

# NSA, Prism und co - Wie schützt man sich vor Überwachung?

Marius Melzer & Stephan Thamm  
Chaos Computer Club Dresden

22.01.2014





# Wer sind wir?



# Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)



# Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
- Datenspuren: Herbst 2014 <http://datenspuren.de>



# Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
- Datenspuren: Herbst 2014 <http://datenspuren.de>
- Podcasts (<http://pentamedia.de>)



# Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
- Datenspuren: Herbst 2014 <http://datenspuren.de>
- Podcasts (<http://pentamedia.de>)
- Chaos macht Schule



# Bundespräsident Gauck zur NSA-Überwachung

"Wir wissen z.B., dass es nicht so ist, wie bei der Stasi und dem KGB, dass es dicke Aktenbände gibt, wo unsere Gesprächsinhalte alle aufgeschrieben und schön abgeheftet sind. Das ist es nicht."





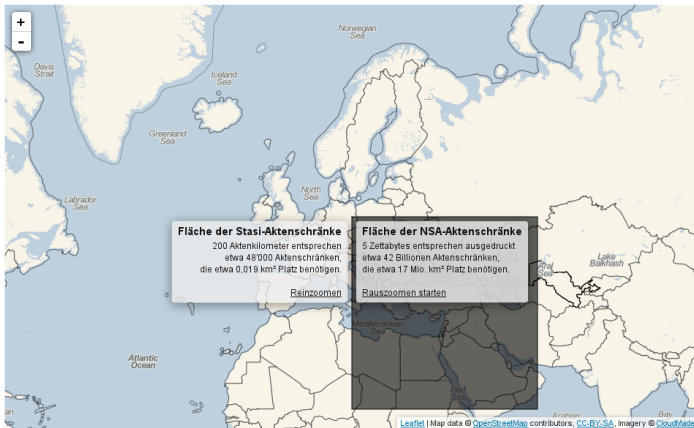
# Stasi vs. NSA



Realisiert von [OpenDataCity](#). Anwendung steht unter [CC-BY 3.0](#).



# Stasi vs. NSA



Realisiert von [OpenDataCity](#). Anwendung steht unter [CC-BY 3.0](#).



# Merkels Handy

## News

[Newsticker](#) [7-Tage-News](#) [Archiv](#) [Foren](#)Themen: [NSA](#) [Xbox](#) [Playstation 4](#) [Windows 8.1](#) [VDSL](#) [iPad](#) [iPhone](#) [Android](#) [Google Nexus](#)[heise online](#) > [News](#) > [2013](#) > [KW 48](#) > NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

26.11.2013 09:43



### NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

[vorlesen](#) / [MP3-Download](#)

Angela Merkel wurde in ihrer Amtszeit als Bundeskanzlerin nicht nur von der NSA, sondern auch den Geheimdiensten Russlands, Chinas, Nordkoreas und Großbritanniens abgehört. [Das berichtete](#) der Focus am Sonntag unter Berufung auf eine nicht näher erläuterte Analyse deutscher Sicherheitsbehörden. Hilfreich bei den Angriffen [auf das ungesicherte Handy](#) der Kanzlerin sei das weitläufige Regierungsviertel in Berlin, das sich hervorragend für die Funkspionage eigne, wird ein hochrangiger Sicherheitsbeamter zitiert.

Dem Bericht zufolge arbeiten alleine für Russland 120 Geheimdienstler in Deutschland und spähen die Bundesrepublik aus. Offiziell eingesetzt würden sie von der russischen Botschaft. Weiterhin hätten ausländische Geheimdienste in den vergangenen Jahren versucht, mehr als 100 deutsche Politiker, Beamte, Militärs, Manager und Wissenschaftler als Quellen anzuwerben. Das sei aber nur die Zahl derer, die sich danach bei deutschen Behörden gemeldet hätten, die tatsächliche Dunkelziffer sei unbekannt, aber wohl beträchtlich.

