Anonym und sicher im Internet

Workshop zum Safer Internet Day 2018

Inhaltsverzeichnis

Einleitung....2
Gefahren“ im Internet....2
Einige Beispiele....3
Überall soll ich mich "anmelden"....3
Verschlüsselung....5
Historie....5
Asymmetrische Verschlüsselung....6
Verschlüsselung - wo ist das Problem?....8
Unterschiede GnuPG und openSSL....9
Ein paar Kommandos für den Nerd....9
Mailverschlüsselung konkret....11
Alternative: Bitmessage als Mailprogramm verwenden....11
Programme für sicheren File Transfer und Secure Shell....12
Vor dem Start ins Netz....13
Firewall....13
Virtuelle Systeme....15
Wo sind meine Daten?....15
Backup....16
Auf ins Internet....17
Surfen....17
Umwege - Proxies und Tor....18
Tor....20
Anonym trotz Vorratsdatenspeicherung?....21
Verhalten in sozialen Netzwerken....22
Wozu?....22
Fazit....24
Was ist zu tun?....24
Verweise....25
Weitere Links....25

Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

Einleitung

Wie bewege ich mich anonym im Internet?

Überwachungsgesetzen und der Gier der Wirtschaft nach unseren Daten kann man erfolgreich und völlig legal aus dem Wege gehen. Inzwischen weiß jede/r, dass man nicht jede Kundenkarte braucht und dass man nicht alle Fotos der letzten Party oder Firmenfeier ins Internet stellt. Wir wollen aber nicht Verzicht predigen, es reicht wenn man stattdessen einige Punkte beachtet.

Für den Schutz der eigenen Privatheit (hier ist das englische Wort Privacy viel treffender als der gute deutsche Datenschutz) kann es sich ganz schnell auszahlen, wenn man etwas Vorsicht walten lässt, ohne dass man dadurch auf die Möglichkeiten und Angebote im Internet verzichten muss.

Der folgende Artikel enthält einige Vorschlage dazu, die wir zum Safer Internet Day unseren Besuchern präsentiert haben, ohne einen Anspruch auf Vollständigkeit zu erheben. Weitere Vorschläge sind jederzeit über die Kommentareingabe oder per Mail an kontakt@aktion-fsa.de willkommen.

Um die eigene Persönlichkeit und die eigenen Daten gegen Missbrauch aus dem Internet zu schützen, reicht es nicht, einige Einstellungen im Web-Browser zu verändern. Es kommt auf das Zusammenspiel verschiedener Komponenten an und die Maßnahmen müssen aufeinander abgestimmt sein. Schauen wir zuerst wo die "Gefahren" lauern.

Gefahren“ im Internet

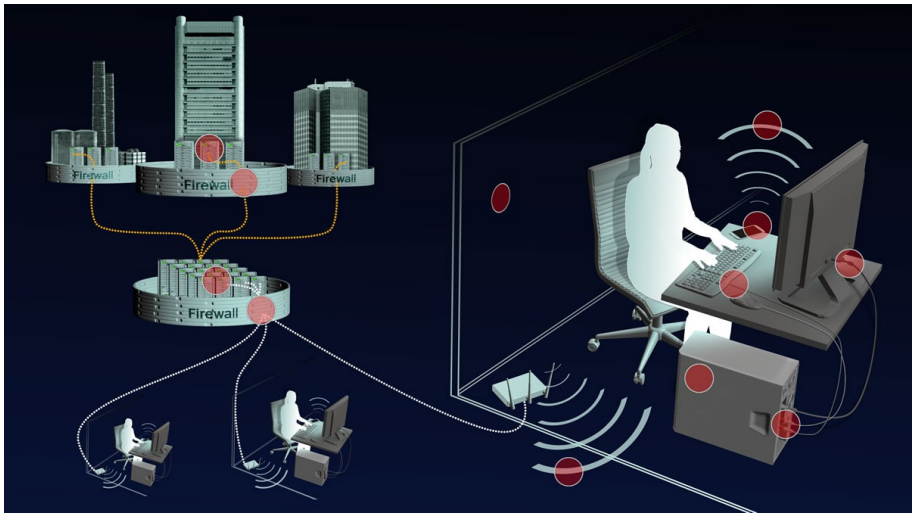
Über die "Gefahren des Internets" kann man täglich mindestens einen Artikel in den Zeitungen lesen.

- Meine Eingaben auf Web-Seiten können für fremde Zwecke missbraucht werden (Erstellung eines Persönlichkeitsbildes, Marketing, Scoring, Identitätsklau).
- Mein Internetverkehr kann auch auf dem Transportweg mitgelesen oder sogar ersetzt werden.
- Fremde können meine persönlichen Daten für ihre Zwecke wegfangen.
- Auf meinem Rechner können Programme laufen die Anderen das Spionieren in meinen Daten ermöglicht.
- Beim Surfen und Runterladen von Web-Seiten oder Programmen aus dem Internet kann ich mir Viren (Schadprogramme) einfangen, die meine Daten ausspähen, meine Programme unbrauchbar und mich erpressbar machen oder meinen Rechner für ihre Zwecke missbrauchen wollen.
- Trojaner oder Bots können mein Gerät für ihre Zwecke benutzen.

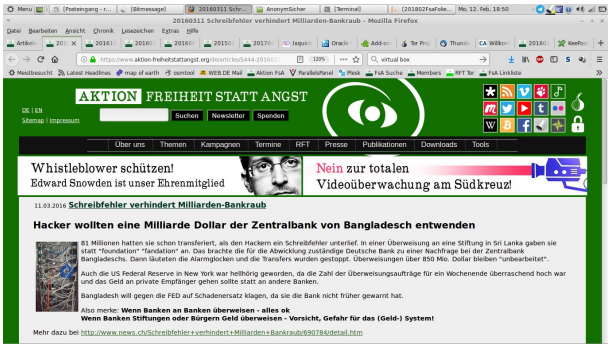
Die Angreifer können dabei Kriminelle, neugierige Unternehmen, gelangweilte Mitarbeiter in Unternehmen oder Geheimdienste sein.

Wie man aus dieser, sicher nicht abschließenden Liste ersieht, reicht nicht eine Maßnahme, um diesen vielfältigen Gefahren zu begegnen. Wie bei jeder Risikoanalyse muss man sich im klaren sein, dass es keine hundertprozentige Sicherheit gibt. Aber wir können versuchen Gefahren zu

minimieren und müssen unsere Handlungen stets nach den Restrisiken hinterfragen.



Einige Beispiele



- ein Milliardenraub
- 500 Millionen gehackte Yahoo Acounts
- Lauschende Glühlampen plaudernde Schlösser
- Mithörende Smart TVs
- Alexa, Echo Look u.a. Mitlauscher
- Hunderte von Datenpannen
- Hunderte von Datenskandalen
- ein Verweis zu unserer Publikation "Überwachung durch die Wirtschaft"

Alles dies bringt nur Ärger und im Schadensfall Kosten für den Einzelnen.

Überall soll ich mich "anmelden"

Auf diversen Web-Seiten werde ich nach meinem Namen und meiner E-Mail-Adresse gefragt. Um ein Kochrezept anzuschauen oder bei einem Online Spiel teilzunehmen, muss ich jedoch nicht eine E-Mail-Adresse verwenden, die mich identifiziert oder mit der ich sonst mit dem Arbeitgeber oder meiner Bank kommuniziere.

