Google TV Gutachten

Prof. Dr.-Ing. Luigi Lo Iacono
Fachhochschule Köln
luigi.lo_iacono@fh-koeln.de
23. Juni 2014

Im Auftrag der
Landesanstalt für Medien NRW (LfM)
Projektinitiative NRW digital

Executive Summary

Mit Google TV liegt ein neuer Ansatz vor, wie das klassische lineare Fernsehen mit Zusatzdiensten aus dem Internet verknüpft wird. Das vorliegende Gutachten hat gezeigt, dass die Art und Weise, wie die Plattform für die Zusatzdienste und das TV-Signal gekoppelt werden, neue Frage- und Problemstellungen in Bezug auf die Einflussnahme des Sehverhaltens sowie auf den Schutz der Privatheit des Fernsehkonsumenten und den Signalschutz aufwirft. Das charakteristische Merkmal von Google TV im Vergleich zu anderen Smart-TV- und Smart-Stick-Angeboten ist in diesem Zusammenhang das Durchschleusen des linearen TV-Signals durch eine App der Plattform, um das Fernsehprogramm zu dekodieren und darzustellen. Durch diesen Ansatz bekommen Apps die Möglichkeit, das Sehverhalten und die Sehvorlieben eines Nutzers zu erfassen und diese sensitiven Informationen gezielt zu verwerten. Als Beispiel kann hier die Beeinflussung der Fernsehkonsumenten gesehen werden. Dies kann in Abhängigkeit der Ausprägung z.B. auf das Kaufverhalten oder die Programmwahl abstellen. Außerdem können Manipulationen am TV-Signal vorgenommen werden. Dies ist die vermeidlich größere Bedrohung, da hierdurch Dritte in die Übertragung eingreifen und gezielt meinungsbildende und manipulative Sichtweisen auch massenweise verbreiten könnten. Diese ist in TV-Ökosystemen - wie eines mit Google TV vorliegt - besonders bedenklich, da derartige Ökosysteme den Zugang für prinzipiell Jedermann durch das Bereitstellen von Apps ermöglichen. Abschließend muss in diesem Zusammenhang angemerkt werden, dass die dargelegten Beobachtungen zwar auf Google TV beschränkt sind, diese aber auch für dritte Anbieter von Plattformen für Internetzusatzdienste im TV gelten, sofern diese das genannte Prinzip der engen Kopplung von TV-Signal und Plattform implementieren, was zur Zeit nach besten Wissen des Gutachters ausschließlich in Google TV vorzufinden ist. Eine vergleichbare Funktionsweise lässt sich allerdings vermehrt in modernen Spielekonsolen wiederfinden, so dass diese vermeidlich auch in die Kategorie zu zählen sind.

Einen Betrachtungsschwerpunkt bei den Untersuchungen hat die Einflussnahme bei der Programmwahl durch die in der Google TV Plattform enthaltenen Apps und Dienste eingenommen. Bereits die in Google TV integrierte Google Suche greift in der Version von Google TV für den US-amerikanischen Markt auf die EPG-Daten zu und fügt passende Suchtreffer in die Ergebnisliste ein. In der Version für den deutschen Markt ist diese Funktion ausgenommen worden. Um derartige länderspezifischen Ausprägungen nachvollziehen zu können, sind im Rahmen des Gutachtens Google TV Geräte für den amerikanischen und deutschen Markt einbezogen worden. Neben der Google Suche, können die verschiedenen bereitstehenden Empfehlungssysteme die Quelle für Einflussnahmen sein. Die Empfehlungssysteme müssen allerdings vom Anwender aktiv verwendet, um daraus Empfehlungen zu beziehen. Eine Veränderung der Programmreihenfolge, die im Empfangsgerät eingespeichert ist, kann und wird von der Plattform nicht vorgenommen. Die

von Google TV selbst integrierten Empfehlungen sind in der App namens „PrimeTime“ enthalten. Diese stellt die verschiedenen verfügbaren Inhaltequellen gruppiert nach Live-TV, TV On Demand und Movies dar. In der Rubrik Live-TV sind die Programminhalte eingeordnet, die aus dem linearen Fernsehsignal empfangen werden. Die beiden anderen Rubriken werden aus Angeboten von Online-Diensten wie z.B. Netflix, HBO Go und Amazon Instant Video befüllt. Bei der Auflistung der Inhalte spielen persönliche Vorlieben eine Rolle. Die Empfehlungen werden auf den Servern von Google berechnet. Der dazu verwendete Algorithmus ist nicht bekannt und kann auf Grundlage der Beheimatung auf den Google-Servern nicht ermittelt werden. Die PrimeTime-App ist in Geräten für den deutschen Markt nicht enthalten. Weitere Empfehlungssysteme sind in den jeweiligen Apps der Inhalteanbieter enthalten und sind damit unabhängig von PrimeTime. Da die Nutzung der PrimeTime-App und auf freiwilliger Basis erfolgt und die dort durchgeführte Personalisierung sowohl eingeschaltet als auch ausgeschaltet werden kann, ergibt sich allein hieraus keine unzulässige Einflussnahme in die Auswahlsvielfalt. Dennoch unterscheiden sich die Empfehlungen in den verschiedenen Apps stark von denen aus klassischen Medien wie z.B. von Programmzeitschriften, da erstere stark individualisiert erfolgen und sich in der Folge Situationen einstellen können, in denen Empfehlungen dauerhaft auf eine kleine Menge von Quellen aus dem Algorithmus kommen, was wiederum eine begrenzte Sicht auf die Programmvielfalt zur Folge hat. Ob und in welchem Umfang derartige Szenarien auftreten können bedarf weiterführender Untersuchungen, für die u.a. Benutzerstudien durchgeführt werden müssten.

Der zweite Betrachtungsschwerpunkt der Studie lag im Datenschutz. Die hierzu durchgeführten Analysen konnten keine Verstöße zu Tage fördern. Generell ist die Datenbegehrlichkeit der verschiedenen Apps und Dienste kritisch zu betrachten. Formal gibt es keine Beanstandungen, da vor der Benutzung der Anwendungen die Zustimmung des Benutzers zur Erhebung, Speichern und Verarbeitung personenidentifizierbarer Daten eingeholt wird. Nennenswert ist jedoch, dass es dem Benutzer vor dem Kauf eines Google TV Geräts nicht ohne weiteres ermöglicht wird, sich über die Datenschutzbestimmungen zu informieren. Insbesondere auf den Produkt-Webseiten finden sich weder Hinweise noch Verlinkungen auf die geltenden Datenschutzvereinbarungen. Auch in der Geräteverpackung sind die Richtlinien nicht beigefügt. Erst während des Installationsprozesses offenbaren sich diese. Hier sind unter Umständen Verbesserungen im Verbraucherschutz denkbar. Ansonsten konnten auch die mitprotokollierten Datenkommunikationsaufzeichnungen, die im Rahmen des Gutachtens gemacht wurden, keine Zuwiderhandlung zu den Datenschutzpolicies feststellen lassen. Die Analysen wurden im Rahmen dieses Gutachtens auf unverschlüsselten HTTP-Datenverkehr beschränkt und in einem begrenzten Zeitfenster während des Gutachtens durchgeführt.

Der dritte Betrachtungsschwerpunkt hat sich dem Signalschutz zugewendet. Die zunächst theoretisch gewonnen Erkenntnisse zur Manipulation des TV-Signals durch Apps Dritter konnten in Testumgebungen praktisch nachgewiesen werden. Die dazu entwickelten Apps sind in der Lage, ferngesteuert aus dem Internet, gezielt auf bestimmte Personen oder massenweise auf alle angeschlossenen Teilnehmer, das laufende TV-Signal mit eigenen Inhalten zu überlagern. Die kann sowohl vollflächig auf das gesamte Bild einschließlich des

Tons erfolgen als auch eine Teilfläche des Bilds begrenzt sein, um z.B. ein Banner einzublenden. Die beschriebenen Angriffstypen sind in dieser Form, wobei insbesondere die praktische Durchführbarkeit in einem konkreten System hierbei hervorzuheben ist, noch nicht publiziert wurden. Entsprechende Veröffentlichungen in einschlägigen Fachorganen werden im Nachgang zu diesem Gutachten in enger Abstimmung mit der Projektinitiative NRW digital der Landesanstalt für Medien NRW angefertigt und publiziert.

Inhaltsverzeichnis

1. Einleitung

Google TV (im Folgenden auch kurz GTV genannt) [1] ist eine Software-Plattform von Google, die traditionelle lineare Fernsehinhalte mit Internetinhalten und Apps verbindet und diese auf den Bildschirm ins Wohnzimmer bringt. Auf Basis des Google-Betriebssystems Android und dem darum etablierten Ökosystem mit einer Vielzahl von Apps und Services geht Google TV damit weiter als Smart-TV-Angebote. Um die Unterschiede zwischen den auf dem Markt verfügbare Produkte besser einordnen zu können, kann die in Abbildung 1 im Rahmen dieses Gutachten erstellte Klassifikation herangezogen werden. Es stellt sich in diesem Kontext zu Beginn die Frage, in wie weit sich Google TV von anderen Smart-TV-Angeboten unterscheidet und wie sich eine gesonderte Untersuchung dazu rechtfertigt.