### Top-News

[Rätselhafte Entführungen im Internet](#)[Ungewisse Zukunft für Windows RT](#)[Satelliten made in Germany](#)[NSA soll 75 Millionen US-Dollar zum Schutz vor Whistleblowing erhalten](#)[Große Koalition setzt auf intelligente Stromzähler](#)

### Videos bei heise online

[1](#) [2](#) [3](#) [4](#) [5](#)

#### c't zockt (Episode 23)

Diesmal: Tower-Defence-Spiel "Kingdom", Japan-Gruseler "Run into the Dark" und "Code Combat".



#### heise open

##### Zehn Jahre bei Fedora

Bei der Mitarbeit an einer Linux-



# Tempora



## Netz-Spähsystem Tempora: Der ganz große britische Bruder



DPA/ dpa/ VIKI/ regentsucher.com

Mehr als 200 Glasfaserkabel sollen die Briten angezapft haben

**Das umstrittene US-Spähprogramm Prism? Ist harmlos im Vergleich dazu, in welchem Umfang ein britischer Geheimdienst unter dem Codenamen Tempora weltweit das Internet ausspioniert - und damit auch deutsche Nutzer. Doch selbst Datenschutzaktivisten halten das Vorgehen für legal.**

Samstag, 22.06.2013 - 19:24 Uhr

Drucken | Versenden | Markieren

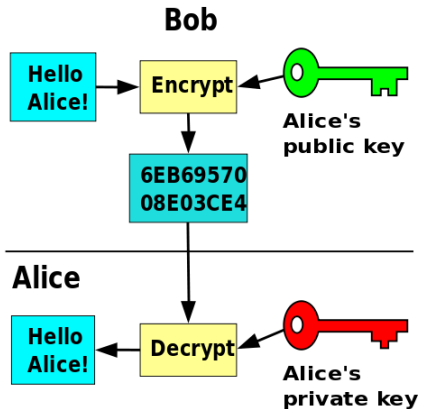
Nutzungsrechte | Feedback

Kommentieren | 189 Kommentare

Hamburg/London - Die Aufregung war riesig, als bekannt wurde, dass die National Security Agency (NSA) im Rahmen ihres unter US-Präsident Barack Obama initiierten Spähprogramms Prism die Kunden von Telefon- und Internetfirmen ausleuchtet - Big Barack is watching you. Doch Brit Brother tut genau dies auch. Und in mancher Hinsicht scheint die Überwachung durch die britischen Netzspläne viel umfassender zu sein als die der Amerikaner.



# Verschlüsselung



# SSL / TLS



# SSL / TLS

- SSL = Secure Socket Layer



# SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...





# SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...
- hierarchische Struktur

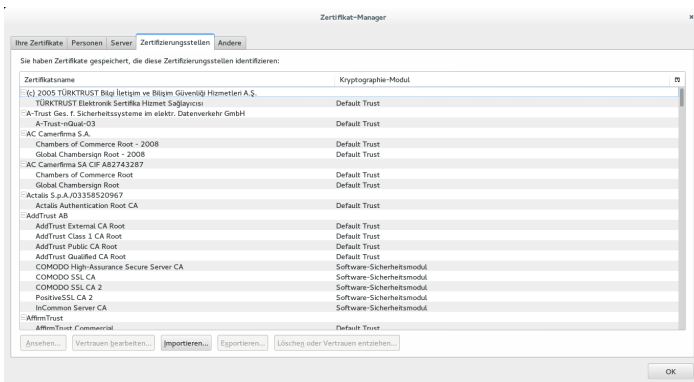


# SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...
- hierarchische Struktur
- gespeicherte Liste von vertrauenswürdigen Zertifikaten



# Von Firefox vertraute Zertifikate



# HTTPS Everywhere

**ELECTRONIC FRONTIER FOUNDATION**  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

HOMEABOUTOUR WORKDEEPLINKS BLOGPRESS ROOMTAKE ACTIONSHOP



## HTTPS Everywhere

**HTTPS Everywhere**  
FAQ  
Report Bugs / Hack On The Code  
Creating HTTPS Everywhere Rulesets  
How to Deploy HTTPS Correctly

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

**Install in Firefox**  
Version 3 Stable

**Install in Chrome**  
Beta Version

**Install in Opera**  
Beta Version

**Donate to EFF** 

**Stay in Touch**  
Email Address   
Postal Code (optional)   
**SIGN UP NOW**

**NSA Spying**  
 [eff.org/nsa-spying](http://eff.org/nsa-spying)  
EFF is leading the fight against the NSA's (regrettable) eavesdropping program. [Learn more](#) about how this program is, how it works, and what you can do.