Für solche Zwecke bietet sich eine kostenlose Wegwerfadresse, z.B. von sofort-mail.de an, die nur kurze Zeit gültig bleibt. Für unterschiedliche Zwecke sollte man auch verschiedene E-Mail-Adressen und Nicknames anstelle des eigenen Vor- und Zunamens verwenden. Es gibt zahllose Anbieter von kostenlosen Maildiensten (z. B. panda.com, mail.com, gmx.de, web.de,...). Nach deutschem Telemediengesetz (TMG) hat man ein Recht auf Anonymität bei der Nutzung des Internets.

Möchte man zusätzlich auch noch gegenüber der staatlichen Vorratsdatenspeicherung anonym bleiben, so sollte der Mailanbieter nicht in Europa und vor allem nicht beim eigenen Netzanbieter

(Provider) liegen, der schon sämtliche Verbindungsdaten speichert.

Je nach der Verwendung ist es auch entscheidend, ob ich meine Mails lokal in einem eigenen Programm (z. B. Thunderbird) oder online auf der Webseite des Mailproviders schreibe, lese und damit auch dort abspeichere. Meine Korrespondenz mit der Bank, der Versicherung oder dem Arbeitgeber möchte ich nicht auf einem entfernten Postfach zu liegen haben.

Natürlich sollte jede vertrauliche Mail verschlüsselt versendet werden, wie ich auch jeden vertraulichen Brief vor dem Versand normalerweise zuklebe.

Ich muss mir auch nicht in jeder Spam-Mail mehr oder weniger "schönen" Bilder anzeigen lassen und durch das Nachladen dieser Bilder beim Öffnen der E-Mail von einer fremden Webseite dem Spam-Absender meine IP-Adresse verraten und ihm damit nebenbei auch die Richtigkeit meiner E-Mailadresse bestätigen. Dieses Nachladen lässt sich in den meisten E-Mailprogrammen ausschalten und beim grafisch verzierten Geburtstagsgruß eines Freundes bei Bedarf wieder anklicken.

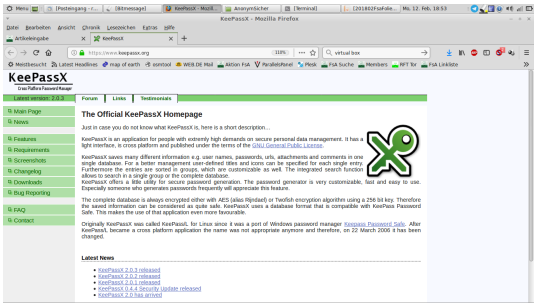
Verschlüsselung

Historie

- Verschlüsselung ist nicht neu, Kryptographie wurde bereits im dritten Jahrtausend v. Chr. eingesetzt.
- Über Jahrtausende mussten Boten dazu die Schlüssel, z.B. auf eingeritzten Skytalen durch die Gegend tragen.
- Die Sicherheit beruhte allein auf der Geheimhaltung dieses Schlüssels und die Möglichkeit der Entschlüsselung auf dem Vorhandensein dieser Information.
- Seit dem Mittelalter werden Geheimschriften im diplomatischen Briefverkehr verwendet. Für jedes Land mussten die Kodierungen an "sicherer Stelle" im heimischen Ministerium und der diplomatischen Vertetung im fremden Land aufbewahrt werden. Die Entschlüsselung ging nur "händisch" Buchstabe für Buchstabe.

- Maschinell wurde dann im 20. Jahrhundert gearbeitet, ab 1932 mit der bekannten ENIGMA. Auch deren Code wurde in den 40-er Jahren durch polnische und britische Mathematiker geknackt.
- Seit 1977 gibt es einen Data Encryption Standard (DES), der maschinelle Verschlüsselung auf eine höhere Stufe hob. Durch die Verwendung eines Computers konnten die Schlüssel wesentlich komplizierter sein.
- Ende der 70-er Jahre entwickeln Diffie und Hellman eine asymmetrischer Verschlüsselung, bei der ein Schlüsselpaar verwendet wird. Ein nicht geheimer, öffentlicher Schlüssel (Public Key) wird zum verschlüsseln benutzt. Die Entschlüsselung ist nur mit einem geheimen Private Key möglich.
- Phil Zimmermann entwickelt daraus das Programm PGP (Pretty Good Privacy).
- Sehr bald wird die Verschlüsselung damit in USA verfolgt. Verschlüsselungen werden ab bestimmten Schlüssellängen verboten, auch der Export seiner Programme. In Frankreich gilt ein generelles Verbot von Verschlüsselung, die erst mit der EU Datenschutzverordnung 1995 aufgehoben wird.
- Angesichts dieser Maßnahmen stellt Phil Zimmermann die Algorithmen zu PGP 1991 online. PGP wird ein Open Source Programm unter dem Namen GnuPG (GPG). Dessen Verschlüsselung ist auch heute noch sicher, ein gutes Passwort vorausgesetzt.
- Der AES (Asymmetric Encryption Standard) ersetzt 2001 den DES.

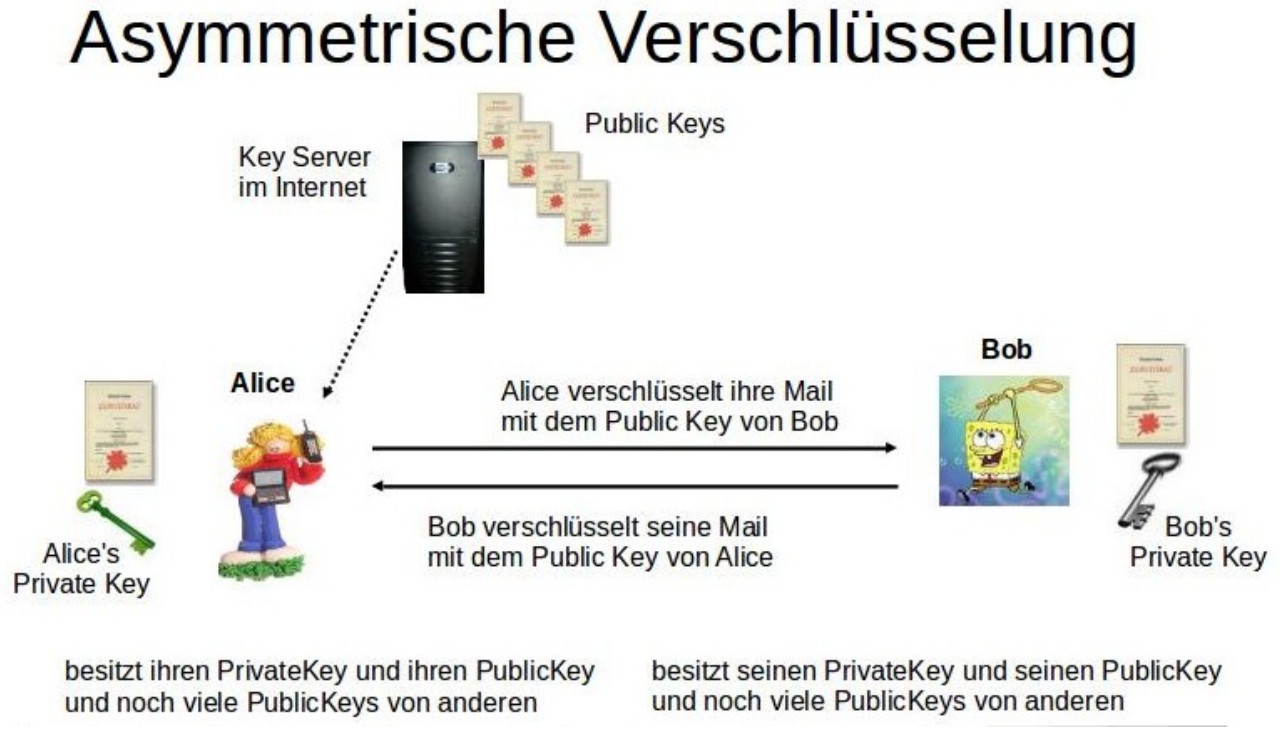
Das "uralte" Problem sich die Passwörter aller Freunde oder Geschäftspartner merken zu müssen ist durch den AES ganz wesentlich reduziert worden. Ich muss jetzt nur noch mein eigenes Passwort sicher aufbewahren. Sollten das inklusive Anmelde-Passwörter und Mail-Accounts immer noch zu viele für den Kopf sein, so hilft ein Passwort-Tresor, wie z.B. KeePassX. Ich muss mir dann nur noch das Passwort zu diesem Tresor merken, alle anderen kann ich bei Bedarf mit Copy&Paste in die entsprechenden Anwendungen übertragen.