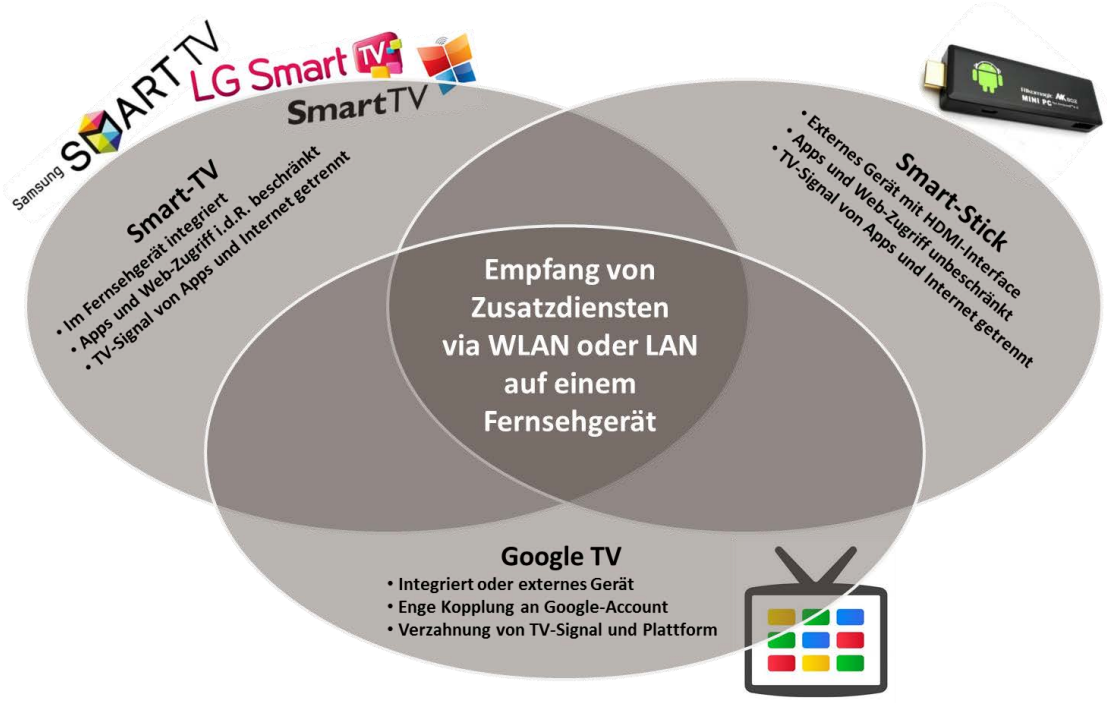


Abbildung 1: Eingrenzung und Abgrenzung verfügbarer TV-Zusatzdienste

Abbildung 1 verdeutlich, dass alle verfügbaren Ansätze und Technologien im Kern den Empfang von Zusatzdiensten auf einem Fernsehgerät über einen haushaltsüblichen Internetzugang zum Ziel haben. In der **Kategorie Smart-TVs** sind die Geräte eingeordnet, die den Internetzugang bereits als integralen Bestandteil beinhalten. Geräte, die sich dieser

Gruppe zuordnen lassen, können ohne weiteres an das Internet angeschlossen werden und bringen vom Hersteller vorinstallierte Anwendungen mit. Die bereitgestellten Zusatzdienste werden durch die mitgelieferten Anwendungen definiert und variieren von Gerätehersteller zu Gerätehersteller bzw. sogar von Modell zu Modell eines Herstellers stark. Als gemeinsamer Nenner lässt sich neben der tiefen Integration in das Fernsehgerät zudem festhalten, dass die Zusatzdienste technisch meist über Web-Standards bereitgestellt werden und eine strikte Trennung vom eigentlichen TV-Signal vorliegt. In Bezug auf Sicherheitsfragestellungen heißt das, dass ein Smart-TV ein vergleichbares Gefährdungspotential wie andere Geräte mit Webzugang aufweist, wie dies z.B. für das webbasierte HbbTV nachgewiesen wurde [2]. Im Gegensatz zu klassischem Fernsehen sind Smart-TVs in der Lage über verschiedene Mechanismen (IP, Cookies, Dienstezugänge usw.) den jeweiligen Rezipienten zu erkennen.

Die **Kategorie Smart-Stick** ist der Smart-TV-Kategorie sehr ähnlich. Die von der Form an einen Bauklotz erinnernde Hardware beinhaltet die technischen Komponenten, die einen Smart-TV direkt zum Empfang von internetbasierenden Zusatzdiensten befähigen. Angeboten werden die Smart-Sticks für Fernseher, die keine Smart-TV-Funktionalität beinhalten, über die man aber gerne dennoch in den Genuss von internetgehosteten Zusatzdiensten kommen will. Über eine HDMI-Schnittstelle lässt sich ein Fernseher mittels eines Smart-Sticks zu einem Smart-TV erweitern. Da die Hersteller von Smart-Sticks sich von Fernsehgeräte-Herstellern unterscheiden, sind die Smart-Sticks durch das zugrunde liegende Betriebssystem und die bereitgestellten Anwendungen häufig unbeschränkter im Zugriff auf das Web. Neben diesen Unterschieden, ist auch bei den Smart-Sticks das TV-Signal strikt von den Internet-Zusatzdiensten getrennt.

Google Chromecast

Der HDMI-Stick von Google mit dem Namen „Chromecast“ gehört in die Smart-Stick-Kategorie. Seit März 2014 kann man den Smart-Stick von Google auch in Deutschland für einen empfohlenen Kaufpreis von 35,00 Euro erwerben. Als Betriebssystem gibt Google eine angepasste Version von Chrome OS an, dem Cloud-Betriebssystem auf Basis des Chrome-Browser, das hauptsächlich auf speziellen Notebooks, den sogenannten Chromebooks, installiert ist. Die initiale Konfiguration erfolgt nicht wie bei vielen der Smart-Stick-Mitstreiter via kabellose Tastatur, sondern über die Chromecast-App. Diese ist für Android- und iOS-Geräte frei-verfügbar. Mit der Chromecast-App lässt sich der Chromecast-Stick dann mit dem heimischen WLAN verbinden. Die Steuerung kann dann über Smartphone, Tablet oder PC erfolgen. Der PC wird mittels einer Erweiterung für den Chrome-Browser zur Steuerung des Sticks. Chromecast verhält sich als passives Medienwiedergabegerät, d.h. es lassen sich keine zusätzlichen Apps installieren. Hiermit ist Chromecast eingeschränkter als viele andere Smart-Sticks – insbesondere wenn diese auf dem Android-Betriebssystems beruhen –, die die freie Installation von Apps ermöglichen. Softwareupdates für Chromecast werden hingegen ohne Ankündigung oder Bewilligung durch den Benutzer heruntergeladen und installiert. Die vorinstallierten Anwendungen werden über die Steuerung mit Inhalten versorgt (via URL), die dann vom Stick entweder aus dem lokalen Netz oder dem Internet zugegriffen und wiedergegeben werden. Viele der Zusatzdienste, die Chromecast in den USA

so erfolgreich gemacht hat, sind in der Version für den deutschen Markt nicht enthalten. Darunter fallen z.B. Pandora, Netflix und Hulu. Diese wurden durch die zwei nationalen Dienstangebote Maxdome und Watchever ersetzt. Die Integration dieser Dienste geht so weit, dass die Apps für Android und iOS von Maxdome und Watchever das Streaming von Medieninhalten aus den genannten Apps zum Chromecast-Stick bereits eingebaut haben. Mit Google Music, Google Video und YouTube sind natürlich auch die Google eigenen Dienste verfügbar. Entwicklern stellt Google seit dem 3. Februar 2014 ein Software Development Kit (SDK) für Android-, iOS- und Web-Apps bereit. Mit dem SDK lassen sich Anwendungen mit einer Casting-Funktion ausstatten, die Inhalte an den Chromecast ausliefert. Neue Anwendungen kommen fast täglich hinzu. Einen Überblick über Chromecast-Apps kann man sich über die kostenlose Cast-Store-App verschaffen.

Google TV[1] ist den beiden vorgenannten Kategorien sehr ähnlich. Technische Ausprägungen liegen in Form von Set-Top-Boxen, Blu-Ray-Playern und Fernsehgeräten vor (siehe Abbildung 2). Damit gibt es Google TV Geräte in den Formfaktoren beider vorgenannter Kategorien.

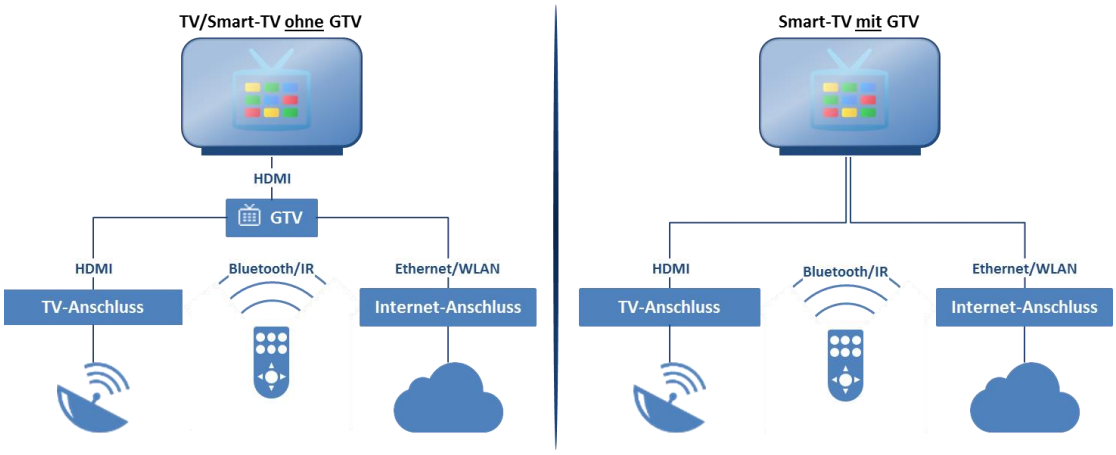


Abbildung 2: Anschlussmöglichkeiten von Google TV Geräten

In Bezug auf Beschränkungen und Vorselektion von Anwendungen und Inhalten ist Google TV so offen wie es für die Kategorie der Smart-Sticks der Fall ist. Besonders und neu an Google TV ist, wodurch es auch in der vorliegenden Klassifizierung einer eigenen Kategorie

[1] Im Rahmen dieses Gutachtens ist die vorliegende Kategorisierung als Grundlage der Arbeiten entwickelt worden. Da es zur Zeit der Erstellung keine weiteren Angebote gab, die in diese Kategorie einzuordnen gewesen wären, hat sich die Benamung an dem einzigen Vertreter dieser Kategorie ausgerichtet: Google TV. An dieser Stelle wird daher explizit darauf hingewiesen, dass es zukünftig durchaus andere Plattformen geben kann, die sich dieser Kategorie zuordnen lassen und das sich dann der Kategoriename an diese Gegebenheiten anpassen muss. Für das bessere Verständnis und die Lesbarkeit des Gutachtens wird im Rahmen des vorliegenden Dokuments die eingeführte Benamung beibehalten.

bedarf, ist die Tatsache, dass das TV-Signal in die Plattform eingespeist wird, bevor es zur Darstellung auf dem Bildschirm kommt. Genauer gesagt erfolgt die Darstellung des linearen Programms durch eine spezielle App, die in Google TV den Name „Live TV“ trägt. Somit ist diese Kategorie insbesondere dadurch charakterisiert, dass es keine strikte Trennung zwischen dem TV-Signal und den Zusatzdiensten gibt, so wie es in den beiden anderen Kategorien vorliegt. Durch das Fehlen einer strikten Trennung von TV-Signal und TV-Plattform ergibt sich eine ganze Reihe von neuen Gefährdungspotenzialen, die theoretisch das Ausspähen und Manipulieren des TV-Signals einzelner bis hin zur Gesamtheit aller angeschlossener Nutzer ermöglicht. Dies ist besonders brisant, da auf dieser Basis schwerwiegendere Gefährdungen eintreten können als bei den beiden anderen Kategorien, die zudem aus einer zusätzlichen Quelle stammen können, nämlich von App-Anbietern. Neben diesen genannten Spezifika ist weiterhin die Besonderheit der aggregierten Dienstzugänge zu berücksichtigen. Da Dienstzugänge im Google-Universum durch den Google-Account abgebildet werden, ist es Google und Dritten daher theoretisch sehr leicht möglich, anhand des Nutzungsverhaltens detaillierte Nutzerprofile erstellen und diese mit Daten der eigenen Dienste verknüpfen aber auch anderer Dienste in Beziehung setzen zu können.

