

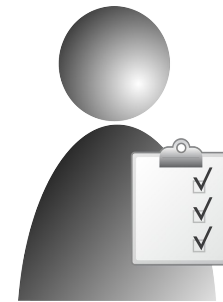
# Watt - wer bist Du denn?

Anonym  
im Internet bewegen mit  
Tails

Cornelius Kölbel  
[cornelius@privacyidea.org](mailto:cornelius@privacyidea.org)  
TÜBIX, 2015

# Beweggründe für Anonymität

- Angst vor Profiling
  - durch Firmen
  - oder Staaten
- Minimieren der Angriffsfläche
  - Keine Personendaten
  - Keine Infrastrukturdaten
- Freie Meinungsäußerung
- Angst vor Massenüberwachung



# Kriminelles Tagesgeschehen

- Sorge nicht unbegründet



# Kriminelles Tagesgeschehen

Bug in iOS ermöglicht abgreifen von Passwörtern.

Seit 5 Monaten.

In Worten „Fünf“.



Newsticker Magazin Fragen & Antworten Jobbörse Shop

Entwicklung ▾ Design ▾ Marketing ▾ E-Commerce ▾ Startups ▾ Software ▾ Infrastruktur

← Vorheriger Artikel

Nächster Artikel →

f 9 likes

27 tweets

share me!

weiterleiten

## iCloud-Phishing: Diese Schwachstelle in Apple Mail ist noch immer nicht gefixt

Eine von einem Entwickler entdeckte Lücke in Apple Mail betrifft Millionen iOS-Nutzer. Obwohl Apple angeblich seit Monaten Bescheid weiß, ist die Schwachstelle noch immer nicht gefixt.

Google-Anzeigen

### Recruiting Videos

Stärkt jetzt Eure authentische Arbeitgebermarke & findet Talente!

[www.whatchado.com](http://www.whatchado.com)

Der Entwickler Jan Soucek hat nach eigenen Angaben vor einigen Monaten eine Schwachstelle in Apples Mail-Client für iPhone und iPad entdeckt, die gewiefte Cyberkriminelle für Phishing-Angriffe auf iCloud-Konten nutzen können sollen. Soucek will das Problem bereits Mitte Januar an Apple gemeldet haben. Einen Fix soll es aber bis heute nicht geben, auch in der aktuellen iOS-Version 8.3 soll die Schwachstelle bestehen.

**Apple Mail: Bug ermöglicht Abgreifen von Passwörtern**



# Kriminelles Tagesgeschehen

Bundestrojaner  
2008-2014

2014:  
Der Bundestrojaner sei  
einsatzbereit.



The screenshot shows the homepage of tagesschau.de with a blue header. The main navigation bar includes links for Startseite, Videos & Audios, Inland (selected), Ausland, Wirtschaft, Wahlarchiv, Wetter, and Ihre Me. Below this, a breadcrumb trail shows Startseite > Inland > NDR: Bundestrojaner ist einsatzbereit. The main article is titled 'Überwachungssoftware des BKA' and 'Bundestrojaner ist einsatzbereit', dated 15.08.2014 05:02 Uhr. It features social media sharing icons for Facebook, Twitter, Google+, Email, and Print. The article text states that the BKA has developed new spyware for monitoring computer programs, based on a request from a member of the Bundestag. It mentions that the software is now ready for use. The article is attributed to Benedikt Strunz from NDR. A sidebar on the right contains a 'VIDEO' section with a link to a video about the Bundestrojaner and a 'MEHR IN' section with a link to a video about the Bundestrojaner.

tagesschau.de

Startseite Videos & Audios Inland Ausland Wirtschaft Wahlarchiv Wetter Ihre Me

■ Startseite ▶ Inland ▶ NDR: Bundestrojaner ist einsatzbereit

Überwachungssoftware des BKA

## Bundestrojaner ist einsatzbereit

Stand: 15.08.2014 05:02 Uhr

[f](#) [t](#) [g+](#) [✉](#) [🖨](#)

Das BKA hat eine neue Software zum Ausspionieren von Computerprogrammen fertiggestellt. Das geht aus einer bislang unveröffentlichten Anfrage des Bundestagsabgeordneten der Linkspartei, Andrej Hunko, hervor, die *NDR Info* vorliegt. In der Antwort des Innenministeriums heißt es, das neue Programm sei ab sofort "einsatzbereit".

