



KNF-Kongress 2016

Andreas Sachs
Dipl.-Inform.(Univ.)
Referatsleiter

Smart-TV, Apps und Online-Angebote –
Datenschutzprüfungen online und im IT-Labor



Agenda

- 1 **Vorstellung** des BayLDA
- 2 **Wieso prüfen** – Aufgabe der Aufsichtsbehörde
- 3 **Onlineprüfungen** – Das Internet machts möglich
- 4 **IT-Labor**: Den Daten auf der Spur
- 5 **Prüfung**: Tracking mit Google Analytics und Adobe Analytics

Agenda

- 6 Prüfung: Apps „entzaubert“
- 7 Prüfung: Transportverschlüsselung im Zeitalter der Massenüberwachung
- 8 Prüfung: Smart TV und das Ende der Anonymität
- 9 Prüfung: Sind Wearables „kritisch“
- 10 **Ausblick:** Prüfungen morgen

1 Vorstellung



Wir überwachen die Einhaltung des
Datenschutzrechts

im **nicht-öffentlichen Bereich**

in **Bayern**, das heißt

- in den privaten **Wirtschaftsunternehmen**,
- bei den freiberuflich Tätigen,
- in Vereinen und Verbänden,
- und im Internet.

1 Vorstellung



Anzahl
Unternehmen
in Bayern:
über 600.000

Anzahl
Stellen
der Behörde:
16*



*davon drei Informatiker

Unsere Zahlen

Beschwerden im Jahr:
ca. 1000

Beratung von
Unternehmen im Jahr:
ca. 1800

Beratung von Bürgern im
Jahr:
ca. 900

Tendenz: steigend 



2

Wieso prüfen – Aufgabe der Aufsichtsbehörde

■ §38 BDSG (Aufsichtsbehörde)

- Die Aufsichtsbehörde **kontrolliert** die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz
- Die Aufsichtsbehörde **berät** und **unterstützt** die verantwortlichen Stellen
- Die Aufsichtsbehörde kann Maßnahmen zur Beseitigung von Verstößen **anordnen**

2 Wieso prüfen – Aufgabe der Aufsichtsbehörde

▪ „Grechtenfragen“ (Auszug):

- Was ist der **Stand der Technik**?
- Wie verarbeiten **smarte Produkte** personenbezogene Daten?
- Wie funktionieren Trackingverfahren **genau**?

➔ Ein sehr genaues **technisches Verständnis** ist für die rechtliche Anwendung notwendig

➔ Aufgabe: Vom **Glauben** zum **Wissen** kommen



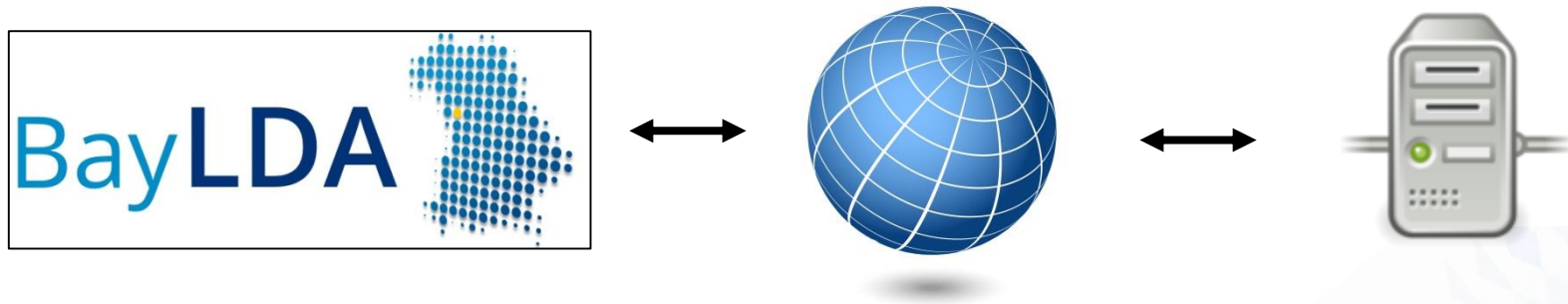
2

Wieso prüfen – Aufgabe der Aufsichtsbehörde

▪ Folgen von (technischen) Prüfungen:

- **Vorgaben** für den beanstandungsfreien Einsatz erstellen (z.B. Orientierungshilfen)
- **Hilfestellungen** für die Praxis geben (z.B. Checkliste Apps)
- **Anordnungen**
- **Bußgelder**
- **Rechtssicherheit** schaffen

3 **Onlineprüfungen:** Das Internet machts möglich



- Breite Prüfmasse mit wenig Personalaufwand
- Aber: In der Nachbereitung nicht zu unterschätzen

▪ **Prüfgegenstände**

- **Webseiten**
- **Webanwendungen**
- **Kommunikation**
- **Apps**

3 **Onlineprüfungen:** Das Internet machts möglich

- **Prüfdurchführung mit eigener Prüfsoftware (Skripte)**
 - **Webseiten**
 - Download und Analyse von öffentlich zugänglichen Inhalten
 - **Serversysteme**
 - Prüfung auf bestehende Sicherheitslücken (z.B. Heartbleed).
 - Vorsicht: Nicht einfach irgendwelche Tools verwenden
 - **Kommunikation**
 - Aufbau und Prüfung einer verschlüsselten Verbindung