2. Zielsetzung

Das Gutachten soll untersuchen und darstellen, in welchem Umfang die in der Einleitung dargelegten Manipulationen und Gefährdungen durch die Google TV Umgebung technisch auch tatsächlich möglich ist.

Von besonderem Interesse ist dabei die Frage, ob und in welchen Ausprägungen sich das Gesamtangebot und die technischen Algorithmen der US-amerikanischen Version der Box von der auf dem deutschen Markt befindlichen unterscheiden. Ist die amerikanische Version der deutschen bereits im Wesentlichen technisch inhärent und sind bestimmte Spezifikationen lediglich nicht aktiviert?

Für die Medienaufsicht ist die Fragestellung des Gutachtens besonders relevant hinsichtlich eines Datenschutzaspektes - Erhebung und die weitere Verarbeitung personenbezogener Nutzerdaten durch Google TV - und eines Vielfaltsaspektes - Beeinflussung des Nutzungsverhaltens aufgrund von Voreinstellungen bzw. Nutzerprofilen durch die personalisierte Angebotsgestaltung durch Google TV.

(1) Datenschutzaspekt: Verarbeitung von personenbezogenen Daten

Innerhalb des Google TV-Angebots werden personenbezogene Daten von Nutzern für unterschiedliche Zwecke von verschiedenen Stellen erhoben und gespeichert, so z.B. für die jeweiligen Einstellungen in Bezug auf die individuelle Nutzung. Aber auch andere Verwendungsmöglichkeiten bestehen bzw. sind hier denkbar.

Im Rahmen des geplanten Gutachtens soll untersucht und detailliert aufgeführt werden, welche personenbezogenen Daten bzw. welche potentiell personenbeziehbaren Daten im Verlauf des gesamten Nutzungsprozesses unter Ausnutzung des gesamten Anwendungs-Portfolios ermittelt und gespeichert werden - in welcher Form, mit welchem Ziel und für welche Dauer. Hier soll auch die Nutzererkennung aufgrund von akustischen Merkmalen miteinbezogen werden.

Gegebenenfalls sollten die Ergebnisse mit den allgemeinen Nutzungsbedingungen des Angebots abgeglichen werden. Interessant ist dabei auch die Frage, ob und in welcher Form der Nutzer auf die jeweilige Erhebung und Verarbeitung seiner personenbezogenen Daten hingewiesen wird und ob er Gelegenheit erhält, in die jeweiligen Nutzungszwecke aufgeklärt einzuwilligen sowie eine Löschung der erhobenen Daten zu veranlassen und wie dies wiederum transparent gemacht wird.

(2) Vielfaltsaspekt: Erstellung personalisierter Fernseh- und Videoangebote durch Google TV anhand von Nutzerdaten

In einem zweiten Teil des Gutachtens soll ermittelt und beschrieben werden, welche Voreinstellungen ohne Einbeziehung der Nutzerdaten vorhanden sind, die die Auswahl und Anordnung von Fernseh- und Videoangeboten bestimmen. Daneben sollen die Veränderungen dieser Voreinstellungen aufgrund der jeweiligen persönlichen Nutzung des Angebots untersucht werden. In diesem Zusammenhang sollen erstens Voreinstellungen und Navigationsmechanismen von Google TV umfassend beschrieben und zweitens Fragestellungen und Problemstellungen in Bezug auf mögliche Einschränkungen der Vielfalt, des diskriminierungsfreien Zugangs und der Navigation abgeleitet werden.

Hier erscheint u.a. ein Vergleich des Google TV-Angebots in Deutschland und in den USA lohnenswert, da etwa EPGs (Electronic Program Guides) im deutschen Angebot nicht enthalten sind, diese in den USA jedoch teilweise sogar Navigationsfunktionen übernehmen, was wiederum Auswirkungen auf das individuelle Nutzungsverhalten haben könnte.

(3) Signalschutz: Manipulative Eingriffe in das ausgestrahlte Signal des linearen Fernsehens

Ein dritter Teil des Gutachtens soll untersuchen, welche prinzipiellen und technischen Möglichkeiten zur Manipulation des TV-Signals sich aus der engen Kopplung von TV-Signal und Internet-Zugang ergeben. Diesem Aspekt wird ein hohes Gewicht zugeordnet, da es sich bei Google TV zudem um ein TV-Ökosystem handelt, dass es einer Vielzahl von Systemteilnehmern ermöglicht, mit Ihren Apps Zugriff auf die Google TV Umgebung zu erlangen. Auf Basis von eigenentwickelten Apps soll untersucht werden, ob und wenn, dann in welchem Umfang sich die Wiedergabe des linearen TV-Signals durch Dritte über das Internet manipulieren lässt und damit die aktuell hohe Vertrauenswürdigkeit dieser Signalübertragung ins Wanken bringen kann.

3. Methodik

Um die gesetzten Ziele zu erreichen, ist für das vorliegende Gutachten die im Folgenden dargelegte Vorgehensweise entwickelt worden, die verschiedene, sukzessive aufeinander aufbauende Analysen zur Beobachtung und Ermittlung der Gegebenheiten vorsieht. Diesen Analysen wurden vier verschiedene Google TV Boxen unterzogen, um Gemeinsamkeiten und Unterschiede insbesondere in Geräten für den US-amerikanischen und den deutschen Markt feststellen zu können. Bei den untersuchten GTV-Boxen handelte es sich konkret um die folgenden Geräte:

- Hisense Pulse (US)
- Sony NSZ-GS7 (US)
- VIZIO Co-Star (US)
- Sony NSZ-GS7 (DE)

Die genauen Spezifikationen dieser Geräte sind im Anhang A aufgeführt.

Die Vorgehensweise sieht als ersten Schritt die Analyse des initialen Zustands der GTV-Box vor. Hierbei soll die installierte Software protokolliert werden. Interessante Merkmale stellen dabei die enthaltenen Softwarekomponenten, Versionsnummern, Zugriffsberechtigungen, Datenschutzerläuterungen und Standardeinstellungen dar. Wie dies genau erfasst wurde, ist in den nachfolgenden Kapiteln 3.1 und 3.2 beschrieben. Anschließende Untersuchungen fokussierten auf den Betrieb einer GTV-Box und analysierten den aus- und eingehenden Datenverkehr (siehe Kapitel 3.3) sowie die Möglichkeiten, die installierte Apps auf einer GTV-Box haben (siehe Kapitel 3.4).

Eine vollständige und umfassende Analyse ist nur möglich, wenn die GTV-Box in einen Zustand versetzt wird, in dem man von außen alle Zugriffsberechtigungen auf dem System erlangt. Dies wird auch als „rooten“ bezeichnet und meint den Eingriff in das System, um sich mit Administrationsrechten (im englischen wird der Administrator häufig auch als der root-Benutzer tituliert) zu versehen. Ein derartiger Systemeingriff ist für den Rahmen dieses Gutachtens ausgeklammert worden, da es zum Bearbeiten der Zielsetzung nicht zwingend erforderlich ist. Für ggf. anschließende und tiefergehende Untersuchungen sollte das Rooten von Testgeräten erneut in Betracht gezogen werden.

3.1 Initialer Zustand

Mittels des in Abbildung 3 dargestellten Analyseaufbaus ist der initiale Zustand der Google TV Testgeräte ermittelt worden. Bemerkenswert bei diesem Aufbau ist, dass das Gerät weder über eine Verbindung zum linearen TV-Signal noch zum Internet verfügt. Letztgenannter Punkt ist besonders hervorzuheben, da somit verhindert wird, dass das

Gerät bereits beim ersten Einschalten während der Initialisierungsprozedur Software aus dem Internet bezieht und installiert bzw. bestehende Programme aktualisiert. Auf diese Weise kann erhoben werden,

- was zur Inbetriebnahme erforderlich ist,
- wie die Systemumgebung standardmäßig konfiguriert ist und
- welche Anwendungen in welcher Version bereitstehen.

Die auf diese Weise ermittelten Urzustände der vier Testgeräte ist auf besondere Weise dokumentiert worden. Durch das Mitschneiden des HDMI-Signals sind angefangen vom Initialisierungsprozess bis zum manuellen Inspizieren der vorinstallierten Apps, ihrer rechtlichen Erläuterungen, den Standardeinstellungen und den Zugriffsrechten als Videos aufgezeichnet worden. Die Methode zum Aufzeichnen dieser Videos ist sehr besonders, da es sich beim HDMI-Signal um eine verschlüsselte Datenübertragung handelt. Daher wurde das digitale HDMI-Signal mit einer spezieller Hardware in ein analoges Signal umgewandelt und anschließend dieses zur Abspeicherung in ein digitales Signal transformiert. Durch diese Konvertierungskette kommt es zu Qualitätsverschlechterung, andererseits erlaubt dieser Ansatz bereits die Initialisierungsphase aufzuzeichnen. Die Videos sind in der Materialsammlung zusammengestellt. Im Anhang B ist der Inhalt der Materialsammlung angegeben.