Von Benedikt Strunz, NDR

Die neue Spähsoftware erlaubt es Ermittlern, mehrere Programme gleichzeitig auf dem Computer eines Verdächtigen zu überwachen. Der sogenannte Staatstrojaner wird beispielsweise per E-Mail oder USB-Stick auf Rechnern von Verdächtigen installiert. Anschließend können Kriminalbeamte unter anderem Skype sowie Mail- und Chatprogramme des Computers über das Internet überwachen.

**VIDEO**

Benedikt Strunz  
Bundestrojaner  
15.08.2014

Bundesregierung  
Agenda" zu  
tagesschau.de  
Kristin Bopp

**MEHR IN**

[🏠](#)

[👤](#)

[🖥](#)

[👤](#)

[👤](#)

# Kriminelles Tagesgeschehen

## **Musst**

Du was zu erzählen,  
was andere nicht  
mögen?

Foto: Laura Poitras / Praxis Films





# Kriminelles Tagesgeschehen

Erzählst Du **einfach was**, was andere nicht mögen?

Merkel: Deutsche sollen Datenschutz für die Wirtschaft aufgeben.



The screenshot shows the WinFuture website interface. At the top, there are navigation links for 'Login' and 'Registri'. Below the header, there are tabs for 'Startseite', 'Ticker', 'Downloads', 'Videos', 'Forum', and 'Preisvergleich'. Underneath these tabs, there are sub-tabs for 'Wirtschaft', 'Recht, Politik & EU', 'Wirtschaft & Firmen', 'Handel & E-Commerce', and 'P'. The main content area features a headline: 'Merkel: Deutsche sollen Datenschutz für die Wirtschaft aufgeben'. To the left of the headline is a small video thumbnail showing Angela Merkel. To the right of the thumbnail is a text block: 'Bundeskanzlerin Angela Merkel hat die deutsche Bevölkerung aufgefordert, endlich ihre ständigen Datenschutz-Bedenken fallen zu lassen und den Schutz ihrer Privatsphäre der Weiterentwicklung der nationalen Wirtschaft unterzuordnen. Nur so könne man im digitalen Zeitalter international mithalten.' Below the headline, there is a large blue button with a white right-pointing arrow. At the bottom of the page, there is a section titled 'IT-Spezialisten gesucht' with the text 'Zahlreiche offene Stellen Bewerben Sie sich jetzt!'. To the right of this section, there is a small circular progress indicator with two dots, the first of which is filled. At the bottom right, there is a link to an infographic: 'Infografik: Big Data - Das steckt hinter den Mengenangaben Vom Bit zum Yottabyte'.

WinFuture

Login | Registri

Startseite | Ticker | Downloads | Videos | Forum | Preisvergleich

Wirtschaft | Recht, Politik & EU | Wirtschaft & Firmen | Handel & E-Commerce | P

## Merkel: Deutsche sollen Datenschutz für die Wirtschaft aufgeben

Bundeskanzlerin Angela Merkel hat die deutsche Bevölkerung aufgefordert, endlich ihre ständigen Datenschutz-Bedenken fallen zu lassen und den Schutz ihrer Privatsphäre der Weiterentwicklung der nationalen Wirtschaft unterzuordnen. Nur so könne man im digitalen Zeitalter international mithalten.

## IT-Spezialisten gesucht

Zahlreiche offene Stellen Bewerben Sie sich jetzt!