4 IT-Labor: Den Daten auf der Spur

Unser Prüflabor – eigentlich nichts Besonderes



5 Prüfung: Tracking mit Google Analytics und Adobe Analytics

Motivation des BayLDA: Vollzug von gemeinsamen Beschlüssen

Sitzung des Düsseldorfer Kreises am 26./27. November 2009 in Stralsund

Beschluss

**der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
am 26./27. November 2009 in Stralsund**

**Datenschutzkonforme Ausgestaltung von Analyseverfahren zur
Reichweitenmessung bei Internet-Angeboten**

5 Prüfung: Tracking mit Google Analytics und Adobe Analytics

1. Großprüfung des BayLDA: Google Analytics

- Andere Aufsichtsbehörden waren schon **Vorreiter** (Bayern, Rheinland-Pfalz)
- Neu: **Massenprüfung** mit Vollzug
- April - Mai 2012 : Prüfdurchführung
- **Anforderungen:**
 - Datenschutzerklärung vorhanden
 - Information in Datenschutzerklärung
 - Anonymisierung der IP-Adresse implementiert
 - Opt-Out verfügbar
 - Vertrag zur Auftragsdatenverarbeitung geschlossen
- **Geprüfte** bayerische Webseiten (von Unternehmen): **13404**
- Festgestellte **Mängel** (unterschiedlicher Ausprägung) bei **2371** Unternehmen -> **Alle** wurden angeschrieben
- **Bußgelder** wegen nachhaltiger Weigerung
- Bei (fast) allen Stellen wurden die Anforderungen **umgesetzt**



Google Analytics



5 Prüfung: Tracking mit Google Analytics und Adobe Analytics

1. Großprüfung des BayLDA: Google Analytics

WebTrackAnalyzer des BayLDA

Szenario: Erstprüfung Nachprüfung
 GoogleAnalytics

Daten:
 Eingabe: C:\pruefung\Firmenliste.txt
 Ausgabe: C:\pruefung\PruefungGA_1.txt
 Inhalt: C:\pruefung\Inhalt

Geladene Datensätze: 13404
 Ungültige Datensätze: 0
 Stop

Status: Webseite 39 von 13404 Restdauer:00:08:48:26.678

Log

Status	Zeitpunkt	URL	Firma	DS	GA	GA(C)	AnonIP	Anz	Anz(C)	AnzIP	AnzIP(C)	ID1	ID2	ID1(C)	ID2(C)
O	Mittwoch, 2. Mai 2012 08:40:54	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:40:56	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:40:59	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:02	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:03	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:04	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:10	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:13	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:18	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:20	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:23	http://www.	⚠	J	N	J	1	0	1	0
O	Mittwoch, 2. Mai 2012 08:41:25	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:26	http://www.	✓	N	N	N	0	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:28	http://www.	✗	J	N	N	1	0	0	0
O	Mittwoch, 2. Mai 2012 08:41:29	http://www.	✓	N	N	N	0	0	0	0

5 Prüfung: Tracking mit Google Analytics und Adobe Analytics

2. Großprüfung des BayLDA: Adobe Analytics

- Auswahl der Adobe Deutschlandsitz in **München** hat
- Sorge von Seiten der Fa. **Google**, dass nur deren Produkt aufsichtlich geprüft würde
- April - Mai 2013 : Prüfdurchführung
- Anforderungen:
 - Datenschutzerklärung vorhanden
 - Information in Datenschutzerklärung
 - Anonymisierung der IP-Adresse implementiert (nur **serverseitig** machbar -> Stichprobennachweise durch Screenshots)
 - Opt-Out verfügbar
 - Vertrag zur Auftragsdatenverarbeitung geschlossen
- **Geprüfte** bayerische Webseiten (von Unternehmen): **10.238**
- Einsatz festgestellt bei **44** -> Alle wurden angeschrieben
- Bei allen Stellen wurden die Anforderungen **umgesetzt**



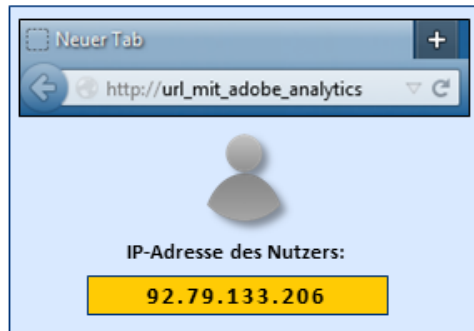
5 Prüfung: Tracking mit Google Analytics und Adobe Analytics

2. Großprüfung des BayLDA: Adobe Analytics

- Anonymisierung der IP-Adresse musste von Seiten Adobe nachgebessert werden. Nun passt es:



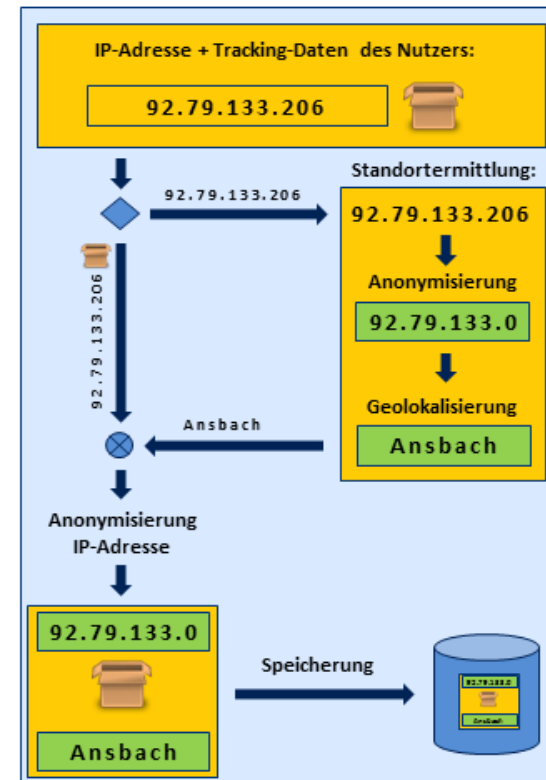
Webseitenaufruf des Nutzers



Datenübertragung an Adobe



Datenverarbeitung bei Adobe



6 Prüfung: Apps „entzaubert“



Motivation:

- **Presseberichte:** Apps können „Spione in der Hosentasche“ sein
- Fragen: Welche personenbezogenen Daten verarbeitet eine App denn **wirklich**?
 - An **wen** werden Daten übertragen
 - **Welche** Daten werden übertragen
 - Zu welchem **Zweck** werden diese übertragen
 - Sind **Grundsätze** der Erforderlichkeit, Transparenz und Rechtsgrundlagen erfüllt?
 - Sind die technischen und organisatorischen **Maßnahmen** ausreichend?

