



Themenabend der Braunschweiger Linux-User-Group

Digitale Selbstverteidigung

2019



Themenabend: Digitale Selbstverteidigung Vorstellung

Ein Vortrag
von
Marius Schwarz



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Internetanbieter verlieren öfters mal Ihre Daten an Dritte,



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Internetanbieter verlieren öfters mal Ihre Daten an Dritte,
gern auch absichtlich.



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Facebook: Nächster Skandal? Millionen Passwörter unverschlüsselt gespeichert

FOCUS Online • Vor 2 Tagen



Zahlungsdaten, Passwörter...alles: Gearbest-Kundendaten offen im Netz

WinFuture • Vor 8 Tagen

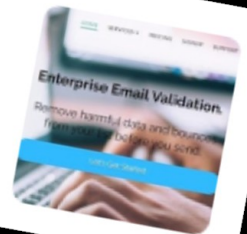
E-Mail-Marketing: Datenbank mit 800 Millionen E-Mail-Adressen online - Golem.de

Golem.de • Vor 13 Tagen



Passwort-Leaks weiten sich aus: Inzwischen 2,2 Milliarden Zugangsdaten betroffen

t3n Magazin • 28. Jan.



Aldi Talk: Passwörter im Klartext gespeichert?

e-Recht24.de • Letzter Monat



Datenschutz - Was Facebook mit Ihrer Handynummer anstellt

Süddeutsche Zeitung • Vor 19 Tagen





Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Was können Sie dagegen tun ?



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Ganz einfach:

Passwörter und Emailadressen **nicht mehrfach** verwenden.



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Ganz einfach:

Passwörter und Emailadressen **nicht mehrfach** verwenden.

... und lügen, bis die Schwarte kracht!



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Bei EMailadressen ist das mit einer
eigenen Domain
ganz einfach.



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Weiterleitungen auf eine Hauptadresse

Bestehende Weiterleitungen

[?](#) (Hilfe)

E-Mail-Adresse	Zieladresse	
artikel13@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
ebayusergerd@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
Ebooks4free@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
facebook@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
finanzamt@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
hertie@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
kontakt@notls.de	<input type="text" value="support@evolution-hosting.eu"/>	<input type="button" value="Entfernen"/>
mozilla@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
youtubechannelalpha@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>
zalando@notls.de	<input type="text" value="kontakt@notls.de"/>	<input type="button" value="Entfernen"/>



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Passwörter

Eigenes Passwort für **jeden** Dienst benutzen.



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Passwörter

Eigenes Passwort für **jeden** Dienst benutzen.

FireFox hilft



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Firefox hilft

Datenschutz & Sicherheit

Zugangsdaten & Passwörter

Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen

Master-Passwort verwenden

[Ausnahmen...](#)

[Gespeicherte Zugangsdaten...](#)