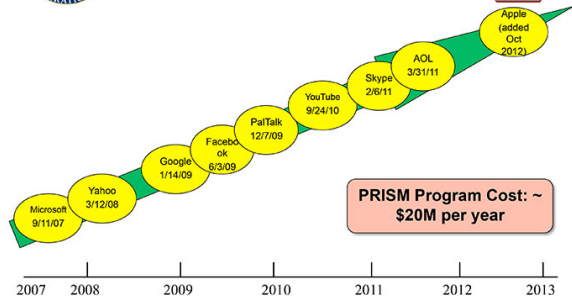
# Prism

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF)

Dates When PRISM Collection  
Began For Each Provider



PRISM Program Cost: ~  
\$20M per year

TOP SECRET//SI//ORCON//NOFORN



# Dezentrale Dienste



# Dezentrale Dienste

- Email



# Dezentrale Dienste

- Email
- Jabber





# Dezentrale Dienste

- Email
- Jabber
- Bitmessage



# Dezentrale Dienste

- Email
- Jabber
- Bitmessage
- palava.tv



# Lavabit

[heise online](#) > [News](#) > [2013](#) > [KW 32](#) > Lavabit: E-Mail-Anbieter von Edward Snowden schließt

09.08.2013 09:12  « [Vorige](#) | [Nächste](#) »

## Lavabit: E-Mail-Anbieter von Edward Snowden schließt und protestiert

 [vorlesen](#) / [MP3-Download](#)

Der US-amerikanische E-Mail-Anbieter Lavabit, der bekannt geworden war, weil der NSA-Whistleblower Edward Snowden [ihn benutzt hat](#), wurde [dicht gemacht](#). Ladar Levison, der Chef des Dienstes, der verschlüsselte Kommunikation anbietet, erklärte, er könne sich entweder an Verbrechen gegen US-Amerikaner beteiligen oder das Ergebnis zehn Jahre harter Arbeit aufgeben. Er habe sich für das zweite entschieden. Ihm sei es aber gesetzlich verboten, mitzuteilen, was ihn zu diesem Schritt bewogen hat. Vor der Schließung hatte Lavabit etwa 350.000 Nutzer und es konnten kostenlose aber auch kostenpflichtige Accounts eingerichtet werden, [berichtete](#) Ghacks.

Levison erwähnt in dem Statement seine Erfahrungen der "vergangenen sechs Wochen", auf die er nicht eingehen dürfe, obwohl er zwei Anfragen gestellt habe. Es liegt nahe, dass US-Behörden Druck ausgeübt haben, etwa um einen Zugang zu



# Ende-zu-Ende-Verschlüsselung I

- Email: GPG = Gnu Privacy Guard
- Thunderbird: Enigmail
- Outlook: Gpg4win
- Web: Mailvelope (Firefox, Chrome)
- Alternative: Bitmessage



# Ende-zu-Ende-Verschlüsselung II



# Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - GibberBot oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS



# Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - GibberBot oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie



# Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - GibberBot oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefonate (Android)





# Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - GibberBot oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefonate (Android)
- TextSecure für SMS (Android)



# Vorratsdatenspeicherung (Deutschland)

Alle | Shop | E-Paper | Apps | Audio | Anzeig. | Support

ZEIT ONLINE | DEUTSCHLAND

ZEIT ONLINE durchsuchen

Start | Politik | Wirtschaft | Meinung | Gesellschaft | Kultur | Wissen | Digital | Studium | Karriere | Lebensart | Reisen | Mobilität | Sport

Start | Politik | Wirtschaft | Meinung | Gesellschaft | Kultur | Wissen | Digital | Studium | Karriere | Lebensart | Reisen | Mobilität | Sport

Anmelden | Registrieren

## Maas bereitet Vorratsdatenspeicherung vor

Der Justizminister löste einen Koalitionskrach aus, als er die Vorratsdatenspeicherung "auf Eis" legte. Nun beginnt er laut einem Bericht doch schon mit der Umsetzung.