6 Prüfung: Apps „entzaubert“



Dynamische
Analyse



Reverse
Engineering



Systemanalyse



6 Prüfung: Apps „entzaubert“

Dynamische Analyse mit Man-in-the-Middle Methodik

Eingesetzte Software

- BurpSuite
- Wireshark
- Kali



Labor-PC



DSL



The screenshot shows the Burp Suite interface with a list of intercepted items. The list includes various hosts and URLs, such as mydas.mobi, gstatic.com, and admob.com. Below the list, a Wireshark packet capture window is visible, showing details of an HTTP GET request to a specific URL.

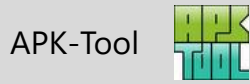
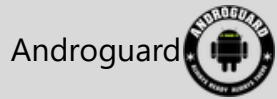
#	Host	URL	MIME type	Extension	Title	SSL	IP
1	http://androidsdk.ads.mg.mydas.mobi	/getAd.php?acc=clerometer=true&adtype=MMBannerAdTop&h=205.55	HTML	php5		<input type="checkbox"/>	216.157.12
2	http://bank-12.ads.mg.mydas.mobi	/getmage.php?appid=641306&mode=live&cid=1352758&uid=mmid_fr	GIF	php5		<input type="checkbox"/>	216.157.12
3	http://met.adwhirl.com	/exmet.php?appid=a1181798980748a69b194424285e5da6&id=b3f311c	HTML	php		<input type="checkbox"/>	54.235.103
4	http://www.gstatic.com	/afmas/dk-core-v40.js	script	js		<input type="checkbox"/>	173.194.95
5	http://googleads.g.doubleclick.net	/mads/gma?preqs=1&u_sd=26&u_w=720&msid=goldenshoretechnology	HTML			<input type="checkbox"/>	173.194.95
6	http://media.admob.com	/formats/templates.js	script	js		<input type="checkbox"/>	173.194.95



6 Prüfung: Apps „entzaubert“

Statische Analyse durch Reverse Engineering (Android)

Eingesetzte Software



Labor-PC



Verbindung per USB



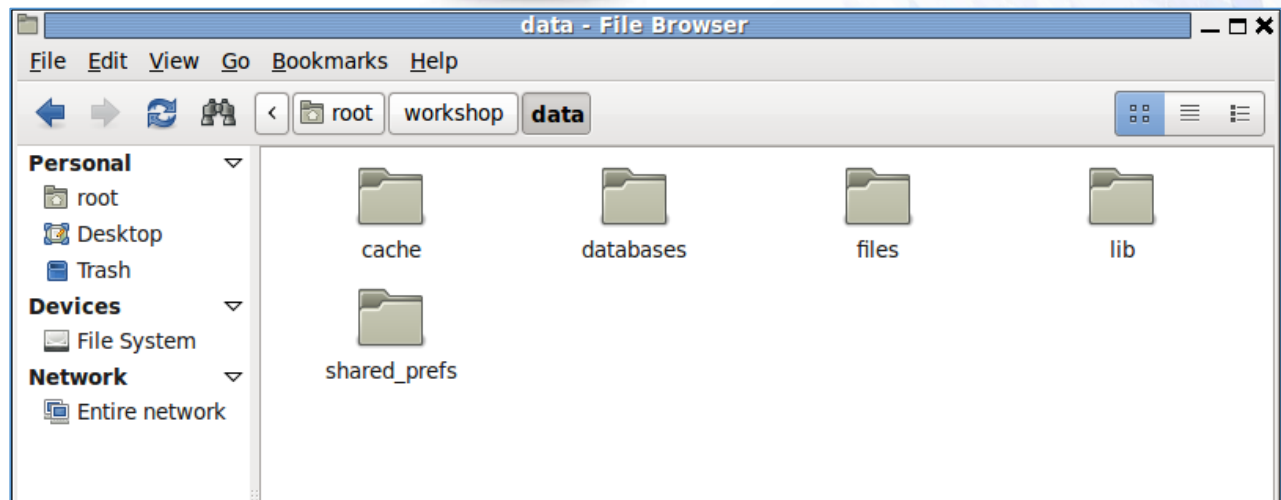
```
package goldenshoretechnologies.brightestflashlight.free;

import android.app.Activity;

public class BrightestFlashlightMain extends Activity
implements AdWhirlLayout.AdWhirlInterface
{
    private static final int LED_NOTIFICATION_ID = 777;
    private static final String TAG = "BrightestFlashlightMain";
    AdWhirlLayout adWhirlLayout2 = null;
    SurfaceHolder.Callback camPreviewSurfaceCallback = new SurfaceHolder.Callback()
    {
        public void surfaceChanged(SurfaceHolder paramAnonymousSurfaceHolder, int param
        {
            try
            {
                if (BrightestFlashlightMain.this.mCamera != null)
                {
                    Camera.Parameters localParameters;
                    List localList;
                    int i;
                    int j;
                    int k;
                    if (!Globals.bUsingTorchNoPreviewResize)
                    {
                        localParameters = BrightestFlashlightMain.this.mCamera.getParameters();
                        localList = localParameters.getSupportedPreviewSizes();
                        i = 2147483647;
                        j = 1;
                        k = 1;
                    }
                    for (int m = 0; ; m++)
                    {
                        if (m >= localList.size())
                        {
                            localParameters.setPreviewSize(j, k);
                            BrightestFlashlightMain.this.mCamera.setParameters(localParameters);
                        }
                    }
                }
            }
        }
    }
}
```