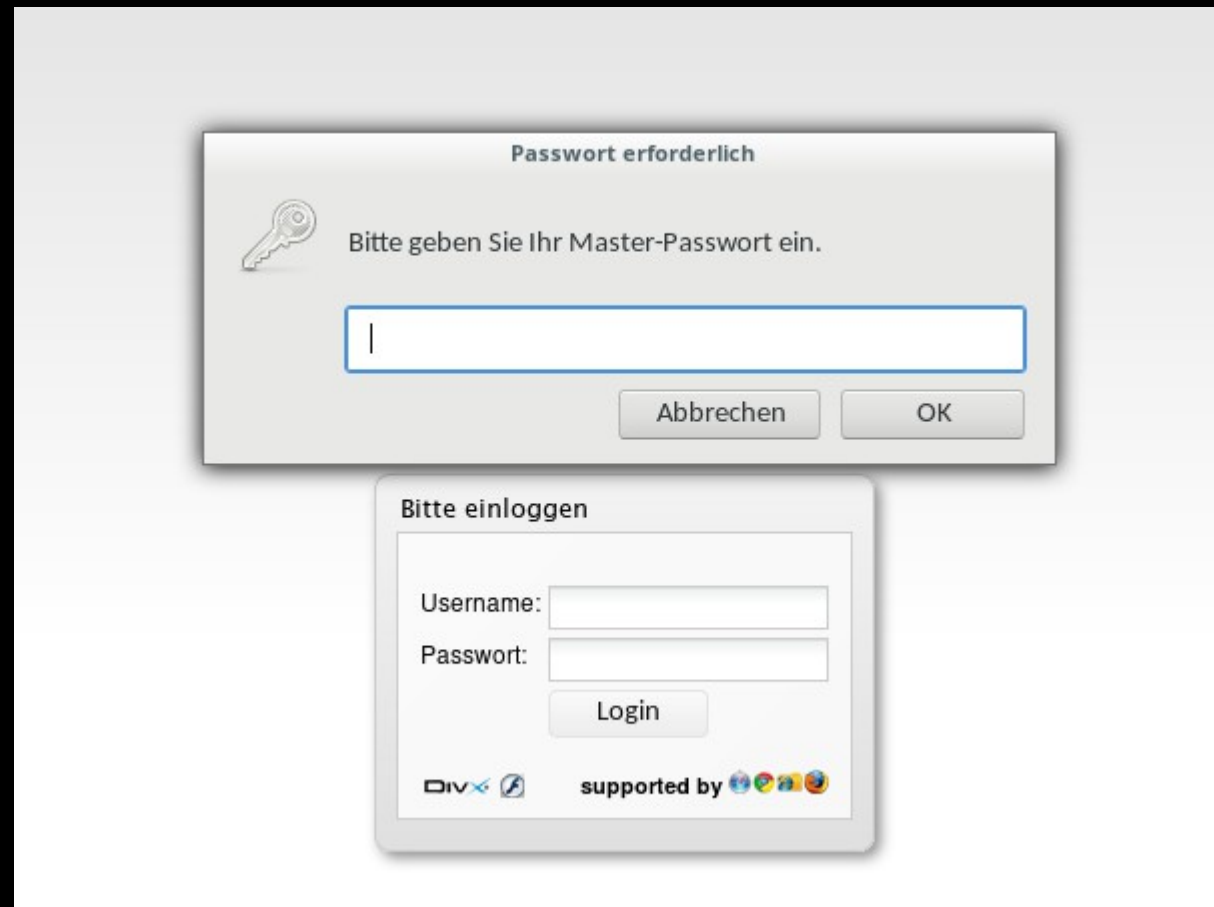
[Master-Passwort ändern...](#)



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

Firefox hilft





Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten

... oder ...