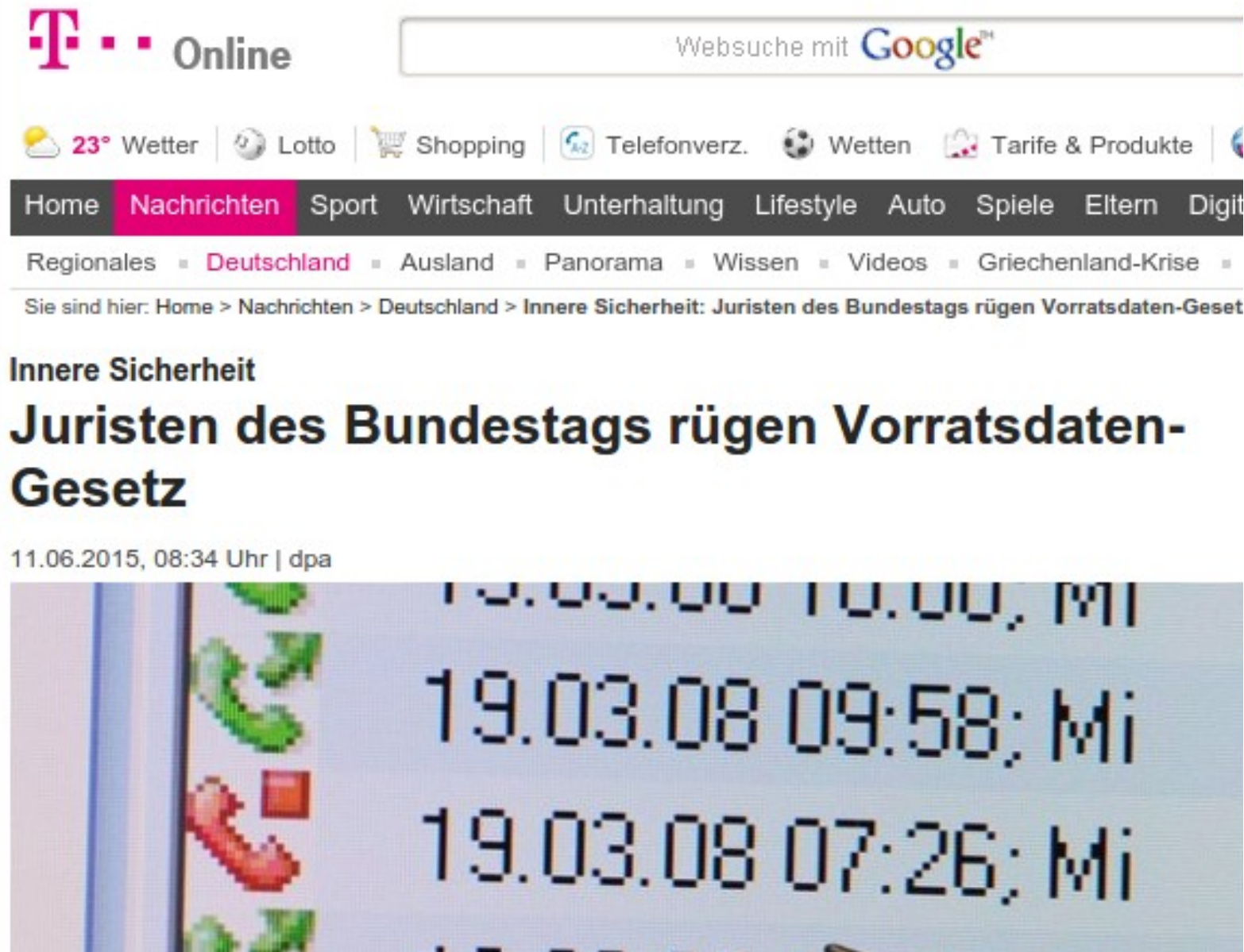
Infografik: Big Data - Das steckt hinter den Mengenangaben Vom Bit zum Yottabyte

Quelle: WinFuture

# Kriminelles Tagesgeschehen

- Anlasslose Massenüberwachung.
- Kriminalisierung

Quelle: T-Online



The screenshot shows the T-Online website interface. At the top, there is a search bar with the text "Websuche mit Google™". Below the search bar, there are several navigation links: "Wetter 23°", "Lotto", "Shopping", "Telefonverz.", "Wetten", and "Tarife & Produkte". The main navigation bar includes "Home", "Nachrichten" (highlighted in pink), "Sport", "Wirtschaft", "Unterhaltung", "Lifestyle", "Auto", "Spiele", "Eltern", and "Digit". Below the navigation bar, there is a breadcrumb trail: "Regionales", "Deutschland", "Ausland", "Panorama", "Wissen", "Videos", "Griechenland-Krise". The main headline reads "Innere Sicherheit" followed by "Juristen des Bundestags rügen Vorratsdaten-Gesetz". The date and time of the article are "11.06.2015, 08:34 Uhr | dpa". The image shows a close-up of a digital display, likely a mobile phone screen, showing a list of dates and times: "19.03.08 09:58; Mi" and "19.03.08 07:26; Mi". On the left side of the display, there are green and red icons, possibly representing a calendar or a list of events.