6 Prüfung: Apps „entzaubert“

Systemanalyse (Forensischer Ansatz)





6 Prüfung: Apps „entzaubert“

Technische App-Prüfung

- Im ersten Halbjahr **2013** wurden eigenständig Apps in unterschiedlicher Prüftiefe mit flexiblem Prüffokus untersucht:
- Es wurden **31 Apps** aus den Stores heruntergeladen und systematisch technisch geprüft, davon überwiegend schwerpunktmäßig Android und geringfügig iOS
- Dauer pro Prüfung **1/2 - 2** Personentage
- Bei nicht geringfügigen Mängeln wurde ein **aufsichtliches Verfahren** nach § 38 BDSG eröffnet
- Die **Ergebnisse** der Prüfungen wurde den App-Anbietern mitgeteilt (zwischen 2 bis 10 Seiten) und Nachbesserung verlangt

6 Prüfung: Apps „entzaubert“

Aufsichtsbehörden und Apps

- Deutsche Aufsichtsbehörden haben „**Orientierungshilfe Apps**“ herausgegeben

Download (auch) unter:

www.lda.bayern.de/de/orientierungshilfen.html



- **App-Prüfkatalog** für den technischen Datenschutz bei Apps (BayLDA)

Download unter:

www.lda.bayern.de/de/infoblaetter.html



7

Prüfung: Transportverschlüsselung im Zeitalter der Massenüberwachung

Motivation des BayLDA: Vollzug von gemeinsamen Beschlüssen

87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 27. und 28. März in Hamburg

Entschließung

Stand: 27. März 2014

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

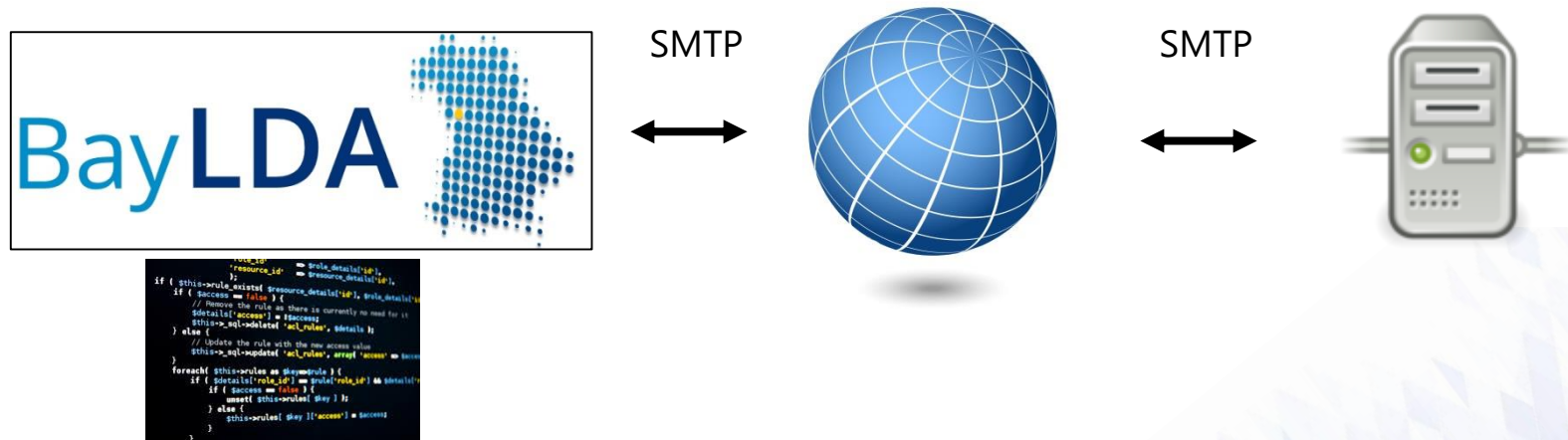
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,

2. Bereitste Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

7

Prüfung: Transportverschlüsselung bei Mailservern



Prüffokus:

- Unterstützung von **STARTTLS** (opportunistisch)
- Unterstützung von **Perfect Forward Secrecy** (PFS)
- Mindestanforderung an **Schlüssellängen** (RSA, EC)
- Bei **allen** TLS-Protokollversionen

7

Prüfung: Transportverschlüsselung bei Mailservern



Prüfung im Herbst 2014:

- **2.236** Unternehmen wurden geprüft
- **772** Unternehmen hatten **Mängel** -> Aufsichtliche Verfahren wurden eröffnet
- Bei 6 Unternehmen wurden **Anordnungen** nach § 38 Abs. 5 BDSG erlassen
-> Alle wurden bestandskräftig
- Bei (fast) allen geprüften Unternehmen wurden die **Mindestanforderungen** an die Transportverschlüsselung **durchgesetzt**
- Leider **keine gerichtlichen Verfahren** bezüglich der Frage nach dem Stand der Technik und der Verhältnismäßigkeit

Das Bayerische Landesamt für Datenschutzaufsicht erlässt gemäß § 38 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) folgende

Anordnung:

1. Die Musterfirma GmbH, vertreten durch den Geschäftsführer Bud Spencer, wird verpflichtet, bis zum 23. Oktober 2015 den E-Mail-Server mx.musterfirma.de so umzustellen, dass dieser bei Einsatz der Transportverschlüsselung mit dem STARTTLS-Protokoll die Verschlüsselungstechnik Perfect Forward Secrecy (PFS), die dem Stand der Technik entspricht, wirksam unterstützt wird.
2. Bei Einsatz von PFS muss der Email-Server derart konfiguriert werden, dass PFS **prior**, d.h. vorrangig vor anderen Verschlüsselungstechniken, verwendet wird.
3. Die sofortige Vollziehung der Ziffer 1 und 2 dieses Bescheides wird angeordnet.
4. Für den Fall, dass die Musterfirma GmbH der Verpflichtung nach Ziffer 1 nicht nachkommt, wird ein Zwangsgeld in Höhe von 8.000,00 EUR fällig.
5. Die Musterfirma GmbH hat die Kosten des Verfahrens zu tragen. Für diesen Bescheid werden eine Gebühr von 100,00 EUR festgesetzt und Auslagen in Höhe von 3,45 EUR in Rechnung gestellt.