Über sinnvolle Passwortlängen und die Sicherheit dabei werden wir später reden.

Asymmetrische Verschlüsselung

Das folgende Bild soll dazu dienen das Verfahren bei asymmetrischer Verschlüsselung zu veranschaulichen.

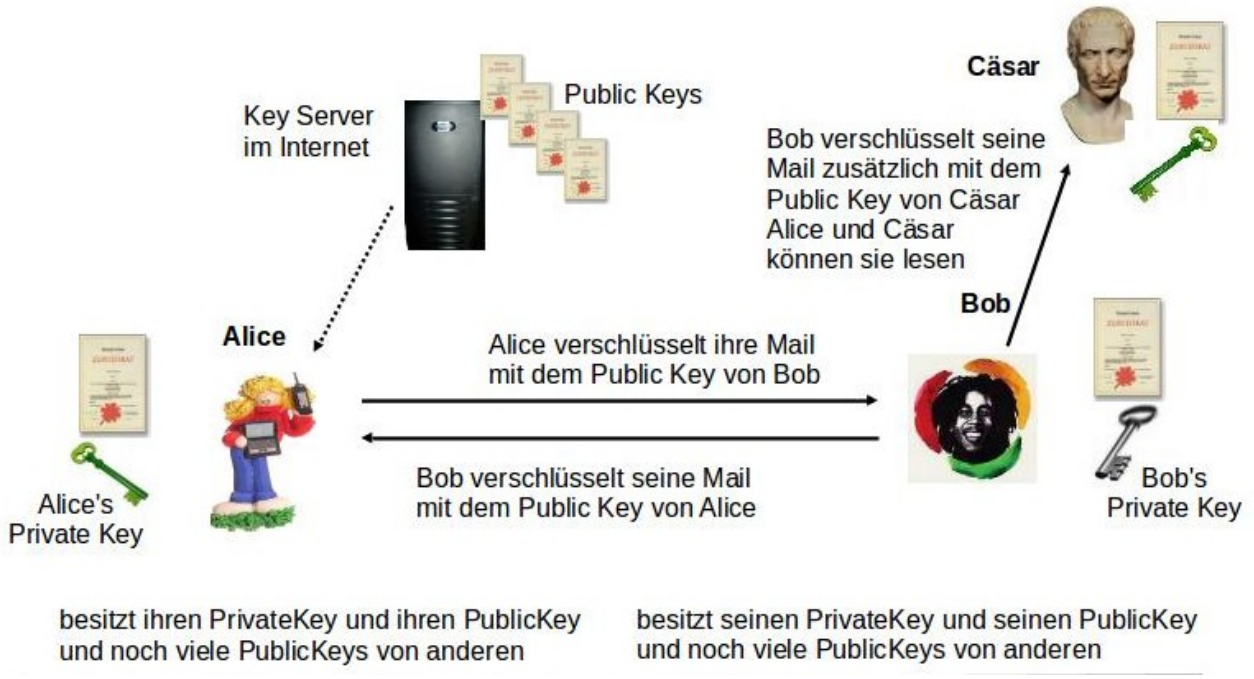


Jede/r besitzt zur Verschlüsselung ein Paar, einen öffentlichen Schlüssel (Public Key oder Certifikate) und einen geheimen Schlüssel (Private Key). Den öffentlichen Schlüssel verschickt der Besitzer an alle seine Freunde oder lädt ihn auf einen öffentlich zugänglichen Schlüsselserver im Internet. Auf solchen Key Servern kann man an Hand der Mailadresse oder des Namens nach Public Keys suchen und diese herunterladen. In Key Servern suchen kann man z.B. hier https://www.heise.de/security/dienste/Keyserver-474468.html

Betrachten wir die Kommunikation von Alice und Bob (A und B).

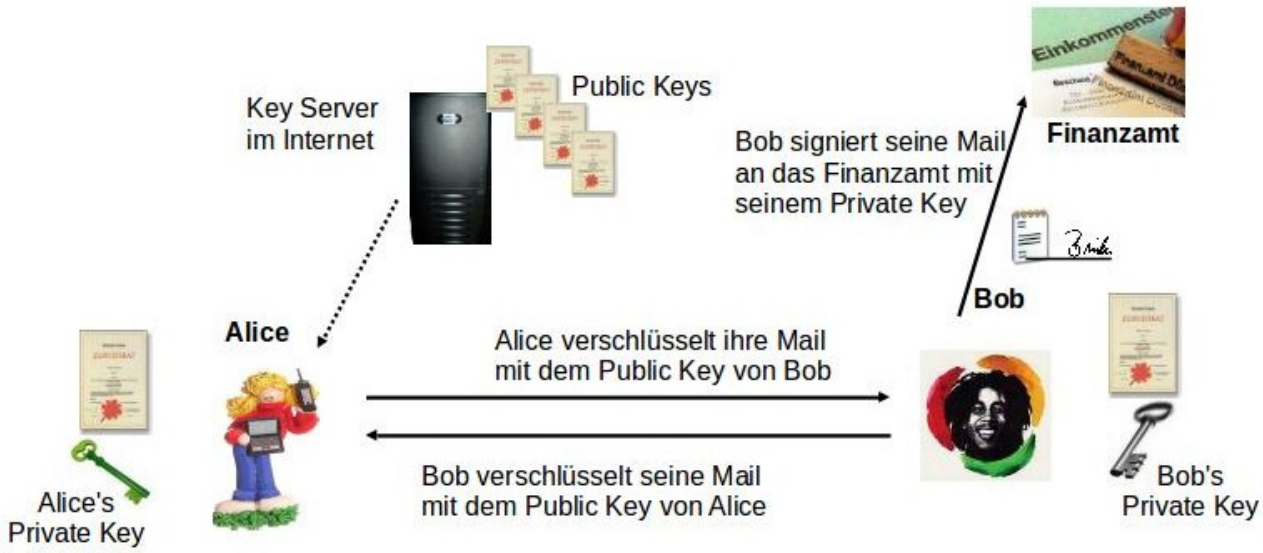
- Alice besitzt ihren PrivateKey und ihren PublicKey und noch viele PublicKeys von anderen.
- Bob besitzt seinen PrivateKey und seinen PublicKeyund noch viele PublicKeys von anderen.