VON SÖHNE CALLSEN

16. Januar 2014 17:32 Uhr

17 KOMMENTAR | 1



Erstreckung des Netzlaufs bei der Vorratsdatenspeicherung

5. ANZEIGE: ZEIT ONLINE

8. KOLLEKTIV: Vorratsdatenspeicherung | Heiko Maas | Enklopädie: Gerichte | Justiz | Justiz | Hans-Peter Uhl

NEU AUF ZEIT ONLINE

1. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
2. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
3. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
4. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
5. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
6. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung

NEU IM RESSORT

1. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
2. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
3. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
4. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
5. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung
6. KOLLEKTIV: Die Minister des Problems in der Gesetzgebung

EMPFEHLUNGEN BEI FACEBOOK

Hier werden aktuelle Empfehlungen aus Ihrem Facebook-Freundeskreis angezeigt.

Aus Datenschutzgründen werden diese erst geladen, wenn Sie die Social Media Dienste aktiviert haben. Bitte beachten Sie, dass nach Ihrer Zustimmung Daten mit anderen externen Diensten ausgetauscht werden.

ZEIT ONLINE auf Facebook



# Vorratsdatenspeicherung (USA)

[Home](#)[Über uns](#)[Kontakt](#)[Podcast](#)[Netzpolitik TV](#)[Facebook](#)[Youtube](#)[Twitter](#)[RSS](#)VERMARKET VON  
ZEIT ONLINE

## US-Geheimdienst NSA der geheimen Vorratsdatenspeicherung überführt

Von Markus Beckedahl | Veröffentlicht: 06.06.2013 um 7:51h | 1 Antwort

Was der US-Geheimdienst National Security Agency (NSA) alles überwacht, ist in der Regel Spekulation. Weil dieser im Geheimen agiert. Es wird vermutet, dass die NSA als eine Art Staubsauger sehr viele öffentlich im Netz fluktuierende Daten sammelt und speichert. Aber da die NSA im geheimen operiert, fällt es in der Regel schwer, etwas zu beweisen.

Der Journalist Glenn Greenwald schreibt im britischen Guardian über eine als geheim klassifizierte [Verordnung des Foreign Intelligence Surveillance Court \(FISC\)](#), die der Guardian auch veröffentlicht hat: [NSA collecting phone records of millions of Americans daily - revealed](#). In dieser wird der US-Provider Verizon angewiesen, eine Vorratsdatenspeicherung für drei Monate durchzuführen. Und zwar für lokale, nationale und ausländische Verbindungen mit allem, was dazu gehört. Es wird spekuliert, dass eine solche Verordnung regelmäßig erneuert und zudem nicht nur an Verizon verschickt wird.

Die Electronic Frontier Foundation (EFF) berichtet darüber: [Confirmed: The NSA is Spying on Millions of Americans](#).

### Suchen

Suchen

### Über uns

netzpolitik.org ist ein Blog und eine politische Plattform für Freiheit und Offenheit im digitalen Zeitalter.

### Blog abonnieren

netzpolitik.org Blog Feed

### Spenden

netzpolitik.org produziert eine Reihe kostenloser Inhalte. Eine Spende erhält das Projekt am Leben und ermöglicht uns einen Ausbau der Redaktion.

Unser Bank-Konto (ohne Gebühren)

Inhaber: netzpolitik.org e. V.