Themenabend: Digitale Selbstverteidigung

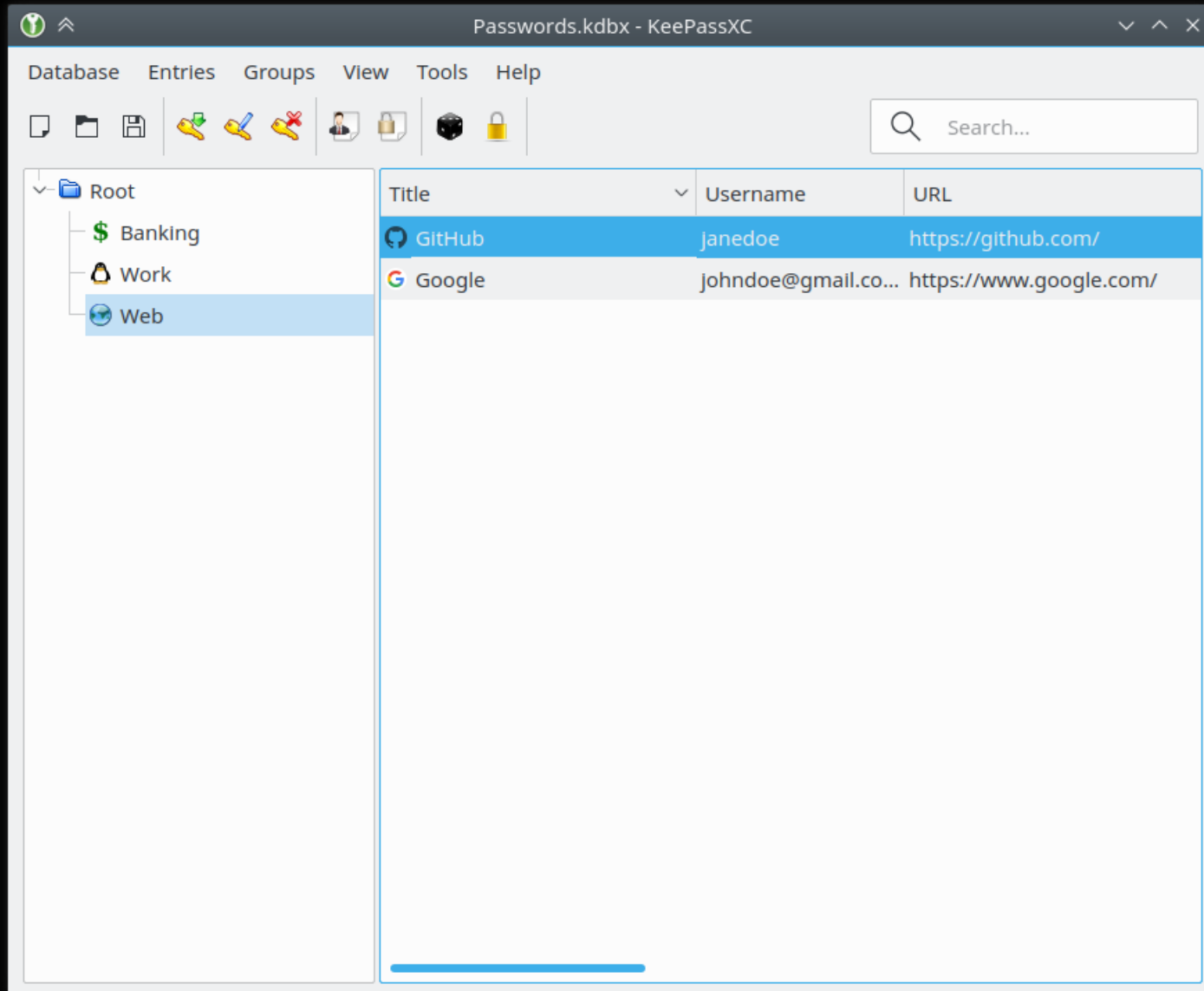
Kapitel 1: Datenbefreiung bei Webdiensten

... einen Passwort-Manager benutzen !



Themenabend: Digitale Selbstverteidigung

Kapitel 1: Datenbefreiung bei Webdiensten



KeyPassX – Passwordmanager

Alle Passwörter an einem Platz,
übersichtlich sortiert,
durch Verschlüsselung geschützt.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Kapitel 2:

Der Kampf gegen die Meinungsfreiheit



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

EU Urheberrechtsreform

&

EU Verordnung zur Verhinderung terroristischer Online-Inhalte



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Was haben die beiden Projekte gemeinsam?



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Was haben die beiden Projekte gemeinsam?

Wer weiß es !?!



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Uploadfilter !



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Was machen Uploadfilter ?



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Jedes Wort,
jeden Ton,
jedes Bild
und jedes Video
analysieren.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Was haben solche Algorithmen nicht ?



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Was haben solche Algorithmen nicht ?

Verstanden, was sie da analysieren.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Folge:

„ungewollte“ Unterdrückung von Medien und Meinungen.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Beispiel:

Sie fertigen mit Bildmaterial eines Fernsehsenders eine Kritik einer politischen Aussage an und laden diese vor einer Wahl auf YouTube hoch.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Beispiel:

Sie fertigen mit Bildmaterial eines Fernsehsenders eine Kritik einer politischen Aussage an und laden diese vor einer Wahl auf YouTube hoch.

Sie dürfen das laut **Zitaterecht**,
wenn es eine Auseinandersetzung mit dem Inhalt ist.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Nur weiß das der Upload-Filter nicht,
weil er das nicht beurteilen kann.