- Alice verschlüsselt ihre Mail mit dem Public Key von Bob.
- Bob verschlüsselt seine Mail mit dem Public Key von Alice.



- Nun verschlüsselt Bob seine Mail an Alice und Cäsar zusätzlich mit dem Public Key von Cäsar.
- Alice und Cäsar können sie lesen - und auf der ganzen Welt nur sie beide.

Asymmetrische Schlüsselpaare erlauben eine weitere sinnvolle Funktion:



- Bob schickt eine Mail an das Finanzamt und signiert seine Mail mit seinem Private Key.

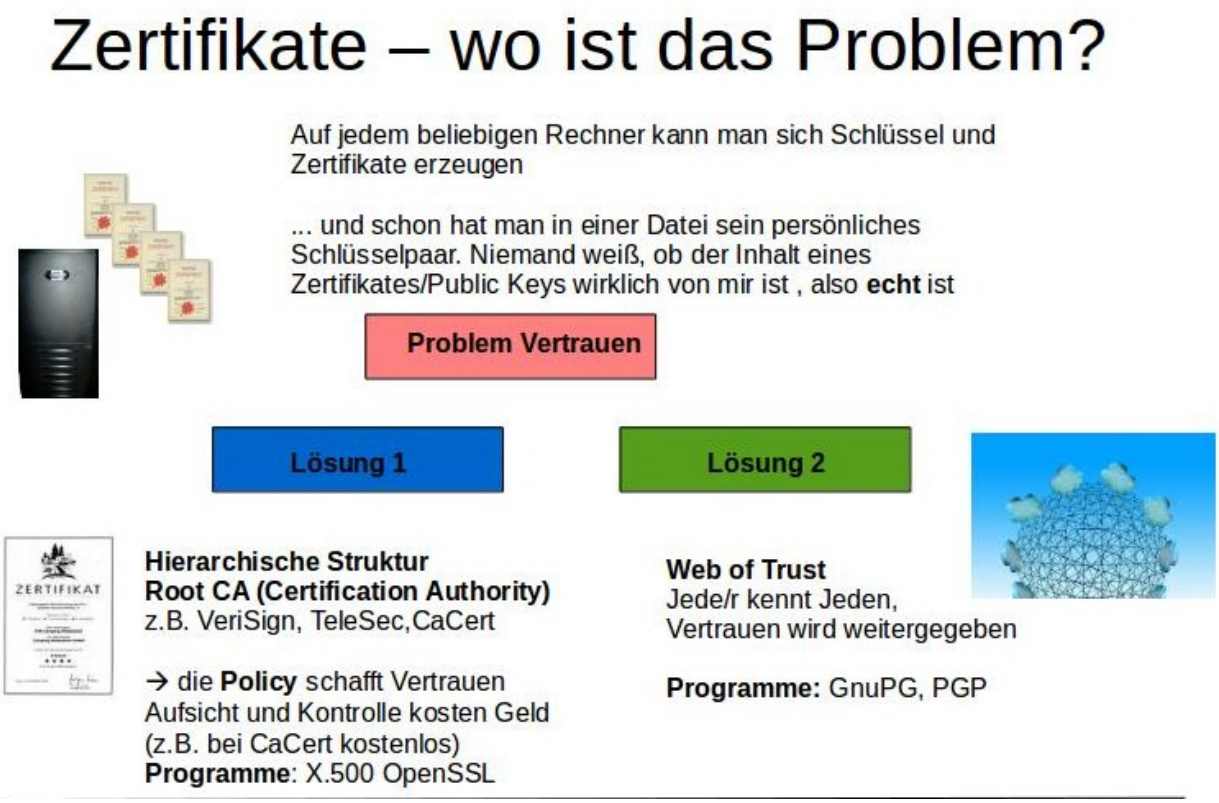
Damit wird sichergestellt, dass der Inhalt der Mail auf dem Weg zum Finanzamt nicht verändert wurde und dass der Absender wirklich Bob war, denn nur er ist im Besitz seines Private Keys. Also sollte man jede Mail, die man verschickt auch signieren, denn nur dann kann der Empfänger darauf vertrauen, dass sie so abgeschickt wurde.

Nachtrag: "mit seinem Private Key signieren" heißt nicht diesen dort anzuhängen, dann wäre er nicht mehr geheim, sondern mt Hilfe des Private Key wird ein Hash (eine eindeutige Zahl) über den Mailinhalt berechnet, so dass der Empfänger mit Hilfe des Public Keys des Absenders verifizieren kann, dass der Inhalt nicht verändert wurde.

Verschlüsselung - wo ist das Problem?

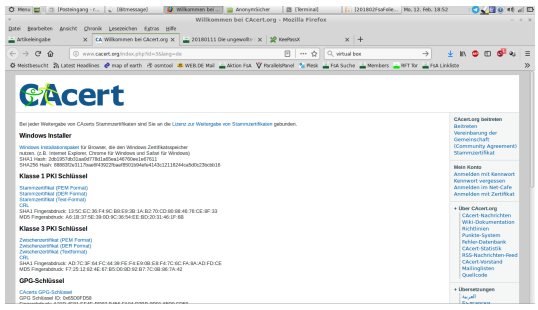
Auf jedem beliebigen Rechner kann man sich Schlüssel und Zertifikate erzeugen ...

... und schon hat man in einer Datei sein persönliches Schlüsselpaar. Niemand weiß, ob der Inhalt eines Zertifikates/Public Keys wirklich von der Person ist auf dessen Mailadresse oder Namen sie lautet, also echt ist.



Wir haben also ein Vertrauensproblem. Es gibt zwei Wege dieses zu lösen. In einer hierarchischen Struktur vertrauen wir in den Staat oder eine angesehene Firma, die sogenannte Root CA (Certification Authority). Das sind z.B. Firmen wie VeriSign, TeleSec, CaCert, ...

Diese schreiben in einer Policy welche Garantien sie geben, welche Belege jemand liefern muss, um ein Zertifikat oder ein Schlüsselpaar von ihnen ausgestellt zu bekommen. Diese Aufsicht und Kontrolle kosten Geld und damit auch meist die von ihnen ausgestellten Zertifikate. Bei der australischen Firma CaCert sind private Zertifikate kostenlos, werden aber leider von anderen



CAs nicht anerkannt. So weigert sich z.B. der Mozilla Firefox Browser von CaCert ausgestellte Zertifikate als vertrauenswürdig einzustufen.

Das Programm für solche nach dem Standard X.500 ausgestellten Schlüssel heißt OpenSSL und steht für alle Betriebssysteme kostenlos zur Verfügung (Open Source).