T-Online

Websuche mit Google™

Wetter 23° | Lotto | Shopping | Telefonverz. | Wetten | Tarife & Produkte

Home | Nachrichten | Sport | Wirtschaft | Unterhaltung | Lifestyle | Auto | Spiele | Eltern | Digit

Regionales | Deutschland | Ausland | Panorama | Wissen | Videos | Griechenland-Krise

Sie sind hier: Home > Nachrichten > Deutschland > Innere Sicherheit: Juristen des Bundestags rügen Vorratsdaten-Gesetz

**Innere Sicherheit**

**Juristen des Bundestags rügen Vorratsdaten-Gesetz**

11.06.2015, 08:34 Uhr | dpa

19.03.08 09:58; Mi

19.03.08 07:26; Mi



# Kriminelles Tagesgeschehen

## Metadaten

"Denn Inhalte sagen, was wir sagen.  
Metadaten aber sagen, war wir tun,  
und was wir denken."

Quelle: Big Brother Awards



*Laudatoren: Kai Biermann und Martin Haase – [Video der Laudatio](#)*

Geheimdienste und Regierungen beteuern immer wieder, dass sie sich nicht für die Daten der Bürger interessieren, sondern „nur“ für die

## Metadaten

als ginge es dabei um völlig Irrelevantes, nachgerade um Datenabfall, der sowieso bei jeder Datenübertragung anfällt und im Gegensatz zu den „richtigen“ Daten nicht besonders schützenswert sei. „Niemand hört mit“, sagte US-Präsident Barack Obama nach Bekanntwerden der Snowden-Dokumente und wollte damit alle beruhigen. Was für eine Lüge.

Das griechische Präfix μετά- bedeutet „nach“ oder „jenseits“, wörtlich sind also Metadaten „Nachdaten“ oder „jenseitige Daten“. Im Deutschen wird das Präfix jedoch meistens verwendet, um anzuzeigen, dass es sich um etwas handelt, das auf einer höheren Abstraktionsebene anzusiedeln ist, in diesem Fall also: Daten über Daten.

# Wunschliste

- Kein mentaler Druck
- Wahrung des Rechts auf Privatheit
- Das soll einfach sein

# Risiken - technisch

- Mapping IP Adresse ↔ Post-Adresse beim Provider
- Email i.d.R. nicht verschlüsselt
  - Transport-Verschlüsselung vs. Ende-zu-Ende
    - DE-Mail
    - STARTTLS (starttls.info)
    - PGP, S/MIME, x.509

Does your mail server support **STARTTLS**?  
If you care about privacy, it should. Read more in the [blog](#).

Results for: bundestag.de [↻](#)

Mail server	Result
mail1.dbtg.de	Error: The server rejected our test
mail4.dbtg.de	Error: The server rejected our test
mail2.dbtg.de	Error: The server rejected our test
mail3.dbtg.de	Error: The server rejected our test

Click the score for details. [Test another!](#)

[About StartTLS.info](#) | [Issue tracker](#) | Check the [stats](#)

Developed by [Einar Otto Stangvik](#).



# Risiken - technisch

- Alte, fehlerhafte Software.
  - Anonymität im Internet vs. Trojaner auf Rechner
- Cookies
  - Erkennen uns, wenn wir wiederkommen (Google)
- LSO (Local Shared Object), Flash Cookies
  - Flash speichert bis zu 100KB lokal per App
- HTTP!s
  - Auch Inhaltsdaten sind einsehbar

# Risiken - technisch

- Browser
  - Identifier, Version, Betriebssystem, Größe des Fensters → Desktop-Größe → Profiling

# Anonym? Pseudonym!

- Anonymität schwer zu erreichen
- Oft erreicht man nur Pseudonymität
  - Google
  - IP-Adresse
  - Foren
  - IRC
  - Email
- Für Anonymität müssten alle User gleich sein.