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Lösungen:

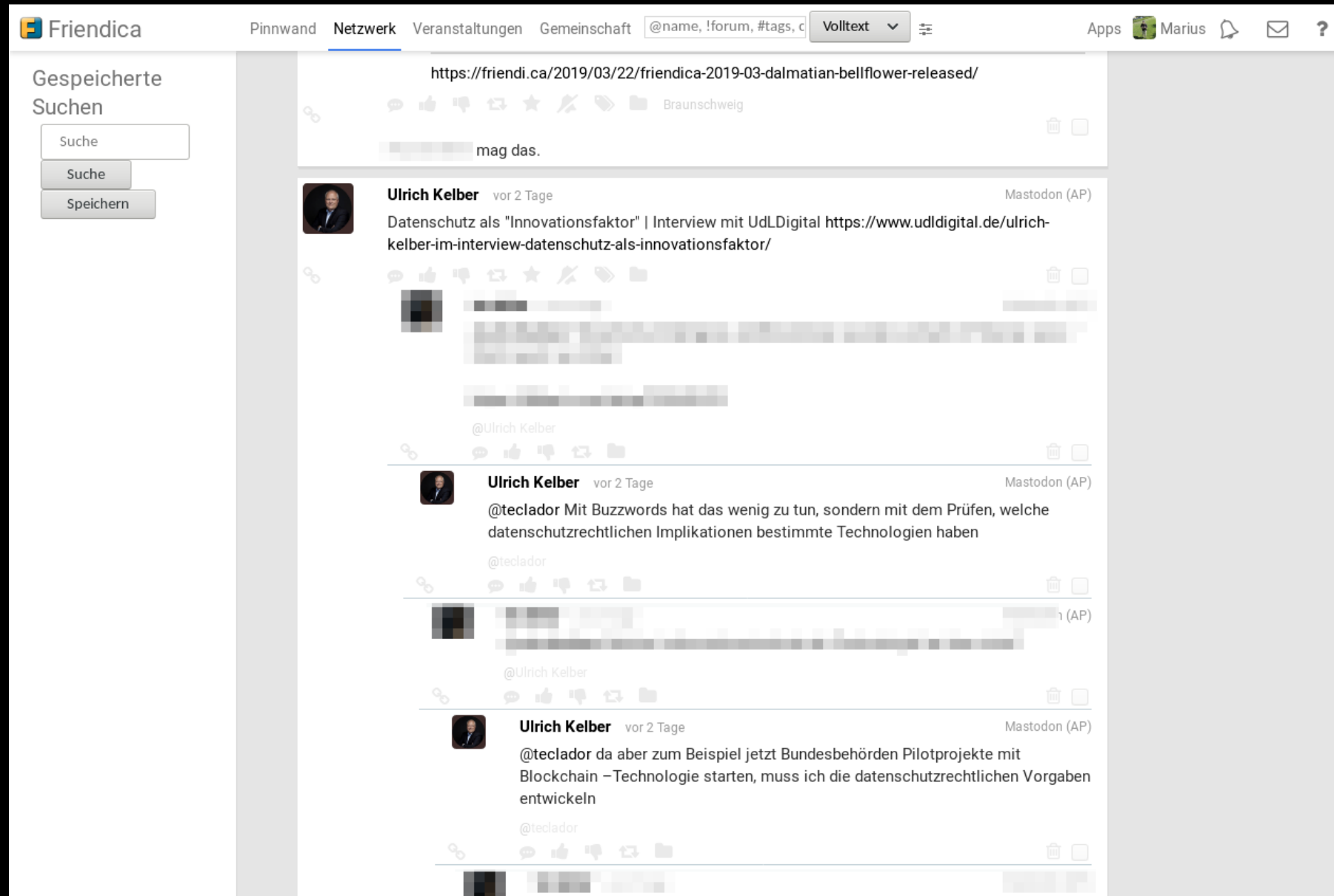
Dezentrale Soziale Netze

Eigene Webseiten betreiben



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit



Friendica

ein **föderiertes**,
dezentrales
Soziales Netzwerk.