Die zweite Lösung ist ein Web of Trust, Jede/r kennt Jede/n und das Vertrauen muss man durch gegenseitiges Kennenlernen erwerben und weitergegeben. Spätestens beim Freund vom Freund vom Freund sollte man mit dem Vertrauen vorsichtig sein. Diesen Vertrauensgrad kann man in den zuständigen Programmen GPG, bzw. PGP für jeden Schlüssel eintragen.

Unterschiede GnuPG und openSSL

Dieses Kapitel ist für die reine Nutzung von Verschlüsselung nicht notwendig und richtet sich an diejenigen, die gern tiefer einsteigen möchten.

PGP	X.509
nicht standardisiert	ITU Standard
GnuPG* ist OpenSource	openSSL ist OpenSource
Web of Trust	Hierarchische Struktur
gegenseitiges Vertrauen	Vertrauensbaum
Sicherheit in Kleingruppen	Sicherheit im Server-Bereich

- beide sind von der Verschlüsselung sicher
- beide sind einfach bedienbar
- beide sind in Thunderbird mit Enigmail enthalten
- beide hatten Probleme in Outlook, diese sollen aber gelöst sein

*) GnuPG basiert auf PGP 2.6.2, das war die letzte unabhängige Version für die Phil Zimmermann "seine Hand ins Feuer" legt. Danach war ihm der Druck durch staatliche Stellen und finanzielle Interessen der Mitbesitzer zu groß geworden.

Ein paar Kommandos für den Nerd

Wie sieht denn so ein Schlüssel überhaupt aus?