# Wunschliste

- Kein mentaler Druck
- Wahrung des Rechts auf Privatheit
- Das soll einfach sein

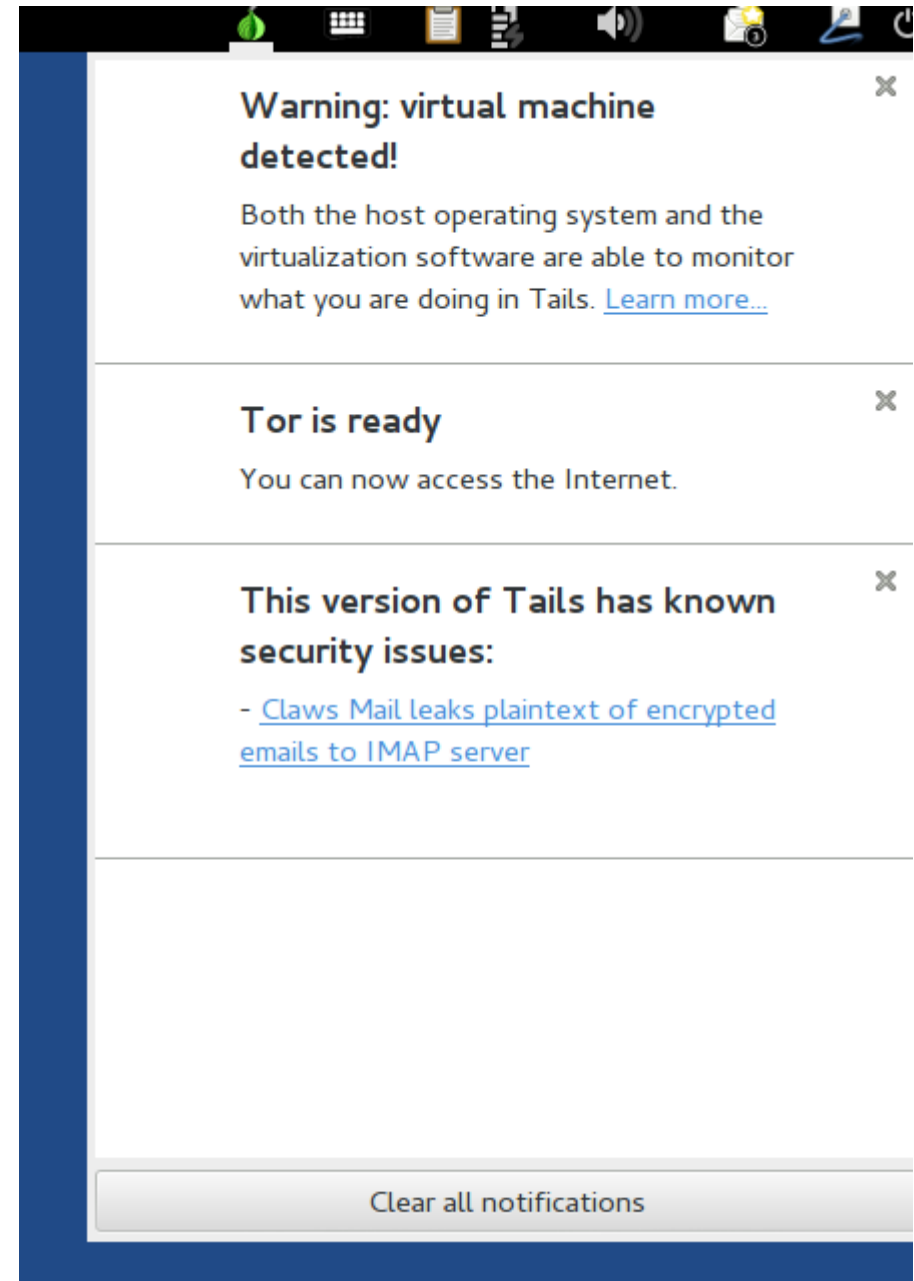


# Tails

- The
- Amnesic
  - RAM wipe, vergisst, was man gemacht hat
- Incognito
  - „unbekannt, unter fremden Namen“ (Meyers Grosses Taschen Lexikon)
- Live
  - Muss nicht installiert werden
- System
  - Eigenes Betriebssystem

# Tails - Basis

- Basiert auf Debian 7
- Live per CD oder USB (persistent volume)
- Weist auf bekannte Schwachstellen hin
- RAM Wipe beim Shutdown





# Tails – persistent Volume

- Persistent Volume verschlüsselt eigene Daten, SSH Keys, GPG Keys, KeePassX...
- Allerdings nur, wenn das System von USB-Stick oder SD-Karte läuft
  - Dann kann es aber auch modifiziert werden
- Da das System aber offline in der Hosentasche steckt, ist es „besser“ als LUKS

# Tails - Internet

- TOR
- Angepasster Firefox
  - NoScript
  - Tor
  - DisconnectMe
  - HTTPS Everywher
  - Browser Maximize Warnung

