter Werbung dienen. „Nutzeranalysen sind nicht prinzipiell schlecht, wenn die Nutzer über den Zweck informiert sind und die Überwachung mit Zustimmung erfolgt“, ergänzt Ghiglieri. Derzeit hat der Nutzer nur die Wahl, Datendienste auf dem Fernseher abzuschalten, verliert aber dadurch auch alle neuen Funktionen. Eine Übersicht des Verhaltens einzelner HbbTV-Sender geben die Autoren in ihrer Veröffentlichung.

Kommunikation und Medien  
Corporate Communications

Karolinenplatz 5  
64289 Darmstadt

Ihre Ansprechpartnerin:  
Silke Paradowski  
Tel. 06151 16 - 32 29  
Fax 06151 16 - 41 28  
[paradowski.si@pvw.tu-darmstadt.de](mailto:paradowski.si@pvw.tu-darmstadt.de)

[www.tu-darmstadt.de/presse](http://www.tu-darmstadt.de/presse)  
[presse@tu-darmstadt.de](mailto:presse@tu-darmstadt.de)



„Anbieter und Hersteller müssen lernen, dass Sicherheit und Privatsphäre schon „by Design“, also im Entwurfsstadium berücksichtigt werden muss. Nachträgliche Absicherung ist oft teurer und kann das Vertrauen der Kunden erschüttern“, sagt Michael Waidner, CASED-Direktor und Professor für Sicherheit in der Informationstechnik.

### **Appell an Sender und Gerätehersteller: Datenschutz standardisieren**

Die Wissenschaftler sind mit den Sendeanstalten im Gespräch und fordern sie auf, sich mit den Geräteherstellern möglichst schnell auf einen Standard mit konkreten, technischen Datenschutzlösungen zu einigen. Eine Datenübertragung soll dann erst nach Aktivierung der HbbTV-Funktion durch den Nutzer möglich sein. In ihrer Veröffentlichung schlagen die Forscher mögliche Gegenmaßnahmen vor. Weiterhin müssen die Daten so übertragen werden, dass kein Angreifer Informationen abfangen und auswerten kann.

Wenn der Standard nicht angepasst wird, ist nicht auszuschließen, dass über zukünftige Funktionen auch kritischere Daten versehentlich oder wissentlich übermittelt werden – beispielsweise, wenn über den Fernseher auch Bezahldienste, private Bilder oder eine integrierte WebCam genutzt werden.

Die Forscher haben ihre Ergebnisse von Dezember 2012 Anfang Mai überprüft. Noch immer zeigen die Sender das gleiche Verhalten, nur die eingesetzten Trackingdienste haben sich teilweise geändert.

### **Weitere Informationen**

>> [Download der Veröffentlichung mit detaillierter Senderliste.](http://www.cased.de/files/2013_CASED_HbbTV.pdf)  
[http://www.cased.de/files/2013\\_CASED\\_HbbTV.pdf](http://www.cased.de/files/2013_CASED_HbbTV.pdf)

>> [Download des Folienvortrags vom IT-Sicherheitskongress](http://www.cased.de/files/2013_CASED_HbbTV_Vortrag.pdf)  
[http://www.cased.de/files/2013\\_CASED\\_HbbTV\\_Vortrag.pdf](http://www.cased.de/files/2013_CASED_HbbTV_Vortrag.pdf)

>> [Download Pressebild](http://www.cased.de/presse/bildarchiv.html)  
<http://www.cased.de/presse/bildarchiv.html>



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

#### Fachkontakt

Marco Ghiglieri  
Center for Advanced Security Research Darmstadt (CASED)  
Tel. +49 6151 16-75533  
[marco.ghiglieri@cased.de](mailto:marco.ghiglieri@cased.de)

#### Presse-Ansprechpartnerin

Anne Grauenhorst  
Center for Advanced Security Research Darmstadt (CASED)  
Tel. +49 6151 16-6185  
[anne.grauenhorst@cased.de](mailto:anne.grauenhorst@cased.de)

MI-Nr. 40/2013, Anne Grauenhorst