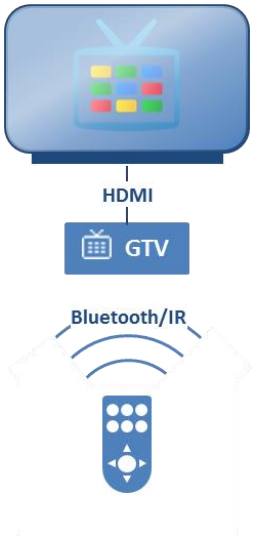


Abbildung 3: Analyse des initialen Zustands eines Google TV Geräts

Da nicht alle Bestandteile der GTV-Box auf die in Abbildung 3 angegebene Analyseform ermittelt werden können, ist eine weitere entwickelt worden, die den Zugriff aus das Dateisystem der GTV-Box erlaubt (siehe Abbildung 4).

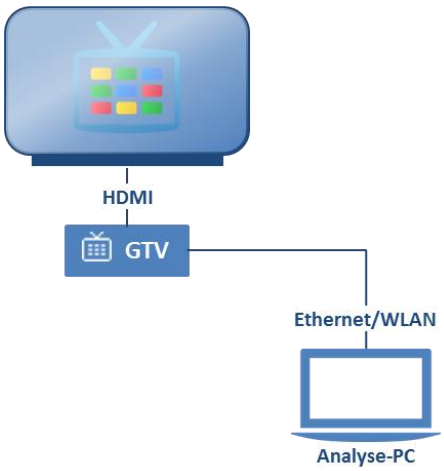


Abbildung 4: Analyse des initialen Zustands eines Google TV Geräts auf Ebene des Dateisystems

Über eine der bereitgestellten Netzwerkschnittstelle (in der Regel kabelgebundenes und drahtloses Ethernet) kann von einem verbundenen PC unter Verwendung der Android Debug Bridge (ADB) [3] Software, die von Google für die Entwicklung von Android-Apps bereitgestellt wird, auf das Dateisystem der GTV-Box zugegriffen werden. Durch entsprechend eingestellte Kommandozeilenparameter können die Ordner rekursiv durchlaufen werden. Bei diesem Durchlauf können die Datei und Ordner, auf die zugegriffen werden darf, auf den Analyse-PC kopiert werden. Die auf diese Weise auf den Analyse-PC vorliegenden Programme und Konfigurationsdateien können auf Gemeinsamkeiten und Unterschiede hin überprüft werden. Software-Komponenten und Apps, die unter der gleichen Versionsnummer auf verschiedenen Geräten vorliegen können somit zum Beispiel durch ein Fingerprinting mittels kryptographischer Hashfunktionen auf die Übereinstimmung der Programmcodes hin überprüft werden. Diese Methode kann unter anderem verwendet werden, um auf das Vorhandensein von Funktionen zu schließen, wie beispielsweise der EPG-Analysefunktion in der GTV-Box für den deutschen Markt.

3.2 Analyse der installierten Apps

In diesem Evaluierungsschritt ist auf Basis der in vorangegangenem Kapitel erläuterten Messaufbauten die installierten Apps untersucht worden. Hierbei ist sukzessive jede App mit denen in den Einstellungen dazu verfügbaren Informationen protokolliert. Auf diese Weise kann erhoben werden,

- wie die Apps standardmäßig konfiguriert sind und
- was diese für Zugriffsrechte innehaben.

Auch in dieser Analysephase sind die Erhebungen durch Video-Aufzeichnungen dokumentiert worden, die sich in der Materialsammlung befinden(siehe Anhang B).

3.3 Analyse der Netzwerkkommunikation

Um festzustellen, ob sich die Apps an die Datenschutzerläuterungen halten und nicht mehr Daten sammeln und kommunizieren als in den Regelwerken angegeben, ist die Datenkommunikation mitgeschnitten worden. Um dies zu bewerkstelligen ist der in Abbildung 5 dargestellte Aufbau implementiert worden. Ein Analyse-PC wird zwischen die GTV-Box und den Internet-Router geschaltet. Der gesamte Datenverkehr von und zur GTV-Box geht somit durch den Analyse-PC. Mit spezieller Kommunikationsmonitoringsoftware können die Datenpakete aufgezeichnet und ausgewertet werden.

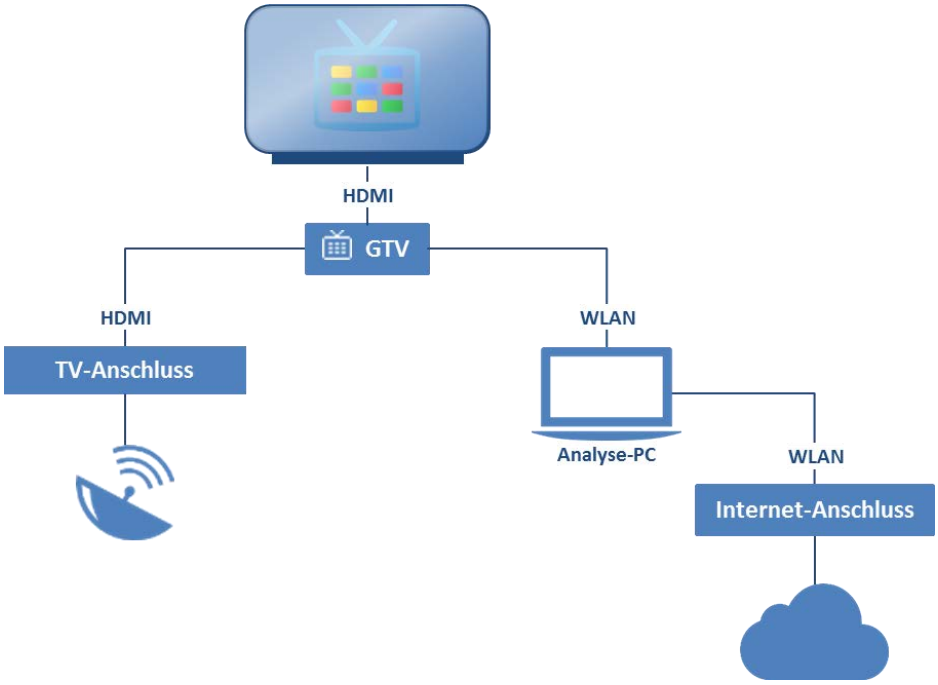


Abbildung 5: Analyse der Netzwerkkommunikation

Als Analyse-PC kam eine spezialisierte Hardware zum Einsatz, die für derartige Kommunikationsanalysen konzipiert ist. Die Protokollierung der Datenpakete erfolgte mit den Werkzeugen tcpdump [4] und Wireshark [5]. Da beide Tools mit dem pcap-Format das gleiche Austauschdatenformat verwenden, lassen sie sich auch kombinieren. Wireshark eignet sich zudem zur Analyse der aufgezeichneten Datenströme durch einen mächtigen Filtermechanismus. Die Auswertung der aufgezeichneten Datenkommunikation beschränkte sich für dieses Gutachten auf unverschlüsselte HTTP-Nachrichten. Die aufgezeichneten Daten liegen im pcap-Format in der Materialsammlung bereit.

Neben der beschriebenen Protokollierung ist zudem Untersucht worden, was für Dienste auf der GTV-Box ausgeführt werden und auf Anfragen aus dem Internet warten. Hierfür ist das Programm nmap [6] verwendet worden. Die Ergebnisse der sogenannten Portscans sind in Form von Screenshots des Resultate-Fensters von nmap festgehalten worden (siehe Materialsammlung bzw. Anhang B).

3.4 Analyse der Möglichkeiten Apps Dritter

Als letzte Testumgebung ist die Sicht des App-Anbieters eingenommen worden. Ziel dieser Analyse ist es festzustellen, was Anbieter von Apps mit ihren Apps im Sinne der Zielsetzung dieses Gutachtens für Möglichkeiten des Zugriffs und der Erhebung sowie der Verarbeitung und Speicherung von personenbezogener bzw. personenbeziehbarer Daten haben und wie diese auf Programmvielfaltsaspekte Einfluss nehmen können. Für diese Analysen ist das in Abbildung 6 dargestellte Analyseumgebung implementiert worden.

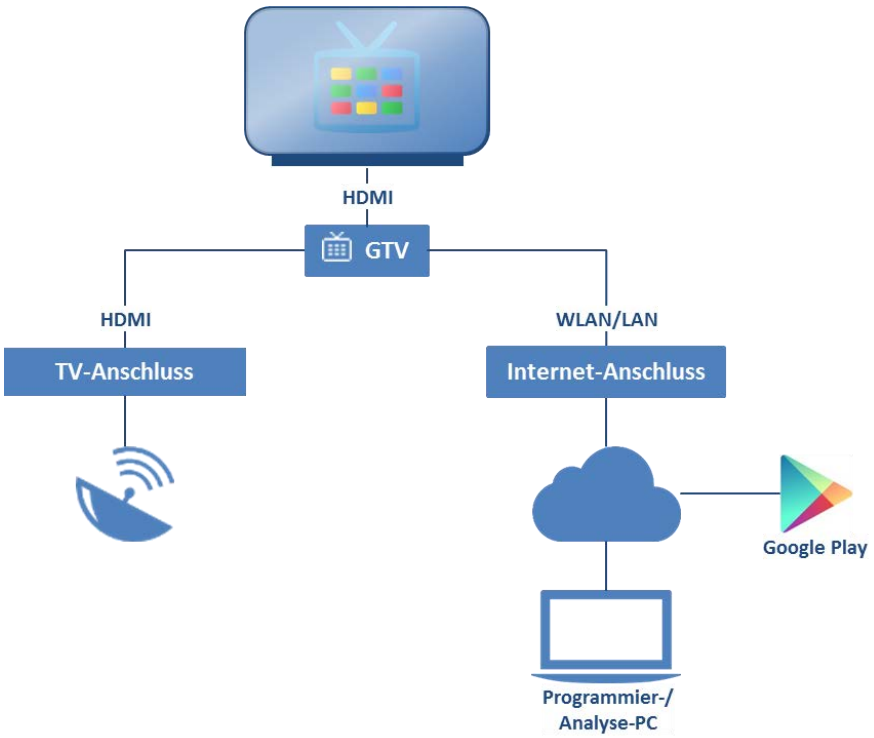
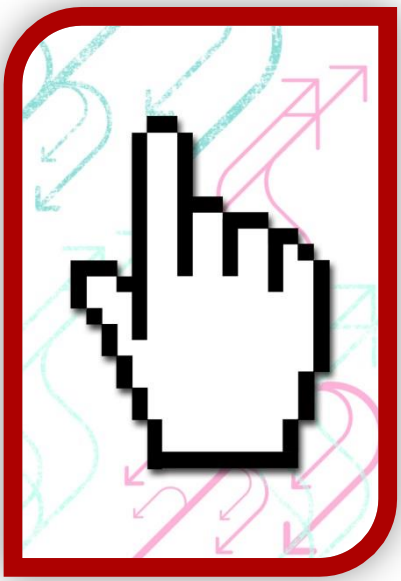