8

Prüfung: Smart TV und das Ende der Anonymität

Fernsehen heute: Smart-TV



Rundfunksignal
→



↓
Internetbasierter
Rückkanal



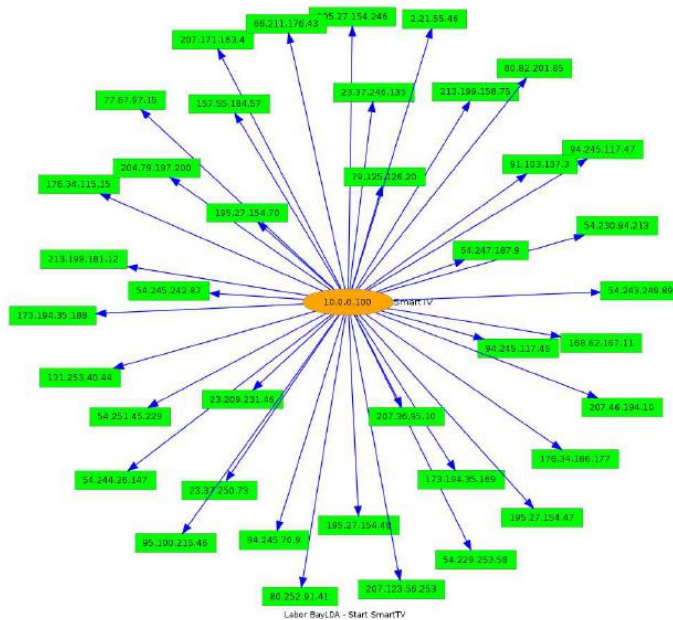
**Smart-Tvs:
Kann anonymes Fernsehen noch
möglich sein?**

8

Prüfung: Smart TV und das Ende der Anonymität

Variante 1: Einschalten des SmartTV ohne Nutzeraktion

- Bei Laborversuch: Es fanden viele Aufrufe an Webserver statt
- Live Demo
- Visualisierung der IP-Adressen:

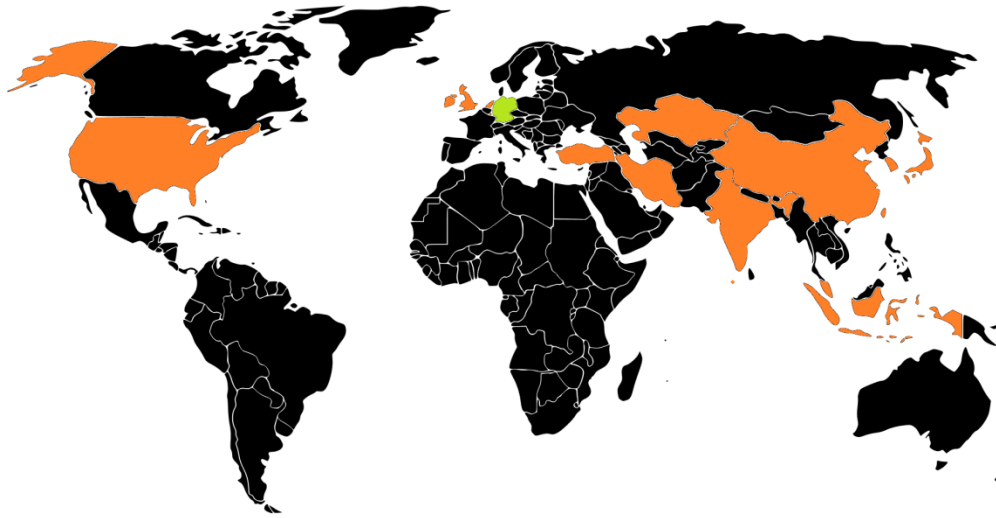


Ein Smart-TV kann
viele Datenempfänger
haben

8

Prüfung: Smart TV und das Ende der Anonymität

Smart-TVs sind International (Geolokation der IP-Adressen)



- | | | | |
|---|-------------|--|----------------|
|  | Südkorea |  | Indien |
|  | Indonesien |  | Irland |
|  | Japan |  | Luxemburg |
|  | USA |  | Großbritannien |
|  | Malediven |  | Türkei |
|  | Taiwan |  | Niederlande |
|  | China | | |
|  | Hong Kong | | |
|  | Iran | | |
|  | Kasachstan | | |
|  | Deutschland | | |
|  | Singapur | | |

8

Prüfung: Smart TV und das Ende der Anonymität

Thema Smart-TV ist nicht so neu:



TECHNISCHE
UNIVERSITÄT
DARMSTADT

HbbTV - I Know What You Are Watching, Mai 2013



**Hacking, Surveilling, and Deceiving victims on
Smart TV, 2013**



**KOREA
UNIVERSITY**

Smart TV Security - #1984 in 21st century -, 2013



**Spion im Wohnzimmer: c't entdeckt
Sicherheitslücken in zahlreichen Smart-TVs, 2014**

8

Prüfung: Smart TV und das Ende der Anonymität

Wieso prüfen die Datenschutzaufsichtsbehörden auch noch?