# Metadaten



# Metadaten

- Handynet



# Metadaten

- Handynetz
  - Telefonnummern



# Metadaten

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)



# Metadaten

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)





# Metadaten

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)
- Internet



# Metadaten

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)
- Internet
  - IP-Adresse



# Metadaten

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)
- Internet
  - IP-Adresse
  - Alle Verbindungen

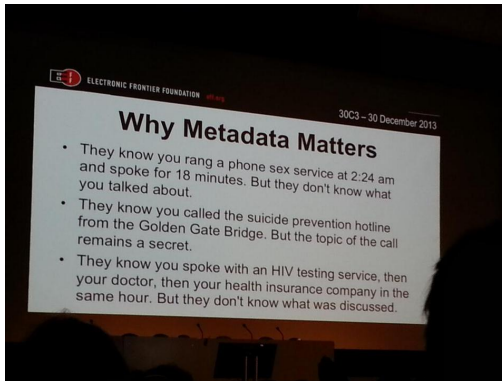


# Metadaten

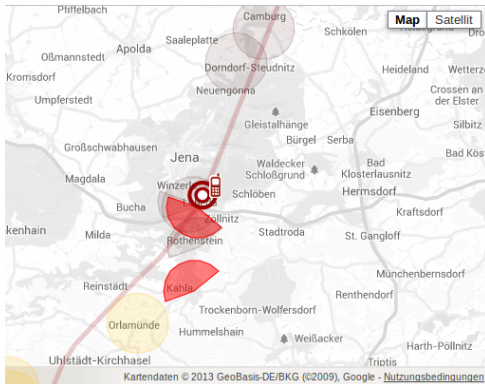
- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)
- Internet
  - IP-Adresse
  - Alle Verbindungen
  - Email: Adressen von Sender und Empfänger, Zugriff



# Metadaten



# Metadaten



speed + 31 Aug 09 15:30

Show the points in time, Malte Spitz was in the selected map segment, too

**Monday, 31 August 2009**

**i** Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.  
(source: [Parteiwebsite](#))

**📞** 6 incoming calls  
21 outgoing calls  
total time: 1h 16min 8s

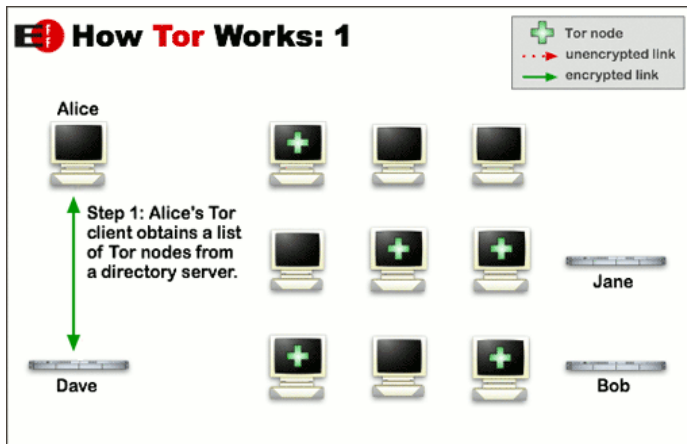
**SMS** 34 incoming messages  
29 outgoing messages