Abbildung 6: Analyse der Möglichkeiten durch Apps bereitgestellt durch Dritte über einen App-Marktplatz

Durch das Entwickeln einer eigener App für Google TV, die über den Google Play Marketplace bereitgestellt wird, sollen die aufgezählten Untersuchungsgegenstände nachvollzogen und analysiert werden. Da es sich bei Google TV um eine herkömmliche Android-Umgebung handelt, die mit speziellen Apps auf die Darstellung von Videoinhalten auf großformatigen Displays abzielt, sind in diesem Umfeld die gleichen Bedrohungen in Bezug auf Datenschutz zu erwarten, wie diese bereits im z.B. Smartphone-Bereich veröffentlicht und bekannt geworden sind. Vom besonderen Interesse sind daher spezifische Gefährdungen, die mit der Anwendung von Android/GTV in der Fernseh-Domäne einhergehen. In diesem Kontext sind erstaunliche Ergebnisse erzielt worden, die einen neuen Angriffsvektor aufzeigen, dem Benutzer von GTV ausgesetzt sind. Dieser wird detailliert in Kapitel 4.3 beschrieben.

4. Analyseergebnisse



Die auf Grundlage der beschriebenen Analyseumgebungen gewonnen Erkenntnisse werden in den folgenden Unterkapiteln aufgezeigt und diskutiert. Die Struktur orientiert sich dabei an den für das Gutachten maßgeblichen Fragestellungen: dem Datenschutz und dem Vielfaltsaspekt. Im Rahmen der Untersuchungen ist eine zusätzliche Gegebenheit aufgefallen, deren Bedeutung als imminent wichtig eingestuft wird und daher als gesonderter Punkt zur Sprache kommt: dem Signalschutz.

4.1 Datenschutz

In Bezug auf Datenschutz ist zu Beginn der Untersuchungen aufgefallen, dass sich ein Benutzer vor dem Kauf eines GTV-Geräts nicht oder nur durch sehr hohen Aufwand und dann aber auch nur lückenhaft über die damit verknüpften Datenschutzrichtlinien informieren kann. Erst nachdem ein Gerät erstanden wurde und dieses konfiguriert wird, werden die Datenschutzvereinbarungen angezeigt und zur Annahme dieser aufgefordert. In der Verpackung liegen diese ebenfalls nicht bei, so dass es zur initialen Installation kommen muss, bevor man darüber in Kenntnis gesetzt wird, wie mit den eigenen Daten umgegangen wird. Dies erscheint aus mehreren Gründen als besonders unglücklich, da die Kaufentscheidung immer stärker von derartigen Faktoren abhängig gemacht wird, dem Benutzer hier aber bei weitem nicht frühzeitig genug die dafür notwendige Information zugänglich gemacht wird. Auch auf der Produkt-Website waren keine Anhaltspunkte in Sachen Datenschutzrichtlinien von Google TV zu finden. Noch unverständlicher wird dieser Sachverhalt, wenn deutlich wird, dass die Datenschutzrichtlinien im Web unter einer öffentlich zugänglichen Adresse abrufbar sind. Diese Verlinkung mittels einer URL ist während des Konfigurationsprozesses ersichtlich geworden. Warum diese nicht auch auf den Produkt-Webseiten verlinkt sind, bleibt fraglich.

Jedes der getesteten Geräte fragte die Zustimmung einiger Richtlinien von Google Diensten und Programmen ab sowie einer herstellerspezifischen Richtlinie. Zu den von Google einverlangten Zustimmungen gehören die folgenden Richtlinien:

- Google Universal Terms of Service
  - EN: https://www.google.com/intl/en/policies/terms/
  - DE: https://www.google.com/intl/de/policies/terms/
- Google Universal Privacy Policy
  - EN: https://www.google.com/intl/en/policies/privacy/
  - DE: https://www.google.com/intl/de/policies/privacy/
- Additional Terms of Service of Google TV Devices
  - http://www.google.com/tv/termsofservice.html

- Diese Richtlinie kann über „Google TV Help“-Website gefunden werden https://support.google.com/googletv/answer/2739586?hl=en&ref_topic=2880325

Nur aus den Geräten gingen die folgenden URLs hervor:

- Google Legal Information
  - http://www.google.com/tv/legal.html
- Additional information about privacy and the Google TV Platform
  - https://support.google.com/googletv/answer/2393412
- Chrome Terms of Service
  - https://www.google.com/intl/en/chrome/browser/privacy/eula_text.html

Vergleichbar undurchsichtig stellt sich die Situation bei den vorinstallierten Apps dar. Diese variieren sehr stark zwischen den jeweiligen Geräte-Herstellern. Die Datenschutzerklärungen der vorinstallierten Apps müssen in der Regel gesondert aus den Systemeinstellungen herausgesucht und geprüft werden. Stimmt man mit diesen nicht überein, bleibt einem die Wahl zwischen der schlichten Nicht-Benutzung bzw. Deinstallation der betreffenden App. Von der Verfahrensweise wäre hier vorzuziehen, dass vorinstallierte Apps erst dann ihren Dienst aufnehmen, wenn diese bei der ersten Verwendung durch den Benutzer die jeweiligen Richtlinien zum Datenschutz anzeigen und erst auf die Einwilligung warten.

Aus Datenschutzsicht bedenklich ist die Datenaggregationsfunktion, in die sich Google mit Google TV bringt. GTV-Geräte lassen die Verwendung der Zusatzdienste nur dann zu, wenn während der Konfiguration ein Google-Account angegeben wird oder man sich entsprechend bei Google registriert und damit einen Google-Account erzeugt. Damit erweitert Google die Sicht auf seine Benutzer weiter und fügt dieser Daten in Bezug auf das Sehverhalten im TV hinzu. Eines der Ziele ist dabei, den Benutzern immer genauere und auf die jeweiligen Vorlieben und Bedürfnisse zugeschnittene Informationen und Werbung zuzustellen.

Allgemein konnte festgestellt werden, dass viele der Zusatzfunktionen, die entweder einen höheren Komfort für den Benutzer bedeuten wie z.B. eine Datensicherung in der Google-Cloud oder das Synchronisieren von Inhalten auf verschiedene Android-Geräte über den Google-Account oder auch Dienste zur Qualitätssteigerung standardmäßig ausgeschaltet sind. Aus Sicht des Datenschutzes ist das positiv zu werten, da eine explizite Einwilligung des Benutzers eingefordert wird, bevor die genannten Funktionen aktiviert werden (Opt-in).

4.2 Vielfaltsaspekt

Die Einflussnahme bei der Programmwahl durch die in der Google TV Plattform enthaltenen Apps und Dienste ist Gegenstand dieser Untersuchungen. Die in Google TV integrierte Google Suche greift in der Version von Google TV für den US-amerikanischen Markt auf die Daten des Electronic Program Guide (EPG) zu und fügt passende Suchtreffer in die Ergebnisliste zwischen den Ergebnissen einer Websuche und der Suche in den lokal vorgehaltenen Medien ein. In der Version für den deutschen Markt ist diese Funktion ausgenommen worden. Durch entsprechende Tests auf Basis der verfügbaren Testgeräte

konnte diese funktionale Einschränkung des Geräts für den deutschen Markt nachvollzogen werden.

Neben der Google Suche, können die verschiedenen bereitstehenden Empfehlungssysteme die Quelle für Einflussnahmen sein. Die Empfehlungssysteme müssen allerdings vom Anwender aktiv verwendet, um daraus Empfehlungen zu beziehen. Eine Veränderung der Programmreihenfolge, die im Empfangsgerät eingespeichert ist, kann und wird von der Plattform nicht vorgenommen. Das von Google selbst in Google TV integrierte Empfehlungssystem steht dem Anwender in Form der App namens „PrimeTime“ bereit. PrimeTime stellt die verschiedenen verfügbaren Inhaltequellen gruppiert nach Live-TV, TV On Demand und Movies dar. In der Rubrik Live-TV sind die Programminhalte eingeordnet, die aus dem linearen Fernsehsignal empfangen werden. Die beiden anderen Rubriken werden aus Angeboten der eingebundenen Online-Diensten wie z.B. Netflix, HBO Go und Amazon Instant Video befüllt. Bei der Auflistung der Inhalte spielen persönliche Vorlieben eine Rolle. Die Empfehlungen werden auf den Servern von Google berechnet. Der dazu verwendete Algorithmus ist nicht bekannt und kann auf Grundlage der Beheimatung auf den Google-Servern nicht ermittelt werden. Die PrimeTime-App ist in Geräten für den deutschen Markt nicht enthalten. Auch dies konnte auf Basis der verfügbaren Testgeräte nachvollzogen werden.

Weitere Empfehlungssysteme sind in den jeweiligen Apps der Inhalteanbieter enthalten und sind damit unabhängig von PrimeTime. Da die Nutzung der PrimeTime-App auf freiwilliger Basis erfolgt und die dort durchgeführte Personalisierung sowohl eingeschaltet als auch ausgeschaltet werden kann, ergibt sich allein hieraus keine erkennbar unzulässige Einflussnahme in die Auswahlvielfalt. Dennoch unterscheiden sich die Empfehlungen in den verschiedenen Apps stark von denen aus klassischen Medien wie z.B. von Programmzeitschriften, da erstere stark individualisiert erfolgen und sich in der Folge Situationen einstellen können, in denen Empfehlungen dauerhaft auf eine kleine Menge von Quellen aus dem Algorithmus kommen, was wiederum eine begrenzte Sicht auf die Programmvielfalt zur Folge hat.