- Ziel 1: **Technische Sachverhalte** verstehen/nachvollziehen
- Ziel 2: **Geräteübergreifende** Aspekte erkennen
- Ziel 3: **Akteure** definieren
- Ziel 4: Rechtliche und technische **Anforderungen** festlegen
- Ziel 5: Einhaltung der Anforderungen **prüfen** und **durchsetzen**

8

Prüfung: Smart TV und das Ende der Anonymität

1. Schritt : Zuständigkeit klären

- Aufsichtsbehörden verständigen sich auf gemeinsames Prüfprojekt
- BayLDA führt dies technisch per Amtshilfe durch

2. Schritt : Geräte beschaffen

- Gerätehersteller werden angeschrieben und um Leihgerät gebeten
- Transparente Prüfung ist ein wichtiges Ziel: Unternehmensvertreter sind zur Vor-Ort Prüfung eingeladen



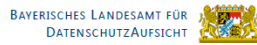


8

Prüfung: Smart TV und das Ende der Anonymität

3. Schritt : Prüfmethodik

- Ergebnisse sollen möglichst singular und reproduzierbar sein



SmartTV/HbbTV-Prüfung

Name des Geräteherstellers	Datum der Prüfung
Unternehmensangaben des Geräteherstellers	BayLDA-Prüfer
Unternehmen:	Name:
Anschrift:	
Bundesland:	
Unternehmensvertreter:	
Angaben zum Testgerät	Sonstige Prüfteilnehmer
Modellbezeichnung:	Name:
Version:	
Seriennummer:	
Firmware-Version:	
MAC-Adresse (Wi-Fi bzw. WLAN):	
MAC-Adresse (LAN):	
Eindeutige Geräte-ID:	

Zusammenfassung Prüfzenarien

Testfall 1: Offline-Start-Informationen Informationen bei erstmaligem Start des Gerätes (offline)	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 2: Online-Start-Informationen Informationen bei erstmaligem Start des Gerätes (online)	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 3: Start ohne Geräteeinrichtung Datenflüsse bei erstmaligem Start des Gerätes ohne Hauptmenü	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 4: Start mit Geräteeinrichtung Datenflüsse bei erstmaligem Start des Gerätes mit Hauptmenü	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 5: Senderaufruf ohne Red-Button Datenflüsse bei Aufruf eines Senders ohne Red-Button-Nutzung	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 6: Senderaufruf mit Red-Button Datenflüsse bei Aufruf eines Senders mit Red-Button-Nutzung	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 7: HbbTV-Start Informationen bei erstmaligem Start von HbbTV mit Red-Button	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 8: HbbTV-Senderwechsel in Sendergruppe Datenflüsse bei Nutzung zweier Sender einer Sendergruppe mit HbbTV mit Red-Button	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 9: Aufnahme mit externem Datenträger Aufnahme von Sendungen auf externe Festplatte	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 10: Abspielen von Aufnahmen ohne Registrierung Abspielen von Sendungen von externer Festplatte ohne Benutzerregistrierung	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 11: Abspielen von Aufnahmen mit Registrierung Abspielen von Sendungen von externer Festplatte mit Benutzerregistrierung	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 12: YouTube-Video Datenflüsse bei Abspielen eines YouTube-Videos	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil
Testfall 13: Stresstest Datenflüsse bei einem Geräte-Stresstest	<input type="checkbox"/> durchgeführt	<input type="checkbox"/> nicht geführt, weil

Testfall 3: Start ohne Geräteeinrichtung: Datenflüsse bei erstmaligem Start des Gerätes ohne Hauptmenü	
Testziel	
Welche Datenübermittlungen finden bei erstmaligem Start eines Gerätes an welche Server (IP-Adressen) statt, ohne dass ein Fernsehsignal vorhanden ist oder gerätespezifische Funktionen (z. B. Apps) genutzt werden?	
Vorbedingungen	
Reset auf Werkzeinstellungen (über Servicemenü)	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil:
Servicemenü erreichbar durch	
Fernseher vom Stromnetz getrennt	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil:
Kein Fernsehsignal	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil:
Prüfschritte	
1 Fernseher an Stromnetz anschließen	<input type="checkbox"/> durchgeführt
2 Fernseher einschalten	<input type="checkbox"/> durchgeführt
3 WLAN aktivieren	<input type="checkbox"/> ok <input type="checkbox"/> nein, weil:
4 Zentrales Menü nicht einrichten	<input type="checkbox"/> ok <input type="checkbox"/> nein, weil:
Prüfaufzeichnung	
1 Wireshark	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil:
2 Prüfdatei	
3 Prüfsumme (SHA1)	
4 Burp Suite	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil:
5 Prüfdatei	
6 Prüfsumme (SHA1)	
Prüfergebnis	
1 Liste TCP-Hosts	
2 Liste http-Hosts	
3 Liste https-Hosts	
4 Detailanalyse der Dateninhalte	
5 Übermittlung von Geräte-IDs an	