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.0.10

mQGiBD0WxX8RBAD090P87skqoGsTZUDO0jP9VJxfkGlDT5rRWYzY5UEfrk8SDr4+Tv54sMHP
aYx5W4K5ZhffAcZVmdGJH+BpSxAq9deiaIWOH3XfsM7ja9fE8/nuU5pRuSvL0+LL3Z1NERU6
whZ0ELN1VSaslPCWrUp8Qpp/DZFGVhHVzkatLeW72wCg/6Q+UYdatmnRIvGU0l6ufNvy+mkD
/0gAeZ4bqZrOZQiHZ5fZu7Rw5i4X46AuZF9u61f90+dHHTv9QZGe+EC+4muRx71XRjTyCHKP
aVeP58LYjkmCXM0FgDqEOcAcVq1eB7FHnxzmuZ1NvKPMpTIdPvO3ta0uu1+yyY9JnXgXdUou
XLcAgPR5CCV6061ewCBIxBNZB9F7A/9pcdSZ2QhLDW65wdRW5uS69JydWftQxyQo0iUvtmi3
3EXqaoPtq8Y2Mgx9jFG5wINta5xqcNyEfZkuHQOqCjeHfxweAuwM4J3kRLokTgQROnMWNJMx
RoeT7NyQv7PIsA2Hdg5P5obX+tcN1cmCfmBMGRJnlQwdJXzGNUMJov3qubQ5UmFpbmVyIEhh
bW1lcnNjaG1pZHQgPFJhaW5lci5IYW1tZXJzY2htaWR0QHQtc3lzdGVtcy5jb20+iE4EEBEC
AA4FAj0WxX8ECwMCAQIZAQAKCRDwONO4mzitSq5dAKD3QqyvmX3npMGBrlGVY6vy3mo42QCf
TVFydVQtAdGuNqCfebAYIBDpPd+5Ag0EPRbFfxAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+2
8W65Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvO
meFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0Oj
HRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+c
fL2JSyIZJrqrol7DVekyCzsAAgIH/2Ls3usk1s6i6vLFrsCiWx+ERSXrRg7Yl3taGUFzp74Q
KzWUDznDzzpnEpg2PRiOXTgP21WlpbH50jglOPchpSGeUo5PbxpiOo8SOEQrRatgORT9FE9e
43rVQn8apeL5McCLkBYhjr/AnlaE9bnaOdvjWM/J1dFzhfC3Pbq2hx4De2Y4e5WOKKLVJNF0
tHFt/JwrvNVfYmJb7MH1CC4KbgeEP2QT/J1UU5FqqosrjcIEHRPnC8Vt8jSrWik313NMhn6t
aKZx3pyXoK6jPatMTV1G7dF6r1RcLKDBkEmOhQI52Keu4+Ojs3oT+ghQlpcdQFJxKScyKzFD
puRX/ZgjwMeIRgQYEQIABgUCPRbFfwAKCRDwONO4mzitSvmCAJ4mpKcLYHWNlOpv0p0LBX/z
5yhPqQCg17XYSxUEoKwu7TbINZYCF12T5z0=
-----END PGP PUBLIC KEY BLOCK-----
```

... und der Private Key sieht so ähnlich aus. Die Länge kann variieren, je nach dem was man in den Schlüssel hineingeschrieben hat. Das ist für unsere Schlüssel zum sicheren Mailen mindestens eine Mailadresse, es kann aber auch ein Name, eine Organisation oder Abteilung in einer Firma sein.

Es ist also nichts, was wir uns ansehen oder gar merken müssen. Computer-afine Menschen, die gern auf der Kommandozeile arbeiten, werden aber nicht umhin kommen solche Zahlenkolonnen anzuschauen. Dafür haben sie dann auch die Gelegenheit zu erfahren, was in einem Public Key alles stecken kann.

Wenn man direkt mit der Verschlüsselungssoftware PGP/GPG reden möchte, dann geht das so:
Einige GnuPG Commands

gpg --gen-key	Schlüssel erzeugen
gpg --list-keys	Schlüssel auflisten
gpg --list-secret-keysprivate	Schlüssel auflisten
gpg --fingerprint	Alices Fingerprint anzeigen
gpg --verify alice.asc	Inhalt prüfen und anzeigen
gpg -s -u Bob text.txt	als Bob unterschreiben
gpg --clearsign -u Bob text.txt	als Bob unterschreiben und den Schlüssel im Klartext ablegen
gpg -e -r Alice text.txt	für Alice verschlüsseln
gpg -s -u Bob -e -r Alice text.txt	als Bob unterschreiben und für Alice verschlüsseln
gpg -d text.txt.gpg	entschlüsseln
gpg -c text.txt	mit Passwort (symmetrisch) verschlüsseln

Wenn man will, kann man sich sein Schlüsselpaar auch mit der ebenfalls offenen Software OpenSSL erzeugen. Zu beachten ist dann, ob man den Zusatzaufwand und eventuelle Kosten für eine RA, eine Registrations-Authorität, und eine CA, eine Zertifikats-Authorität, auf sich nehmen möchte.

Einige OpenSSL Commands (X.509)

Aufgabe des Users	
openssl genrsa -out bsp.key 1024	priv. Schlüssel mit 1024 bit Länge erzeugen
openssl req -new -key bsp.key-out bsp.csr	Zertifikatsrequest erzeugen
Aufgabe der RA	
openssl req -noout -text -in bsp.csr	Zertifikatsrequest ansehen
Aufgabe der CA*	
openssl x509 -req -days 730 -in bsp.csr -signkey bsp.key > bsp.crt	Zertifikat erzeugen
openssl x509 -in bsp.crt -noout -text	Zertifikat ansehen
openssl pkcs12 -export -in bsp.crt -inkey bsp.key -out cert.p12	P12 Export komplett, Private und Public Key
openssl pkcs12 -export -in bsp.crt -nokeys -out cert.p12	P12 Export public key
openssl pkcs12 -in cert.p12 [-nokeys]	P12 Zertifikat ansehen

* z.B. www.cacert.org

Mailverschlüsselung konkret

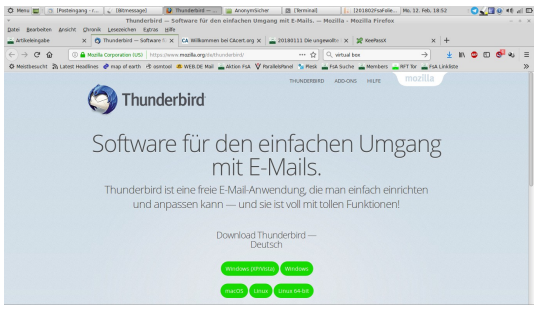
Machen wir also nun konkret den Schritt zur künftigen Verschlüsselung unserer Mail. Das bedeutet, dass wir in Zukunft statt offener Postkarten doch lieber verschlossene Briefe verschicken. Wir unterscheiden zwei Anwendungsszenarien:

Mit Thunderbird als Mailprogramm auf dem eigenen Rechner

- das PlugIn Enigmail hinzufügen
  - GnuPG installieren (in Linux),
  - GPGsuite installieren (auf Apple Mac),
  - GPG4Win installieren (in Windows)
- in Engmail ein eigenes Schlüsselpaar erzeugen
- einstellen: eigene Mails signieren
- Public Key an alle Freunde verschicken und
- danach nur noch auf verschlüsselte Mails antworten ;-))

Mit einem Mailprogramm im Browser (z.B. Firefox)

- das PlugIn Mailvelope hinzufügen
- ein eigenes Schlüsselpaar erzeugen
- einstellen: eigene Mails signieren
- Public Key an alle Freunde verschicken und
- danach nur noch auf verschlüsselte Mails antworten ;-))
- anwendbar bei Posteo, Mailbox.org, web.de, GMX, …



Über sinnvolle Passwortlängen und die Sicherheit dabei werden wir später reden.

Alternative: Bitmessage als Mailprogramm verwenden

Völlig ohne Passwörter kommt das Programm Bitmessage (BM) aus. Bitmessage ist ein sehr kleines, einfaches Programm für Textnachrichten, für Mailinglists und für Twitterchannels. Alle Bitmessages sind verschlüsselt,es gibt keine Metadaten, die eine Vorratsdatenspeicherung speichern könnte. Es gibt keinen Provider, alle Messages werden Peer-to-peer verschickt, komplett unterm Radar. Auch eine Paßworteingabe ist bei der Benutzung nicht erforderlich. Das ist beinahe Sicherheit per Design - allerdings sollte man seine Bitmessages auf einer verschlüsselten Platte ablegen, denn die lokal abgelegten Mails sind unverschlüsselt.

Nur für "amtliche" Mails bzw. Mails mit Anhängen oder an Leute ohne BM bleibt dann noch die "normale Mail".

Programme für sicheren File Transfer und Secure Shell

Bei dieser Gelegenheit wollen wir gleich noch ein paar weitere sinnvolle Open Source Programme hervorheben, die eine sichere Kommunikation ermöglichen.

- File Transfer mit Filezilla, Achtung: als Port stets 22 für sftp (secure file transfer) verwenden!
- Putty für die Verwendung im Terminal (Kommandozeile) oder zum File Transfer
- Putty für Windows https://www.putty.org/
- ssh für die Verwendung im Terminal (Kommandozeile)
- SSH für Windows https://www.ssh.com/ shareware
- SSH für Mac, Linux https://www.openssh.com/de/ freeware

Vor dem Start ins Netz

Firewall