Um die länderspezifischen Ausprägungen tiefergehend nachvollziehen zu können, sind die im Rahmen des Gutachtens bereitstehenden Google TV Geräte für den amerikanischen und deutschen Markt und insbesondere die darauf installierte Software verglichen worden. Dazu sind über die Netzwerkschnittstelle unter Verwendung eines speziellen Debugging-Programms, das Bestandteil des Android-SDK ist, die installierten Programme auf einen Analyse-PC kopiert worden. Für ausgewählte Apps ist der kryptographische Hashwert berechnet worden. Nur wenn zwei Apps über genau den gleichen ausführbaren Code verfügen, stimmt auch ihr Hashwert überein. Hierdurch kann nachvollzogen werden, ob Apps die von unterschiedlichen Geräten stammen, identisch sind. Im Rahmen dieser Untersuchung stammt im Vordergrund, ob eine der betrachteten Apps aus der deutschen Version mit der entsprechenden Apps aus den US-amerikanischen Geräten übereinstimmt. Es wurde auf die Apps abgestellt, die durch den Dateinamen einen Bezug zu TV-Funktionen erkennen ließen. Die Vergleiche haben keine Hinweise auf identische Programme auf dem deutschem und den amerikanischen Geräten geliefert. Weitergehende Untersuchungen

waren aufgrund des dafür benötigten Aufwands im Rahmen der bereitstehenden Ressourcen nicht durchführbar.

4.3 Signalschutz

Während der Untersuchungen in Bezug auf das Ausspähen bzw. die Einflussnahme durch Dritte ist ein interessantes und bisher in diesem Maße in produktiven Systemen nicht dokumentiertes Angriffsszenario entdeckt worden. Dieser beruht auf einer der technischen Tatsachen, die Google TV in der im einleitenden Kapitel 1 eingeführten Klassifikation von den anderen Klassen abgrenzt. Der nachfolgend erläuterte Angriffsvektor nutzt aus, dass das lineare TV-Signal nicht strikt von den Zusatzdiensten getrennt ist, sondern tief in die Systemumgebung integriert ist. Das empfangene TV-Signal wird als Datenstrom in die Plattform eingespeist und dort von einer App verarbeitet und bei Bedarf dargestellt. Abbildung 7 zeigt eine typische Wohnzimmer-Situation. Das Fernsehprogramm, im Beispiel die Tagesschau, wird in der Google TV Plattform von der Live-TV App dargestellt.

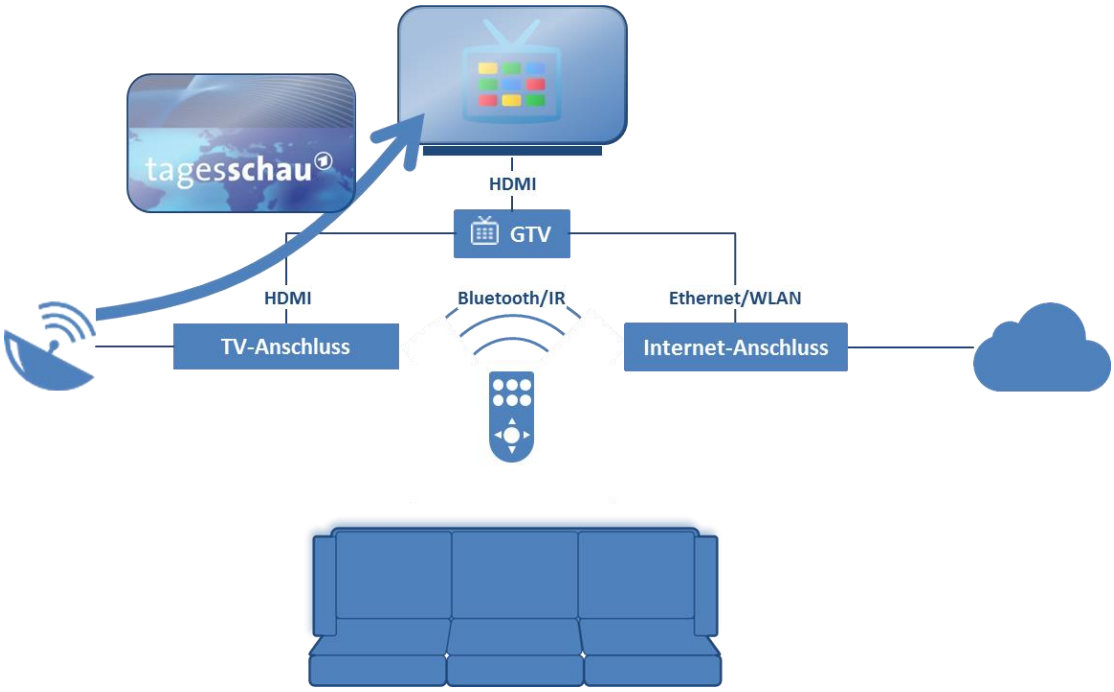


Abbildung 7: Typische Installation von Google TV

Das Fehlen einer strikten Trennung von TV-Signal und Plattform birgt Gefährdungsquellen, die in dieser Form bisher nicht vorlagen. So ist es vorstellbar, dass eine auf der Plattform installierte App die Live-TV App unterbricht oder diese gar überlagert. Die Authentizität des Empfangssignals kann somit nicht mehr gewährleistet werden, wodurch ein hohes Sicherheitsgut verloren geht. Dem Signalschutz wird in Systemarchitekturen, wie sie durch Google TV erstmals im Markt angeboten werden, nicht ausreichend Rechnung getragen und dadurch faktisch ausgehebelt. Um diese Tatsache und die darin lauernden Risiken zu veranschaulichen, zeigt Abbildung 8 wie ein Dritte über die Internet-Verbindung

Manipulationen an der aktuellen Sendung vornehmen kann. Im Beispiel wird die Tagesschau durch eine Fälschung mit dem für das Beispiel plakativ gewählten Namen Tagesschaum zu überdecken. Somit können Fälschungen von Sendungen ausgestrahlt werden, die z.B. gezielt Falschinformationen streuen. Andere Motive können in der Verbreitung unerwünschter und störender Inhalte aber auch gefährlicher Gedankengüter sein. Diesen Signalmanipulationen öffnen Systemarchitekturen die keine strikte Trennung des linearen TV-Signals und des Internets Tür und Tor, wie es bei Google TV erstmals der Fall ist.

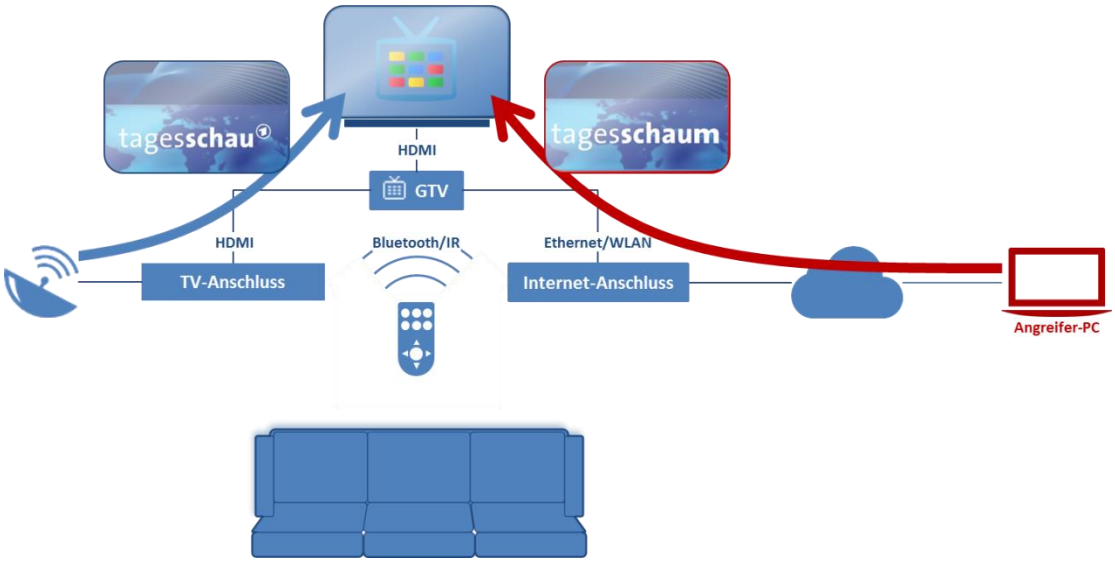


Abbildung 8: Manipulation des TV-Signals durch Dritte aus dem Internet

Im Rahmen des vorliegenden Gutachtens ist dieser Angriffsvektor theoretisch entdeckt und beschrieben worden. Zudem ist versucht worden, für den Angriff eine Implementierung anzugeben, mit der praktisch nachgewiesen werden kann, dass der Angriff auch tatsächlich funktioniert und damit eine reale Bedrohung darstellt. Abbildung 9 zeigt Screenshots, die die erzielten Ergebnisse visuell aufzeigen. Es ist gelungen, ein Angriffs-Werkzeug zu entwickeln, dass in eine beliebige App eingebettet werden kann und es anschießend Angreifern von außen ermöglicht, eine Sendung mit unautorisierten Inhalten zu überlagern. Die Überlagerung kann sowohl als Vollbild- als auch als Banner-Einspielung erfolgen. Die Vollbild-Einspielung überdeckt die eigentliche Sendung vollständig. Es können auf diese Weise vollständig eigene Inhalte (Bild und Ton) ausgestrahlt werden. In Abbildung 9 ist dies durch das Einblenden eines einfachen schwarzen Bilds erfolgt, dass zudem einen Schriftzug am oberen Bildschirmrand zeigt. Mit dem entwickelten Angriffs-Framework ist eine laufende Sendung mit dem dargestellten Bildschirm ausgetauscht worden. Ein Video, das diesen Angriff noch besser veranschaulicht, ist in der Materialsammlung enthalten (siehe Anhang B). Die Banner-Einblendung überlagert die laufende Sendung nur zum Teil. In Abbildung 9 ist diese als rotes Rechteck, das sich über die gesamte Bildschirmbreite erstreckt, aber nur eine geringe Höhe aufweist zu sehen. In dem Banner typischerweise eine textuelle Information enthalten, die für den Angriff ebenfalls integriert wurde. Das entwickelte Angriffs-

Framework erlaubt es einem Angreifer, derartige Banner beliebig oft und mit wechselnden Inhalten in laufende Übertragungen ein- und auszublenden. Auch für diese Angriffsvariante findet sich in der Materialsammlung ein Video, dass die Funktions- und Wirkungsweise deutlich macht.