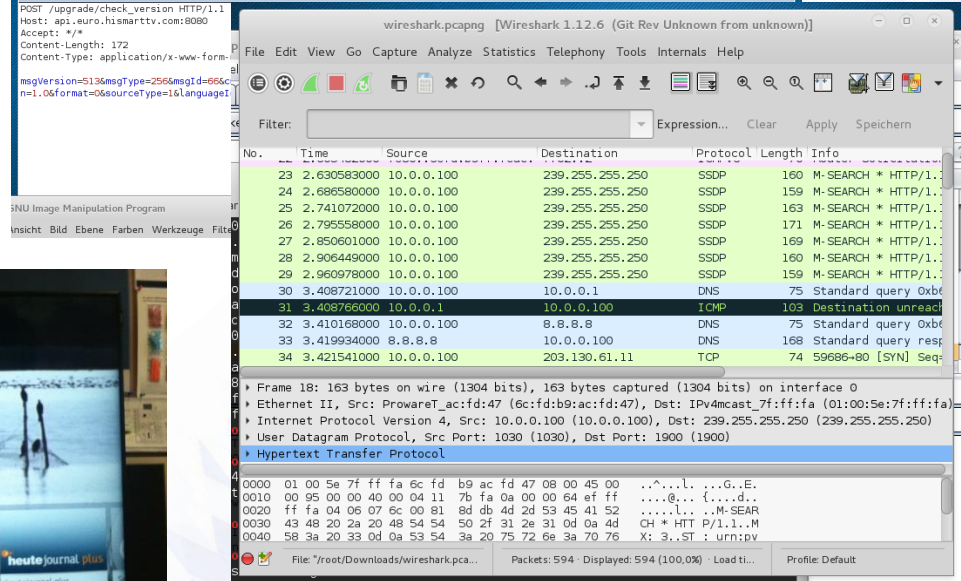
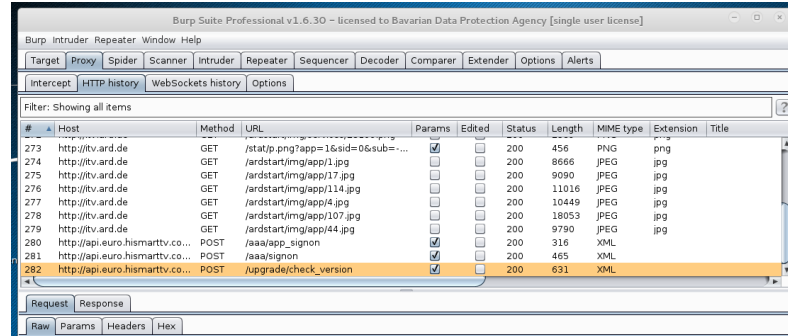


8

Prüfung: Smart TV und das Ende der Anonymität

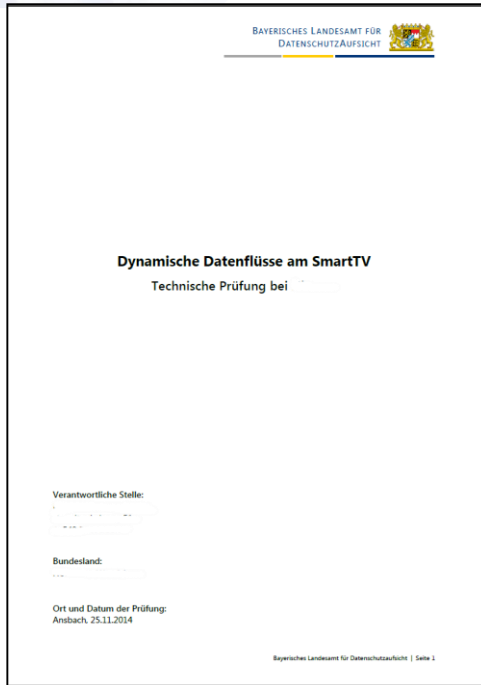
4. Schritt : Durchführung

- Szenarien durchgehen
- Dokumentation
- Protokollierung





5. Schritt : Technischer Prüfbericht



6.3. Datenflüsse bei erstmaligen Start des Gerätes ohne Hauptmenü

Testfall 3: Start mit Geräteeinrichtung: Datenflüsse bei erstmaligem Start des Gerätes ohne Hauptmenü

Testziel
Welche Datenübermittlungen finden bei erstmaligem Start eines Gerätes an welche Server (IP-Adressen) statt, ohne das ein Fernsehsignal vorhanden ist oder gerätespezifische Funktionen (z. B. Apps) genutzt werden?

Vorbereitungen

Reset auf Werkseinstellungen (über Servicemenü)	<input checked="" type="checkbox"/> ja	<input type="checkbox"/> nein, weil:
Fernseher vom Stromnetz getrennt	<input checked="" type="checkbox"/> ja	<input type="checkbox"/> nein, weil:
Kein Fernsehsignal	<input checked="" type="checkbox"/> ja	<input type="checkbox"/> nein, weil:

Prüfschritte

1 Fernseher an Stromnetz anschließen	<input checked="" type="checkbox"/> durchgeführt
2 Fernseher einschalten	<input checked="" type="checkbox"/> durchgeführt
3 WLAN aktivieren	<input checked="" type="checkbox"/> ok <input type="checkbox"/> nein, weil:
4 Zentrales Menü nicht einrichten	<input checked="" type="checkbox"/> ok <input type="checkbox"/> nein, weil:

Prüfaufzeichnung

1 WireShark	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein, weil:
2 Prüfdatei	Testfall2-3/wireshark.pcapng
3 Prüfsumme (SHA256)	8a4087b6edcd7a93df3110f4524c209cb319b49d6b775603d8117498bc86
4 Burp Suite	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein, weil:
5 Prüfdatei	Testfall2-3/burp.dat
6 Prüfsumme (SHA256)	6bb1ec75f91171be09453d8a17346ecca55f91297058c95fe41cb94b7e06f
7 Bildschirmfotos mit Digitalkamera	<input checked="" type="checkbox"/> ja, Dateinamen mit Fotos_ screenshots_, Auszugsbilder siehe nachfolgend

Datenflüsse

1 Liste TCP-Hosts	TCP(203.130.61.11 (203.130.61.11-BI-CNC)) CN, China TCP(203.130.61.91 (203.130.61.91-BI-CNC)) CN, China NTP(132.163.4.101 (tme-a.ttmethq.bldnrc.gov)) US, United States GMP(924.032.02 (ipno-mcast.net)) IP Address not found B/NP(10.0.0.255 ()) IP Address not found SSDP(239.255.255.250 ()) IP Address not found
2 Liste http-Hosts	HTTP(54.68.122.139 (ec2-54-68-122-139.us-west-2.compute.amazonaws.com)) US, United States HTTP(54.68.147.85 (ec2-54-68-147-85.us-west-2.compute.amazonaws.com)) US, United States
3 Liste https-Hosts	-
4 Detailanalyse der Dateninhalte	Verschiedene Parameter wie DeviceID, accessToken, loginName, etc. werden an den Hersteller übertragen. So z.B. beinhaltet der Parameter „device“ den Wert „LTDN50K36WSNEU382“ (vgl. Modellbezeichnung), der an die IP-Adresse 54.68.147.85 gesendet wird.