Für die Sicherheit meiner Daten ist eine gut eingestellte Firewall ein wichtiger Schritt. Ich muss nur die von mir gewünschte Kommunikation erlauben. Über 65000 Ports auf jedem Rechner sind von Programmen über das Netz ansprechbar. Wenn ich selbst keine Dienste auf meinem Rechner für andere anbiete, dann kann ich diese Ports eingehend schon mal schließen und habe auf einen Schlag 65000 Angriffsmöglichkeiten beseitigt.

Hier eine Empfehlung für die Regeln auf meiner Firewall. Alle Betriebssysteme bringen eine Firewall mit, in Linux z.B. **ufw**, man kann auch **firestarter** oder als große Lösung **fwbuilder** installieren.

Meine Firewall sollte ausgehend folgende Ports offen halten

• Namensauflösung,	dns	UDP/TCP 53
• Mail senden,	smtp	TCP 25
• Mail holen,	imaps	TCP 993
• Mail holen,	pop3s	TCP 995
• Netzdrucker		TCP 515
• Secure Terminal	ftpssh sftp	TCP 22
• Web,	http	TCP 80
• Web verschlüsselt,	https	TCP 443
• Zeitaktualisierung,	ntp	UDP/TCP 123

Für alle Ports außer Web und File Transfer lassen sich die Verbindungen auch noch auf wenige Ziel-IP-Adressen einschränken, soweit diese bekannt sind. Das sind wieder viel weinger als 65000. Eingehend können wie gesagt alle Ports geschlossen bleiben solange ich keine eigenen Serverdienste betreibe.

Die obige Liste berücksichtigt aber nicht besondere Dienste, wie Telefonieren über das Internet (VoIP) u.a. - der Teufel steckt immer im Detail. Das Vorgehen, wenn etwas nicht funktioniert wäre dann: Firewall ausschalten , probieren ob es geht und wenn ja, dann nach der (zusätzlich benutzten) Portnummer suchen und diese freigeben, dann die Firewall wieder einschalten.

Bei Linux: wichtig ist hier zu prüfen ob die Firewall nach einem Neustart des Systems auch startet (Autostart).

Bei Windows 10: die vorgegebene Firewall lässt viel Verkehr zu Microsoft passieren (Windows10 telefoniert 5500-mal am Tag "nach Hause"), das sollte man einschränken.

Für Windows Systeme bot sich über Jahre wegen der Einfachheit und der Bedienerfreundlichkeit die freier Software Tiny Firewall an. Man wird durch sie darauf hingewiesen welches Programm über welchen Port gerade wohin möchte und kann dann entscheiden, ob man diesen Verkehr erlauben oder verbieten möchte. Die Tiny Firewall warnt auch sobald ein (bisher erlaubtes)

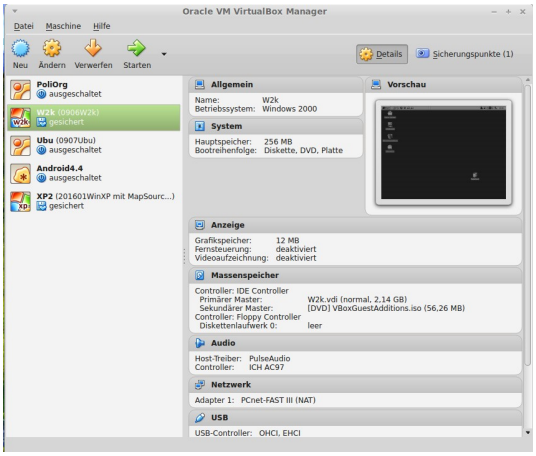
Programm verändert wurde. Per Mausklick auf das Icon in der Menuleiste ist es auch möglich den Internetverkehr völlig zu blockieren und wieder zu öffnen. Leider ist dieses Programm z. Zt. für Windows 8 und 10 nicht kostenlos verfügbar.

Wer in Linux Systemen genauer wissen möchte, welche Kommunikationsvorgänge ins Internet laufen, der sollte zur Konfiguration den frei erhältlichen Firewall Builder 8 verwenden. Wie in der Tiny Firewall gilt auch hier, dass erst einmal jeder Verkehr verboten ist, der nicht explizit erlaubt wurde. Grundsätzlich gilt dies auch für jeden Verkehr ausgehend von meinem Rechner, den eventuelle Trojaner oder Bots gern benutzen möchten, um mit ihrem Hersteller Verbindung aufzunehmen. Ich werde also nur die Ports öffnen, die meine Anwendungen brauchen (Namensauflösung,Web, vielleicht sicheren File Transfer, Netzwerkdrucker und Zeitaktualisierung und auf dem Spiele-PC ein paar Ports mehr). Nutzer des "gesprächigen" Windows werden zusätzlich nach einigen Ports gefragt, da das System auch mal "nach Hause telefonieren" mag, aber das muss man ja nicht unterstützen. Die Warnmeldungen der Firewall erscheinen am Anfang lästig, da man jedesmal gefragt wird ob man diesem oder jenem Programm den Zugang zum Internet erlauben möchte. Aber, wie gesagt, es sind nur wenige Ports wirklich als erlaubt einzustellen. Wenn dann nach einigen Tagen nochmal eine Anfrage kommt, ist die Wahrscheinlichkeit groß, dass hier ein "Schädling" anklopft.

Virtuelle Systeme

Nach dem ein PC zu einem normalen Gebrauchsgegenstand geworden ist, entsteht nun der Wunsch, möglichst mehrere Systeme zur Verfügung zu haben (z. B. einen PC für private Daten, einen Bankrechner, ein System zum Surfen im Internet). Dies ist jedoch schon aus ökologischen Gründen unsinnig. Die Grundidee, verschiedene Anwendungsbereiche zu trennen, lässt sich auch auf einem Rechner realisieren. Das Prinzip heißt Virtualisierung. Programme dafür gibt es für alle Betriebssysteme, z. B. VMware 4 für Windows und Linux, Parallels 5 für Mac und Virtual Box 6 für alle Betriebssysteme auf x86 Prozessoren. Virtual Box und die abgespeckte Version von VMware, der VMware Player, sind sogar kostenlos.

Man installiert dann auf seinem PC nur ein minimales Betriebssystem und die Virtualisierungssoftware, das sogenannte Host System. In dem Virtualisierungsprogramm lassen sich nun weitere voneinander unabhängige Systeme, also zum Beispiel ein Rechner für die Verbindungen zur Bank, ein Rechner zum Spielen und Surfen im Internet, ein Rechner für das private Tagebuch und andere persönliche Daten einrichten. Die Anzahl unabhängiger Systeme ist lediglich durch die Festplattengröße und die gleichzeitige Benutzung durch die Größe des Arbeitsspeichers beschränkt. Diese Systeme stehen auch auf Mausklick zur Arbeit bereit, denn sie werden von dem Virtualisierungsprogramm in den Schlaf (suspend) geschickt und bei Bedarf wieder erweckt, so dass man dort weiter arbeiten kann wo man beim letzten Mal aufgehört hat.



Ein großer Vorteil ist, dass diese Systeme nichts voneinander wissen und unabhängig sind. Sie sehen jeweils nur ihre Daten, so dass eine "Verschmutzung" der anderen Systeme vermieden wird. Man kann natürlich auch die Festplattenbereiche der anderen Systeme anmelden und verwenden oder Daten mit Copy&Paste von einem System ins andere kopieren, wenn man sich vergewissert hat, dass man damit den gerade erreichten Schutz nicht wieder verspielt.

Der größte Vorteil virtueller Systeme ist jedoch, dass sie theoretisch "unkaputtbar" sind. Es lassen sich zu jeder Zeit und auf jeden Fall nach der Installation, Snapshots erzeugen. Bekommt man zu einem späteren Zeitpunkt durch das Herunterladen eines ominösen Programms (z. B. ein Trojaner) aus dem Internet ein unsicheres System, so geht man mit einem Mausklick zu einem sicheren Snapshot zurück. Mit Sicherheit befindet man sich dann wieder in dem ursprünglichen System, da alle inkrementellen Änderungen seit diesem letzten Snapshot gelöscht werden - aber auch alle in der Zwischenzeit veränderten oder neu angelegten Dateien.

Wo sind meine Daten?

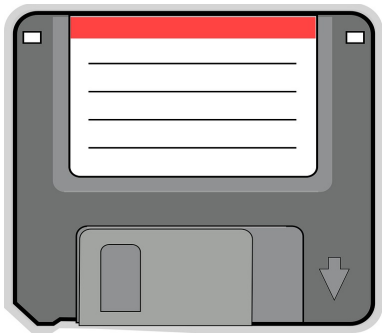
Damit nach so einem Rücksprung zum letzten Snapshot nicht auch der gestern geschriebene Geschäftsbrief weg ist, sollte ich meine Daten in gesonderten Bereichen/Partitionen aufbewahren