Abbildung 9: Screenshots der beiden Manipulationsvarianten: Vollbild- und Banner-Einblendung

Die Bedrohung, die von dem entdeckten Angriff und der Manipulation des TV-Signals ausgeht, konnte anhand der Machbarkeitsstudie als praktisch durchführbar und damit real nachgewiesen werden. Anvisiert können als Opfer dabei selektiv und gezielt ausgewählte Einzelpersonen, aber auch die Masse. Einzelpersonen können anhand der vielen Merkmale und Identifikationen, die sich in der Android-Plattform befinden, ausgemacht werden. Beim massenhaften Ausstrahlen von Inhalten ist es nicht so offensichtlich, wie die dafür benötigten Ressourcen in Form von Rechen- und Netzwerkkapazitäten aufgebracht werden können. Da diese nicht unerheblich sind, kann der Eindruck gewonnen werden, dass die Anwendung des Angriffs auf alle angeschlossenen Haushalte aus Kapazitätsgründen nicht erfolgreich erfolgen kann. Dem ist allerdings nicht so, da in der Praxis auf dem Schwarzmarkt der Cyber-Kriminalität entsprechende Ressourcen und Infrastrukturen angeboten werden. Die als Bot-Netze bekannten Schatteninfrastrukturen bestehen aus der Agglomeration von gekaperten Systemen und für die Belange der Cyber-Kriminalität eingesetzt werden. Der massenweise Versandt von Spam-Email ist nur ein Beispiel für den Einsatz dieser Systeme.

Diesem Beispiel folgend, ist in Abbildung 10 dargestellt, wie sich ein Bot-Netz zur flächendeckenden Ausstrahlung von manipulierten und manipulativen Inhalten im Kontext des vorliegenden Angriffs einsetzen lassen kann.

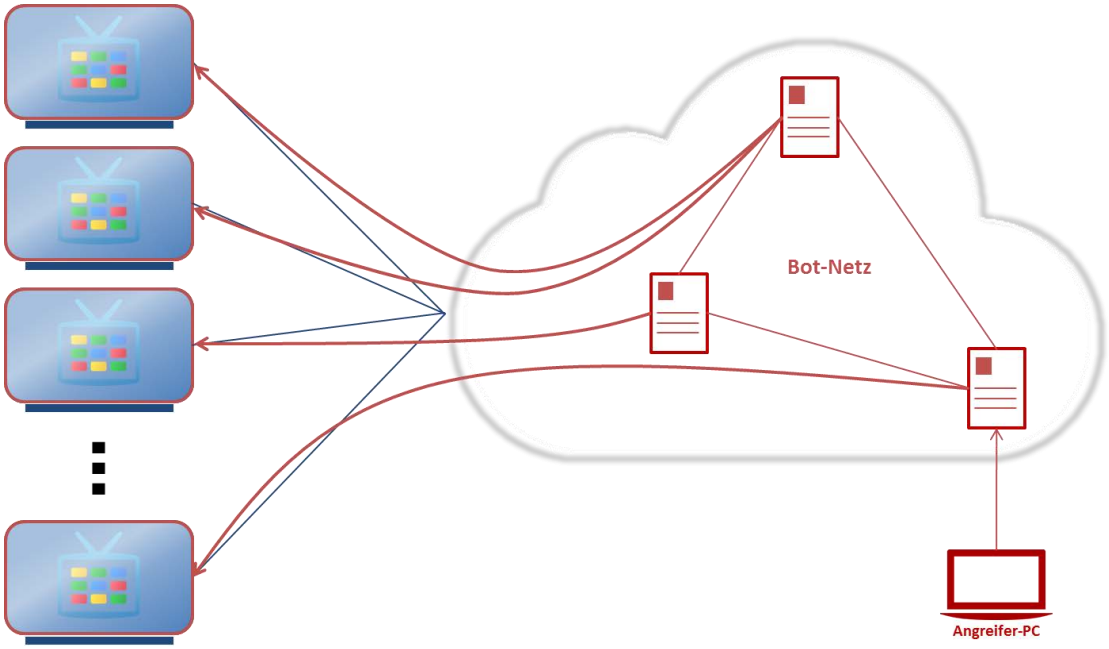


Abbildung 10: Flächendeckender Massenangriffs z.B. unter Verwendung von Bot-Netzen

Abschließend soll noch eine Einstufung des Gefährdungspotenzials vorgenommen werden, dass von diesem neuen Angriffsvektor ausgeht. Wie in den vorangegangenen Absätzen verdeutlicht wurde, ist von der Entdeckung dieser Schwachstelle über eine Machtbarkeitsstudie gezeigt worden, dass dieser Angriff praktisch genutzt werden kann und dieser somit nicht nur theoretische Bedeutung hat sondern eine reale Bedrohung markiert. Diese wird weiterhin verstärkt durch die Tatsache, dass sowohl Einzelpersonen als auch alle angeschlossenen Haushalte weltweit diesem Angriff ausgesetzt sind. Führt man sich schließlich vor Augen, dass qualitativ hochwertige Sendungen heute mit Hardware von der Stange produziert werden können, die für Jedermann günstig zu erwerben ist, erweitert dies die Menge der realistischen Angriffsszenarien weiterhin. Die Eintrittswahrscheinlichkeit für diesen Angriff muss daher als hoch eingestuft werden. Der Schaden, der sich durch einen erfolgreich ausgeführten Angriff einstellen kann, variiert in Abhängigkeit des tatsächlichen Angriffs. Es können aber durchaus verheerende Schäden auftreten, wenn man sich Szenarien wie das Ausstrahlen von gefährlichem Gedankengut vorstellt oder auch monetäre Schäden, wenn man an gefälschte Börsennachrichten denkt. Somit geht ein hohes Risiko vom Content-Injection-Angriff aus, dass nicht vernachlässigt werden darf.

Um sich vor Content-Injection Angriffen zu schützen, ist eine strikte Trennung zwischen TV-Signal und Internet-basierenden Zusatzdiensten von Nöten. Die in Kapitel 1 eingeführten Kategorien Smart-TV und Smart-Stick haben eine derartige Trennung implementiert. Die

Kapselung der Zusatzdienste in einen eigenen Fernsehkanal, wie es in der Kategorie Smart-Sticks realisiert ist, stellt dabei die stärkste Trennung dar, da TV-Signal und Internet-Zusatzdienste hier physisch voneinander separiert sind. Systemarchitekturen, wie sie durch Google TV erstmals vorliegen müssen den Aspekt des Signalschutzes explizit behandeln, um einen vergleichbaren Schutz wie in den anderen Kategorien herzustellen. Ein solcher fehlt aktuell, wonach die Verwendung von Google TV und Systemen mit einer entsprechenden Architektur als eher problematisch einzustufen ist.

5. Zusammenfassung und Ausblick

Das Gutachten hat bedeutsame Erkenntnisse gewonnen, die viele Einblicke in die Möglichkeiten zur Einflussnahme, Ausspähung und Belästigung des Fernsehkonsumenten sowie der Manipulation der Darstellung des TV-Signals geben, die mit TV-Ökosysteme mit einer engen Kopplung des TV-Signals mit dem Internet einhergehen. Hieraus ergibt sich aus verschiedenen Ebenen ein Kontrollverlust.

Für Programmveranstalter ist durch die neu gefundenen Angriffe auf die Wiedergabe des TV-Signals nicht mehr gewiss, dass die ausgestrahlten Inhalte auch in der vorliegenden Form und Qualität die Empfänger erreichen. Die aufgezeigten Möglichkeiten zur Manipulation des TV-Signals in der Google TV Box ermöglichen es Angreifern z.B. Qualitätsverzerrungen vorzunehmen oder die Marke zu verdecken, wodurch die Inhalte nicht mehr visuell auf den Sender zurückführbar sind. Zudem sind unbefugte Werbeeinspielungen durch Dritte denkbar, die in einer ähnlichen Form wie Spam-Emails störend in die Sendung eingreifen.

Aus dem letztgenannten Aspekt kann zudem der Kontrollverlust für Aufsichtsorgane abgeleitet werden, die in diesem Kontext z.B. die Einhaltung der Werberichtlinien nicht mehr ohne weiteres übersehen und durchsetzen können. Durch die Ausgestaltung als TV-Ökosystem steigt außerdem die Anzahl an Systemteilnehmern explosionsartig an, was eine Kontrolle z.B. von Apps, die über die Überprüfungen durch den Systembetreiber hinausgehen, praktisch unmöglich macht. Auch eine Prüfung und Zertifizierung einer derartigen Plattform ist aus Sicht der hochkomplexen Software kaum möglich und zudem einschlägige Zertifizierungen schlicht nicht existieren.

Für den Fernsehkonsumenten stellt sich ein derartiges TV-Ökosystem als undurchsichtige Umgebung dar, die es insbesondere bei der Verwaltung von Datenschutzerklärungen und Zugriffsrechten an Transparenz und Verständlichkeit Mangeln lässt. Jede App kann potenziell Schadcode enthalten und sich mehr Zugriffsrechte einverleiben, als sie es zur Erbringung Ihrer Funktion benötigt. Entsprechende Vorfälle, die sich in der Vergangenheit auf Android-basierten Smartphones ereignet haben und publik geworden sind, können sich in der und anderer Formen auf Google TV auf ereignen, hier allerdings angereichert mit Informationen zum Fernsehverhalten des Betroffenen. Weitreichendere Angriffsszenarien lassen gar den Zugriff auf angeschlossene Peripheriegeräte wie Mikrophone oder Kameras befürchten, die ein Hör- bzw. Fernrohr in das Wohnzimmer bahnen.