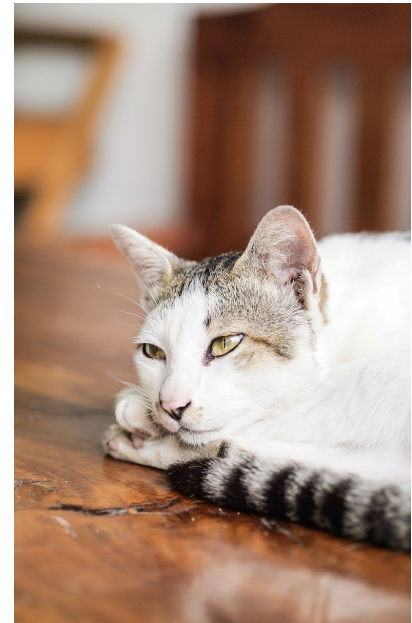
# Tails - Internet

- IRC
  - Namensänderung
- DNS (durch TOR)
  - Schützt falschen DNS-Einträgen oder DNS-Websperren  
**lol**
  - Kein LAN sinnvoll möglich
- Claws + GnuPG
  - Mails können im verschlüsselten, persistenten Bereich abgelegt werden.



# Tails – Probleme

- **Claws** – IMAP Security Issue
  - Entweder POP3 oder Migration Thunderbird
- **UEFI** – unterstützt kein Secure Boot
- OS auf USB-Stick ist veränderbar
- Schützt nicht vor HW-Keyloggern.
  - Aber will man Tails nicht gerade an fremden Computern verwenden?



# Tails – Résumé 1/3

- Versammelt gute Tools und
- Gute Ideen
  - RAM Wipe
  - Persistent container (enc)
- Nicht fürs tägliche Arbeiten



# Tails – Résumé 2/3

- Für Reisen und fremde Computer?
  - Möglich aber suboptimal (UEFI, OS änderbar, HW-Keylogger)
- Gut für gezielten Einsatz wenn man
  - Verschlüsselt,
  - pseudonym und
  - Rückstandsloskommunizieren möchte. An vertrauenswürdiger Hardware.

# Tails – Résumé 3/3

- Es bringt uns bei, worauf wir achten sollten/können:
  - Browser Profiling
  - Verschlüsselung
  - RAM (Shutdown vs. Hibernate)
- **Wir sind nicht machtlos sondern machtvoll!**



# Nicht nur technische Lösungen

## S.P.O.N. - Die Mensch-Maschine: Sie haben die Zukunft verbockt

Eine Kolumne von *Sascha Lobo*



DPA

Laptop- und Smartphone-Nutzer: Ein substantieller Teil des Lebens findet im und mit dem Netz statt

**Die deutsche Digitalpolitik ist eine Katastrophe. Und Sie sind schuld daran. Sie lassen sich alles bieten und wählen weiter die gleiche Partei. Als Bürger haben Sie versagt.**

1 Mittwoch, 10.06.2015 – 16:27 Uhr

Drucken | Senden

i Nutzungsrechte | Feedback

! Kommentieren | 298 Kommentare

**Sascha Lobo**



### Kolumne

Deutschland ist noch weniger als ein digitales Entwicklungsland, Deutschland ist ein Digitally Failed State. Und Sie tragen die Schuld. Sie, der Durchschnittsbürger. Eigentlich sind die Bürger, die Wählerschaft, das Publikum der Mittelpunkt der Medienlandschaft wie auch der der Demokratie. Leute also, die man nicht beschimpfen sollte. Aber ich halte es für notwendig, dass Sie Ihr fundamentales Versagen durch Nichtstun begreifen.

Es ist einfach, auf die böse Politik zu schimpfen, und das tun Sie ja auch. Aber es handelt sich um substanzloses Gemoser, denn Ihrem Unmut lassen Sie keinerlei Konsequenzen folgen. Sie sagen "Man kann ja nichts tun!", um anschließend nichts zu tun. Sie wählen weiter die gleiche Partei, Sie gehen nicht auf die Straße, Sie engagieren sich nicht. Ihre Beschwerde hat nämlich nicht das Ziel irgendetwas zu ändern sondern



# Ausklang

Danke für die Aufmerksamkeit

Danke für die Bilder von Pixabay an:

- openclipartvectors
  - geralt
- ClkerFreeVectorImages
  - thichinajack
  - levellord