hier im Bild :
Bundesdatenschützer Ulrich Kelber

© Marius Schwarz für BS-LUG 2019



Themenabend: Digitale Selbstverteidigung

Kapitel 2: Kampf gegen die Meinungsfreiheit

Marius Welt
Der (IT) Blog aus Braunschweig

LINUX FEDORA JAVA SECURITY BRAUNSCHWEIG DATENSCHUTZERKLÄRUNG

EU VERORDNUNG ZUR VERHINDERUNG TERRORISTISCHER ONLINE-INHALTE

Posted on 16. März 2019 by marius

Der Kampf um das neue EU Urheberrecht und Artikel 13 ist noch nicht mal richtig angelaufen, da kommt schon die nächste Verordnung mit Upload-Filtern um die Ecke. Und die, liebe Kollegen, hat es so richtig in sich. Dem Kampf gegen den Terror ist ja jedes Mittel recht, sogar Mittel, die es gar nicht gibt.

EU Verordnung zur Verhinderung terroristischer Online-Inhalte

Da es sich um ein 40 Seiten [Dokument](#) handelt, nehmt es mir nicht übel, wenn ich hier nicht alles präsentiere oder kommentiere. Es wird ausreichen, glaubt es mir einfach.

Vorweg ein Hinweis:

Eine EU Verordnung hat Gesetzeswirkung (wie die DS GVO) und muß nicht von den Mitgliedsstaaten in nationales Recht umgesetzt werden. Lediglich der in der Verordnung gegebene Spielraum steht jedem Staat offen. Meint: geht das durch, gilt es überall ohne wenn und aber.

Schauen wir uns erst einmal die Begriffsbestimmungen an :

[Artikel 2](#)
[Begriffsbestimmungen](#)

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

(1) „Hostingdiensteanbieter“ einen Anbieter von Diensten der Informationsgesellschaft, die darin bestehen, die durch einen Inhaltenanbieter bereitgestellten Informationen im Auftrag des Inhaltenanbieters zu speichern und die gespeicherten Informationen Dritten zur Verfügung zu stellen;

(2) „Inhaltenanbieter“ einen Nutzer, der Informationen bereitgestellt hat, die in seinem Auftrag von einem Hostingdiensteanbieter gespeichert wurden oder gespeichert werden;

(1) klingt toll, oder? Wißt Ihr, wer das ist ? Ihr. (2) seid auch Ihr oder Eure Besucher, wenn die einen Kommentar im Blog lassen. Ihr merkt schon, dieser Beitrag richtet sich nicht primär an normale Webkonsumenten, sondern an

NEUE BEITRÄGE

Die Gnome Surface Tips
und geschafft ..!
WordPress 5.1.1 Multisites mit DB-Updateproblem
TPM2 Update zerlegt
Fedorainstallation
Tablet und kein Ende in Sicht

NEUE KOMMENTARE

marius bei EU Verordnung zur Verhinderung terroristischer Online-Inhalte
Kommentar zu Docker – Genauso schlimm wie befürchtet | My-IT-Brain bei Docker – Genauso schlimm wie befürchtet
marius bei EFail: Die Katze ist aus dem Sack
ayno5 bei EFail: Die Katze ist aus dem Sack
Wochenrückblick KW 19/2018 – vNotes bei Androids K9 Mail nutzt noch TLS 1.0

BLOG TRAFFIC

Webseiten
Webseiten | Hits | Einmalig

Eigene Webseite

Keine Zensur möglich

Kaum Kosten

Weltweit zugänglich



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Vorratsdatenspeicherung



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Offiziell ist die Vorratsdatenspeicherung noch nicht vom Tisch,
sondern nur ausgesetzt.



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

1. VPN – Virtual Private Network



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

1. VPN – Virtual Private Network

Der Datenverkehr vom DSL-Provider wird an den (**idealerweise**) **eigenen** VPN Server im Netz geleitet, dieser leitet es ans Ziel.

Die Überwacher sehen nur den Datenverkehr zum VPN Server und der ist auch noch **verschlüsselt**.



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

2. TOR – The Onion Router

Der Datenverkehr vom DSL-Provider wird verschlüsselt an irgendeinen Tor Server im Netz geleitet, dieser leitet es im Tornetz über Bande ans Ziel.

Die Überwacher sehen nur den verschlüsselten Datenverkehr zum Tor Server.