Da Google TV nach vier Jahren seit seiner Einführung in 2010 nicht in dem Maße ökonomisch erfolgreich ist, wie dies für viele der Google Dienste und Anwendungen der Fall ist [7], steht zur erwarten, dass Google TV über kurz oder lang eingestellt wird. Als Vorzeichen hierfür lässt sich sicher die Einführung von Chromecast deuten, da es u.a. eine deutlich günstigere Alternative zu Google TV ist. In den USA führt der HDMI-Stick von Google die

Verkaufshitparade für Technik-Gadgets bei Amazon an. Auch in Deutschland ist eine verstärkte Medienpräsenz speziell in der Werbung des Chromecast-Sticks zu verzeichnen. All das lässt darauf schließen, dass sich der zweite Anlauf von Google in die Wohnzimmer seiner Nutzer zu gelangen als erfolgreicher herausstellt, als es mit Google TV bisher gelungen ist. Da Chromecast allerdings in der diesem Gutachten zugrunde gelegten Klassifikation der Kategorie Smart-Stick zuzuordnen ist, und das TV-Signal damit strikter vom Internet-Zugang getrennt ist (durch verschiedene Kanäle des Fernsehers), liegen manche der beschriebenen Gefährdungen hierfür nicht vor. Dies gilt vor allem für die aufgezeigten Manipulationen an der Wiedergabe des TV-Signals. Bedenken in Bezug auf den Datenschutz verbleiben allerdings, da der Google-Account auch in Chromecast die Verknüpfung immer mehr Inhalte eines Benutzers ermöglicht. Die Relevanz der Manipulationen an der TV-Signalwiedergabe bleibt dennoch bestehen, auch wenn Google TV tatsächlich eingestellt werden würde. Die konzeptionelle Bedingung für diesen Angriffstyp liegt in der engen Kopplung zwischen TV-Signal und Internet, was sich aktuell in vielen modernen Spielekonsolen wiederfindet. Der Bedarf an weiterführenden Arbeiten auf diesem Terrain ist damit evident, um für die daraus hervorgehenden neuartigen Herausforderungen geeignete Antworten in Form von technischen aber auch organisatorischen und regulatorischen Maßnahmen entwickeln und bereitstellen zu können.

Literaturverzeichnis

[1] http://www.google.com/tv/
http://www.google.de/tv/

[2] M. Ghiglieri, F. Oswald, E. Tews: *HbbTV - I Know What You Are Watching*, 13. Deutscher IT-Sicherheitskongresses, SecuMedia Verlags-GmbH, 2013. Online verfügbar unter: http://www.sit.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_SIT/Publications/05_Ghiglieri_Oswald_Tews_HbbTV-I_Know_What_Your_Are_Watching.pdf

[3] Android Debug Bridge (ADB)
https://developer.android.com/tools/help/adb.html

[4] tcpdump
http://www.tcpdump.org/

[5] Wireshark
http://www.wireshark.org/

[6] nmap
http://nmap.org/

[7] The Early Days of Google TV Apps, Feb. 2012
http://xyo.net/blog/google-tv-apps-fact-sheet/

Anhang A: Testgeräte

Die Testgeräte, die in den Untersuchungen verwendet wurden, sind in den folgenden Unterkapiteln detailliert beschrieben. Diese Angaben sollen insbesondere beim Nachvollziehen der im Rahmen des Gutachtens ermittelten Erkenntnisse und Ergebnisse unterstützen.

Ein Beobachtungsgegenstand lag im Vergleich von Google TV Geräten, die für den US-amerikanischen Markt bestimmt sind und entsprechenden Geräten, die in Deutschland vertrieben werden. Diese Unterscheidung in der nachfolgenden Struktur berücksichtigt worden.

A.1 Geräte für den US-amerikanischen Markt

A.1.1 Sony NSZ-GS7

Datenblatt

Sony NSZ-GS7	
	Hersteller: Sony
	URL des Herstellers: http://www.sony.com/
	Modell: NSZ-GS7
	Firmware: 3.2 (Build: REL03_NSZGS7_U2_1104_4383_20120724_URSC_S67254)
	Factory Reset: ja, aber kein Schalter am Gehäuse und nicht in der beigefügten Dokumentation beschrieben
	Datenschutzerklärung (In Verpackung): nein
	Datenschutzerklärung (Online verfügbar): nein
	Datenschutzerklärung (Während Installation und elektronisch im Gerät hinterlegt): ja

Bilder


SONY
NSG-MR5U
POWER
TV/AMP
INPUT
TV
DVR
GUIDE
INFO
Fn
SONY


SONY
INFO WIDE 3D AUDIO SUBTITLE
REC
Esc
Tab
Enter
Fn
Ctrl
LIGHT
SONY


IN
HDMI
OUT
DIGITAL OUT
OPTICAL
IR
BLASTER
LAN(100)
AC IN


SONY
MODEL No. NSZ-GS7
NETWORK MEDIA PLAYER
120 V 60 Hz 21 W
Bluetooth
CAUTION
ATTENTION
SONY CORPORATION

A1.2 Hisense Pulse with Google TV

Datenblatt

Hisense Pulse with Google TV	Hersteller: Hisense
	URL des Herstellers: http://www.hisense-usa.com/
	Modell: Pulse with Google TV
	Firmware: 3.2 (Build: MASTER.user.hisense.20121122.124750)
	Factory Reset: ja (Schalter am Gehäuse und in der beigefügten Dokumentation beschrieben)
	Datenschutzerklärung (In Verpackung): nein
	Datenschutzerklärung (Online verfügbar): nein
	Datenschutzerklärung (Während Installation und elektronisch im Gerät hinterlegt): ja

Bilder


PIP
Hi-Media
Web
Discover
Live TV
LAST
INFO
HOME
MENU
OK
ALL Apps
BACK
VOL
CH
A
B
C
D
GUIDE
Hisense


Esc
Tab
Caps
Shift
Ctrl
Fn
Web
MENU
Enter
PIP
HOME
BACK
OK


IR
BLASTER
HDMI IN
HDMI OUT
LAN
DC 12V


Hisense
Model: GX1200V
NETWORK MEDIA PLAYER
INPUT: 12V 2A 15W
IC: 10680A-W9HLCDX0006
FCC ID: W9HLCDX0006
The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
LISTED
E215878
AUDIO/VIDEO APPARATUS
79LN
This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
HISENSE ELECTRIC CO.,LTD.
218 QIANWANGANG RD ECONOMIC& DEVELOPMENT ZONE QINGDAO CHINA
CAUTION
RISK OF ELECTRIC SHOCK DO NOT OPEN
RISQUE DE CHOC ELECTRIQUE - NE PAS OUVRIR
S/N:3TE00G12400835O1322
NOV 15,2012
MADE IN CHINA

A1.3 VIZIO Co-Star with Google TV

Datenblatt

VIZIO Co-Star with Google TV	Hersteller: VIZIO
	URL des Herstellers: http://www.vizio.com/
	Modell: Co-Star with Google TV
	Firmware: 3.2 (Build: U2.3.1)
	Factory Reset: ja (Schalter am Gehäuse und in der beigefügten Dokumentation beschrieben)
	Datenschutzerklärung (In Verpackung): nein
	Datenschutzerklärung (Online verfügbar): nein
	Datenschutzerklärung (Während Installation und elektronisch im Gerät hinterlegt): ja

Bilder


M-GO
NETFLIX
amazon
INFO
SEARCH
GUIDE
CH/PG
OK
VOL
LIST
PIP
LIVE TV
INPUT
QUICK


TAB
SHIFT
Fn
ESC
SPACE
CTRL
SHIFT
DEL
ENTER
X
Y
B
A


IN
CUT
LAN
DC IN


RESET
VIZIO
39 Tesla
Irvine, CA 92618
WWW.VIZIO.COM
Stream Player
Model No.: VAP430
Input : 5V ⎓ 3A
Part No.: 11000050045
Serial No.: WWZOMYAN3802681
c UL us LISTED
E249047
Audio/Video
Apparatus
FC
Contains Wireless Module
FCC ID: NKR-DHSM87B

A.2 Geräte für den deutschen Markt

A.2.1 Sony NSZ-GS7

Datenblatt

Sony NSZ-GS7	
	Hersteller: Sony
	URL des Herstellers: http://www.sony.de/
	Modell: NSZ-GS7
	Firmware: 3.2
	Factory Reset: ja, aber kein Schalter am Gehäuse und nicht in der beigefügten Dokumentation beschrieben
	Datenschutzerklärung (In Verpackung): nein
	Datenschutzerklärung (Online verfügbar): nein
	Datenschutzerklärung (Während Installation und elektronisch im Gerät hinterlegt): ja

Bilder


SONY
NSG-MR5D
TV/AMP
TV
PVR
SONY


SONY
3D AUDIO
TV DIGITAL ANALOG
REC
Esc
Tab
Enter
Fn
Ctrl
TV
SONY


IN
HDMI
OUT
DIGITAL OUT
OPTICAL
IR
BLASTER
LAN(100)
AC IN


SONY®
MODEL No. NSZ-GS7
NETWORK MEDIA PLAYER
220-240 V 50/60 Hz 21 W
Bluetooth
N50
Manufactured under license from Dolby Laboratories. Dolby and the double-D symbol are trademarks of Dolby Laboratories.
SONY CORPORATION
MADE IN CHINA
9-885-169-33
GS7 EC1 S01-2007642-7

Anhang B: Inhalt der Materialsammlung

In den Untersuchungen wurden unterschiedliche Daten erfasst und analysiert. Die Rohdaten sind vollständig in einer Materialsammlung abgelegt. Die Materialsammlung kann bei Bedarf bei der LfM angefordert werden (nrwdigital@lfm-nrw.de).

Das Wurzelverzeichnis der Materialsammlung ist wie im Folgenden dargestellt organisiert und enthält die beschriebenen Inhalte:

Dateisystem	Vorinstallierte Dateien, die ohne besondere Berechtigungen auslesbar waren
Handbücher	Verfügbare elektronische Versionen der Handbücher der Testgeräte
Kommunikationsmitschnitte	Protokollierte Kommunikation
Portscans	Analyseergebnisse in Bezug auf kommunikationsbereite Dienste
Produktphotos	Photos der Tesgeräte, die insbesondere Hardwareschnittstellen dokumentieren
Policies	Policies zur Nutzung von Google TV
Videos	Videos, die die Installation und Voreinstellung der Testgeräte dokumentiert