**🌐** duration of internet connection:  
21h 17min 25s

Download Data



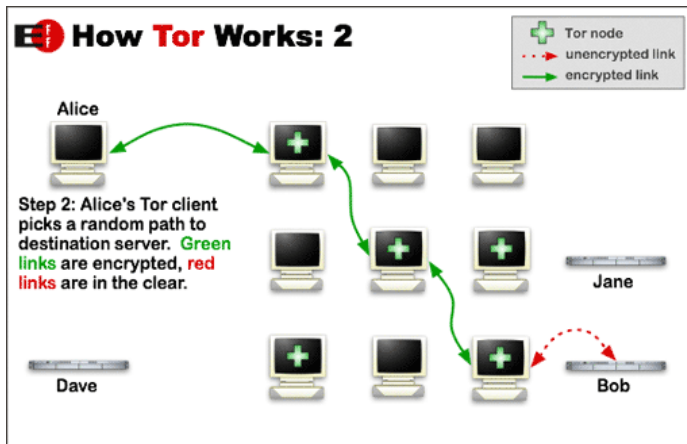
# Tor



Grafik:  The Tor Project



# Tor

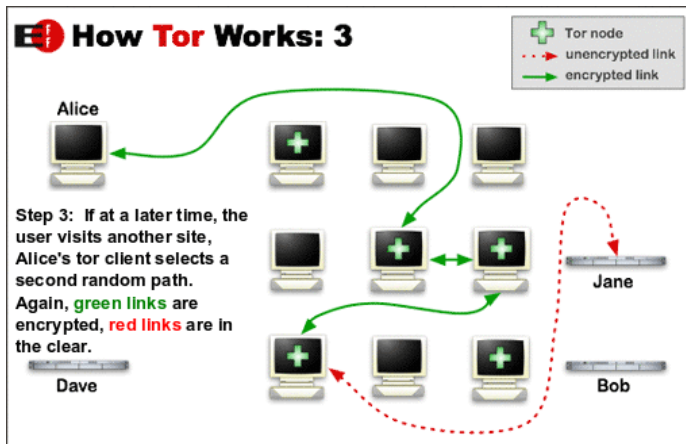


Grafik:  The Tor Project





# Tor



Grafik:  The Tor Project



# Datensparsamkeit



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
  - Pseudonymität



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
  - Pseudonymität
  - mailinator.com



# Passwörter





# Passwörter

- Keine einfachen Wörter



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.§Tsm!f



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.§Tsm!f
  - IchLiebeDich



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.§Tsm!f
  - IchLiebeDich
  - .§)=")=‘



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.ξTsm!f
  - IchLiebeDich
  - .ξ)=")=‘
  - 123456





# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.ξTsm!f
  - IchLiebeDich
  - .ξ)=")=‘
  - 123456
  - qwerty



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.§Tsm!f
  - IchLiebeDich
  - .§)=")=‘
  - 123456
  - qwerty
  - Mks?o/.u,1Psw!



# Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
  - dragon
  - (nCuaJ.ξTsm!f
  - IchLiebeDich
  - .ξ)=")=‘
  - 123456
  - qwerty
  - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!



# Wie schütze ich meinen Computer?

- Virens Scanner
- Firewall
- Aktuelle und vertrauenswürdige Software






# Wie schütze ich mein Smartphone?









- Permissions
- Firewall (z.B. AFWall+: <https://f-droid.org/repository/browse/?fdid=dev.ukanth.ufirewall>)
- Aktuelle und vertrauenswürdige Software



# Freie Software

https://prism-break.org/en/   Google

PRISM  BREAK Platforms [Protocols](#)

Mobile	 <a href="#">Android</a> >
	 <a href="#">iOS</a> >
Computer	 <a href="#">BSD</a> >
	 <a href="#">GNU/Linux</a> >
	 <a href="#">OS X</a> >
	 <a href="#">Windows</a> >
Network	 <a href="#">Routers</a> >
	 <a href="#">Servers</a> >

Opt out of global programs like PRISM and Tempora.

Stop governments from spying on your communications and using proprietary services.



# Freie Software

https://prism-break.org/en/categories/android/

Operating Systems

Proprietary	Free Recommendations
BlackBerry	<b>CyanogenMod</b> Aftermarket firmware for Android devices.
Google Android	<b>Firefox OS</b> Open source operating system for And...
Microsoft Windows Phone	<b>Replicant</b> Fully free Android distribution based o...

Productivity

Proprietary	Free Recommendations
Doodle	<b>dudle</b> A free online poll with an optional priva... Web Service
Evernote	<b>EtherCalc</b> Multi-user spreadsheet server. Web Service
Microsoft Office Web A...	<b>Etherpad</b> Self-hosted, real-time collaborative doc... Web Service
Zoho Office Suite	<b>ProtectedText</b> Free online encrypted notepad. Web Service
	<b>Riseup</b> Secure communication tools for peopl... Web Service

Categories

- Anonymizing Networks
- App Store
- DNS
- Email Accounts
- Email Clients
- Email Encryption
- File Storage & Sync
- Finance
- Instant Messaging
- Media Publishing
- Mesh Networks
- Operating Systems
- Productivity
- Social Networks
- Video & Voice
- VPN Accounts
- VPN Clients
- Web Browser Addons
- Web Browsers
- Web Hosting
- Web Search
- World Maps



# Diskussion

## Diskussion

Marius Melzer und Stephan Thamm

CMS Dresden: schule@c3d2.de