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

2. TOR – The Onion Router

Kann da nicht einer der TOR-Serverbetreiber sehen was ich tue?

Der letzte Server in der Kette sieht den Datenverkehr mit dem Ziel, weiß aber nicht, vom wem dieser kommt. Solange man dann noch HTTPS benutzt, ist die Privatsphäre gesichert.

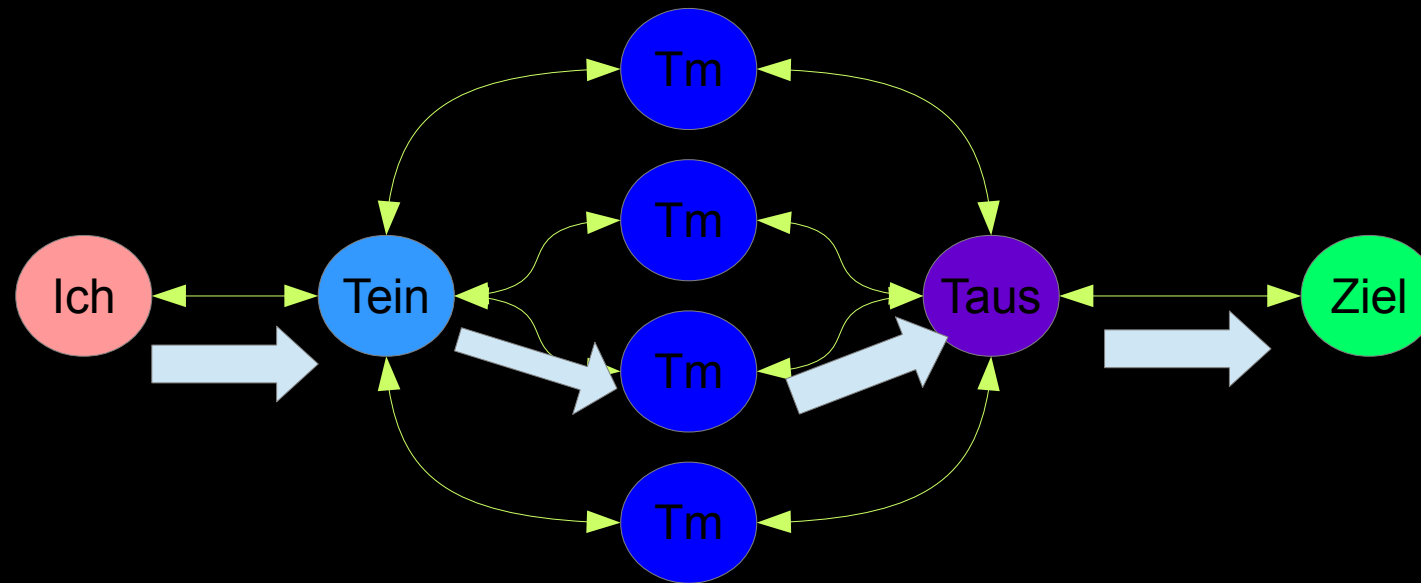


Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

2. TOR – The Onion Router



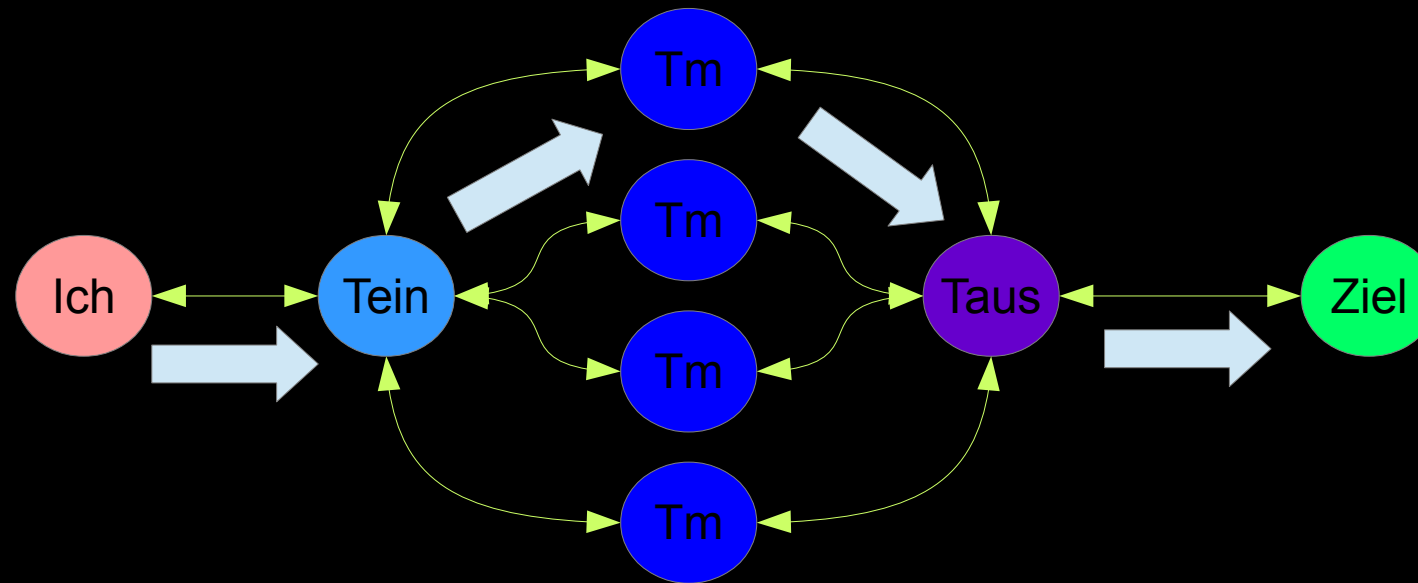


Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

2. TOR – The Onion Router





Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

3. GPG/PGP – Verschlüsselung für Emails



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

3. GPG/PGP – Verschlüsselung für Emails

Dabei wird der Inhalt der Email verschlüsselt,
so daß aus der Postkarte ein Brief wurde.

Absender & Empfänger müssen vorher aber Schlüssel
ausgetauscht haben.



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

3. GPG/PGP – Verschlüsselung für Emails

Mehr dazu im Vortrag „Wieso mit GPG“



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

4. TLS – Transportverschlüsselung für Emails



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

4. TLS – Transportverschlüsselung für Emails

Hier wird der Weg vom PC zum Mailserver verschlüsselt, so daß ein Überwacher den Inhalt der Emails nicht sehen kann.

Die Einrichtung ist mit EINEM Klick getan.



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

4. TLS – Transportverschlüsselung für Emails