Bayerisches Landesamt für Datenschutzaufsicht | Seite 14

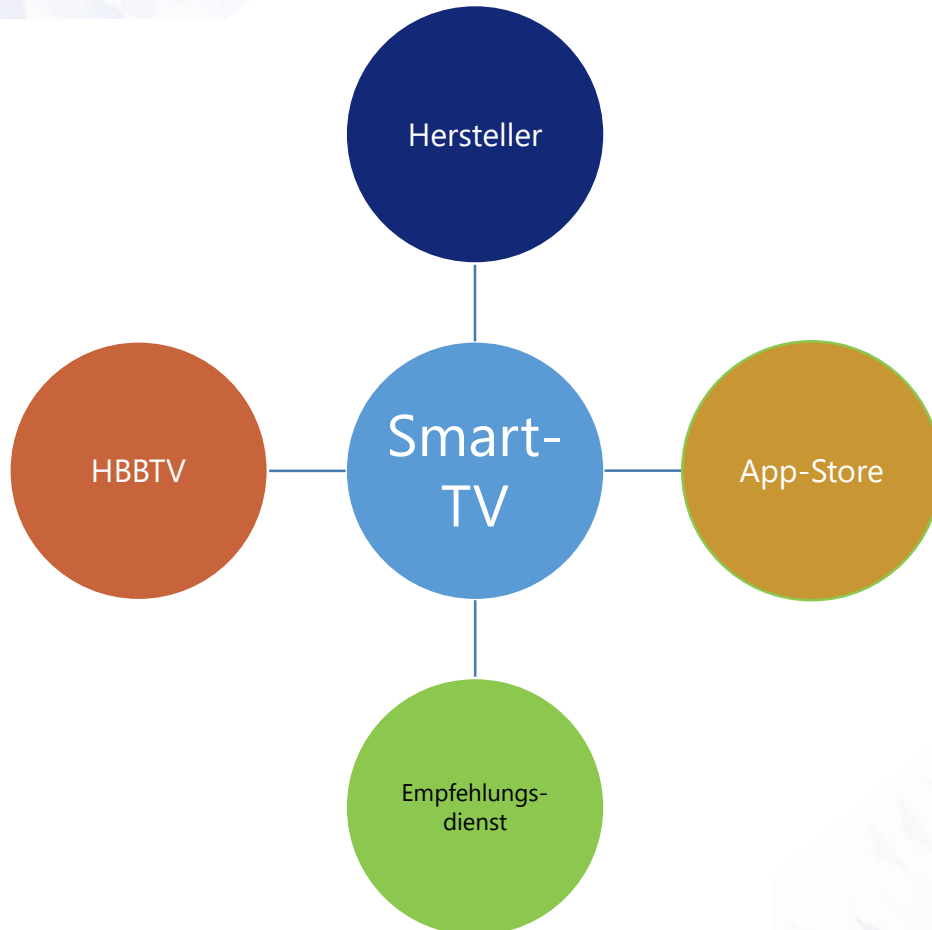
Ziel:

- Qualitätssicherung
- Gemeinsames technisches Verständnis

8

Prüfung: Smart TV und das Ende der Anonymität

Akteure bei Smart-TV



Hersteller: Samsung, LG, Grundig,...

App-Store: Nicht immer gleich Hersteller

Empfehlungsdienst: Nutzungsprofile

HBBTV: Fernsehsender



Aufsichtsbehörden und Smart-TV

- Deutsche Aufsichtsbehörden haben „**Orientierungshilfe Smart-TV**“ herausgegeben
Download (auch) unter:
www.lda.bayern.de/de/orientierungshilfen.html
- Stand heute: Bei den meisten Geräten ist nach einer Internetanbindung kein anonymes Fernsehen mehr möglich. **Ungeklärte Rechtsfrage**: Gilt das TMG automatisch bei HBBTV (Rundfunksignal)

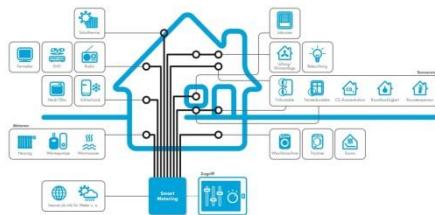
Prüfung: Sind Wearables „kritisch“

- **Aktuelle** Prüfung von Seiten mehrerer Aufsichtsbehörden
- Ziel ist eine relevante **Marktabdeckung** zu erreichen
- **Abgestimmter** Prüfkatalog
- Primäre **dynamische** Analyse
- Ergebnisse sollen im **Dezember 2016** vorliegen
- *Eine zentrale Frage: **Welche** Daten mit erhöhtem Schutzbedarf (Gesundheitsdaten) werden verarbeitet*



Ausblick: Prüfungen morgen?

- **Connected Cars**
- **HTTPS** bei Webseiten
- **Internet der Dinge**
- **Offline Tracking**
- **Smart Home**
- **Ideen?** Bitte Mail an andreas.sachs@lda.bayern.de





Vielen Dank für Ihre
Aufmerksamkeit