Jedes gebräuchliche Emailprogramm kann TLS !



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

4. TLS – Transportverschlüsselung für Emails

Jedes gebräuchliche Emailprogramm kann TLS !

(selbst Microsoftprodukte)



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

5. TLS – Transportverschlüsselung für Server

Seriöse Anbieter von Internetdiensten,
also alle die nicht im TDAX sind,
betreiben Mailserver mit TLS Unterstützung.

(gelegentlich sogar Microsoftprodukte)



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

vorhandene Mailoptions

(Hilfe)

Domain	Verbindung zum Server benötigt Verschlüsselung	Server akzeptiert nur TLSv1.2	Empfangender Mailserver muß TLS benutzen	Server sendet nur TLSv1.2	Keine ZIP Dateien annehmen	Keine Office-Dateien annehmen	Keine PDF-Dateien annehmen	Absender mit SPF überprüfen
notls.de	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Speichern



Themenabend: Digitale Selbstverteidigung

Kapitel 3: Staatliche Überwachung

Gegenmaßnahmen

6. HTTPS – Transportverschlüsselung für Webserver

verantwortliche Anbieter von Internetdiensten,
betreiben Webserver mit HTTPS Unterstützung.

A screenshot of a browser address bar. On the left, there is a green padlock icon indicating a secure connection, followed by a green information icon. To the right of these icons, the URL 'https://federation.cloud-foo.de/network' is displayed in a grey font.

  <https://federation.cloud-foo.de/network>



Themenabend: Digitale Selbstverteidigung

Danke für Ihre Aufmerksamkeit