und immer nur die Datenbereiche öffnen, die ich gerade benötige. Für eine sichere Ablage meiner privaten Daten kann ich auf verschlüsselte Dateisysteme der einzelnen Betriebssysteme zurückgreifen oder die frei verfügbare Software TrueCrypt oder VeraCrypt nutzen, die es erlaubt, über Betriebssystemgrenzen hinweg nutzbare, verschlüsselte Datencontainer zu erzeugen.

Also:

- Daten und Programme auf dem Rechner trennen
- Regelmäßiges Backup der eigenen Daten
    - mehrere Backups (über 3 Generationen)
- Wichtige persönliche Daten verschlüsseln,
    - z.B. in Containern mit TrueCrypt/VeraCrypt, veracrypt.fr
    - und eventuell getrennt aufbewahren (USB Sticks, CDs)

Backup



Auch mein Backup-Konzept ist nun recht einfach. Das Host-System verändert sich nur bei System Updates und müsste im schlimmsten Fall nach einem Hardwarefehler des Rechners neu oder aus dem Backup wiederhergestellt werden. Die virtuellen Gastsysteme sollten nach jedem wichtigen Snapshot ins Backup kopiert werden. Nur noch meine eigenen Daten, beziehungsweise deren Änderungen müssen noch regelmäßig gesichert werden.

Jetzt kann ich mich je nach Anwendung (banking, spielen, mailen, surfen) von dem betreffenden Gastsystem auf den Weg ins Internet machen. Selbstverständlich sollte mein/jedes System durch eine Firewall geschützt sein.

Auf ins Internet

Surfen

Jetzt kann ich mir und meiner Daten sicher sein. Aber wie bewege ich mich nun anonym im Internet? Bevor ich mit meinem Browser ins Internet starte sollte ich mir dessen Einstellungen genauer ansehen. So kann ich die Ausführung von Java- und ActiveX-Programmen durch fremde Web-Seiten abstellen. Da inzwischen viele Web-Seiten mit Java Programmen ausgestattet sind, macht das Surfen dann nicht mehr viel Freude. Vielleicht kommt aber z. B. der eigene Bankrechner ohne Java aus.

Das gleiche gilt für Cookies, kleine Dateien, die nach dem Besuch vieler Web-Seiten auf dem eigenen Rechner gespeichert werden, um das Surfverhalten zu dokumentieren. Verbieten Sie Cookies vollständig, so werden Sie viele Web-Seiten nicht öffnen können. Ein Sicherheitsgewinn ist es jedoch, die Cookies und weitere persönliche Daten beim Schließen des Browsers von diesem löschen zu lassen. So kann man jederzeit durch Schließen und erneutes Öffnen des Browsers die ungewollt gespeicherten Daten löschen.

Da nicht bekannt ist, welche Daten die Betreiber von Suchmaschinen über uns speichern, lohnt es sicher auch öfter mal die Suchmaschine zu wechseln und möglichst nicht zu "googeln".

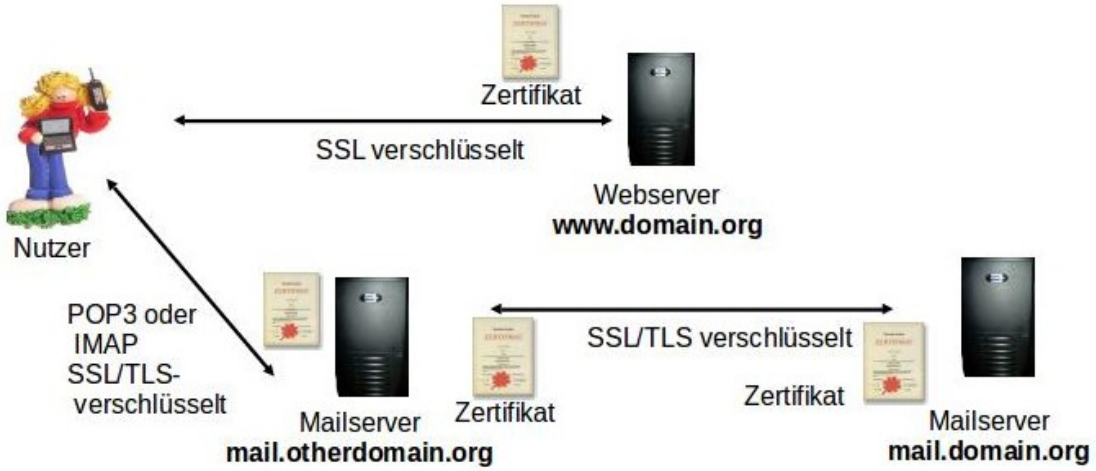
Zu empfehlen sind folgende Suchmaschinen (http://www.suchmaschinen-online.de/):

- Yacy - http://search.yacy.net
- Startpage - https://www.startpage.com/
- Ixquick - https://ixquick.com
- searX - https://www.searx.me
- seeks - http://seeks.org
- MetaGer - https://metager.de
- Googol - http://googol.warriordudimanche.net
- Gigablast - http://gigablast.com
- DeuSu - https://deusu.de
- Faroo - http://www.faroo.com

Bei der verteilten Suchmaschine Yacy kann Jede/r selbst mitmachen, in dem man den eigenen Rechner mit der Software laufen lässt - ist also ganz offen.
Startpage und Ixquick nutzen zur Suche Google (und andere Suchmaschinen wahrscheinlich auch), leiten aber meine Anfrage anonym dorthin weiter. Google erfährt also nicht, dass ich die Suche gestartet habe.

Surfen im Web

http ist unverschlüsselt
https ist SSL verschlüsselt, auch Server benötigen Zertifikate



URL

Wenn wir mit einem Browser im Internet unterwegs sind, wird in einer Zeile (meist oben) die URL (Uniq Resource Location), also die eindeutige Webadresse angegeben. Steht dort zu Beginn http so ist unsere Verbindung dorthin unverschlüsselt. Steht dort ein https so ist die Verbindung SSL (Secure Socket Layer) verschlüsselt. Um diese Verbindung sicher aufbauen zu können, benötigen auch Server Zertifikate, wie wir es bei der Mail gelernt haben. Auch unsere Verbindungen zum Mailserver beim Senden oder Holen von Mails sollte genauso verschlüsselt sein wie Verbindungen zu Webservern.

Die im Bild genannten Abkürzungen stehen für die Protokolle

- POP3 (Post Office Protokoll),
- IMAP (Internet Message Access Protocol)
- SMTP (Smple Mail Transport Protocol)
- SSL/TLS (Secure Socket Layer/Transport Layer Security)
  … auch nutzbar für DNS Server, WLAN- oder ssh- Verbindungen

Umwege - Proxies und Tor

Aber noch immer kann jeder Anbieter einer Webseite, die ich besuche durch meine IP Nummer feststellen, wer ich bin (indem er meinen Provider fragt) oder zumindest wann ich ihn schon einmal besucht habe. Dies kann ich umgehen, wenn ich mit meinem Browser einen Proxy Server nutze. Im meist benutzten freien Webbrowser Firefox kann ich solch einen Proxy unter "Einstellungen/Erweitert/Netzwerk/Einstellungen" angeben. Es gibt tausende offener Proxy Server im Internet. Nutze ich einen solchen Proxy, so geht meine Anfrage nach einer Webseite zuerst zu

diesem Proxy und er schickt sie mit seiner IP-Nummer dann weiter. Die Antwort kommt auf dem gleichen Weg zurück.

Ist das ein Sicherheitsgewinn? Ja, aber nur wenn ich dem Besitzer des Proxy Servers vertraue, denn dieser kann den Verkehr mitlesen. Ich habe mich zwar gegenüber dem Anbieter der aufgerufenen Webseite unsichtbar gemacht. Aber in keinem Fall sollte ich über diesen Weg vertrauliche Daten verschicken. Grundsätzlich sei noch einmal darauf hingewiesen, dass alle Daten beim normalen http-Protokoll auch Usernamen und Passwörter unverschlüsselt übertragen werden und damit auf ihrem Weg durchs Internet mitgelesen werden können. Nur bei dem sicheren https-Protokoll werden die Daten verschlüsselt durchs Internet transportiert. Ebenso verhält es sich mit dem unsicheren ftp File Transfer Dienst im Vergleich zum sftp (Secure File Transfer Protocol).

Eine Erweiterung der Nutzung eines Proxy Servers ist der Dienst FreeGate. Dieser wird von einem chinesischen Geschäftsmann angeboten, um Menschen in Ländern mit Zensurbestimmungen einen unkontrollierten Internetzugang anzubieten. Dazu ist es nötig ein Plugin im Web-Browser zu installieren. Man vertraut damit dieser Software und dem dadurch benutzten Proxy Servern irgendwo auf der Welt.

https ist notwendig aber nicht hinreichend

- der Inhalt der Kommunikation ist unterwegs sicher
- aber Anfangs- und Endpunkt sind beiden Seiten bekannt

Ein Proxy-Server kann den Anfangspunkt verschleiern

- Problem: Vertrauen gegenüber dem Proxy-Betreiber
- Lange Listen solcher Server gibt es im Internet

Einige freie Web-Proxies (ohne Gewähr):

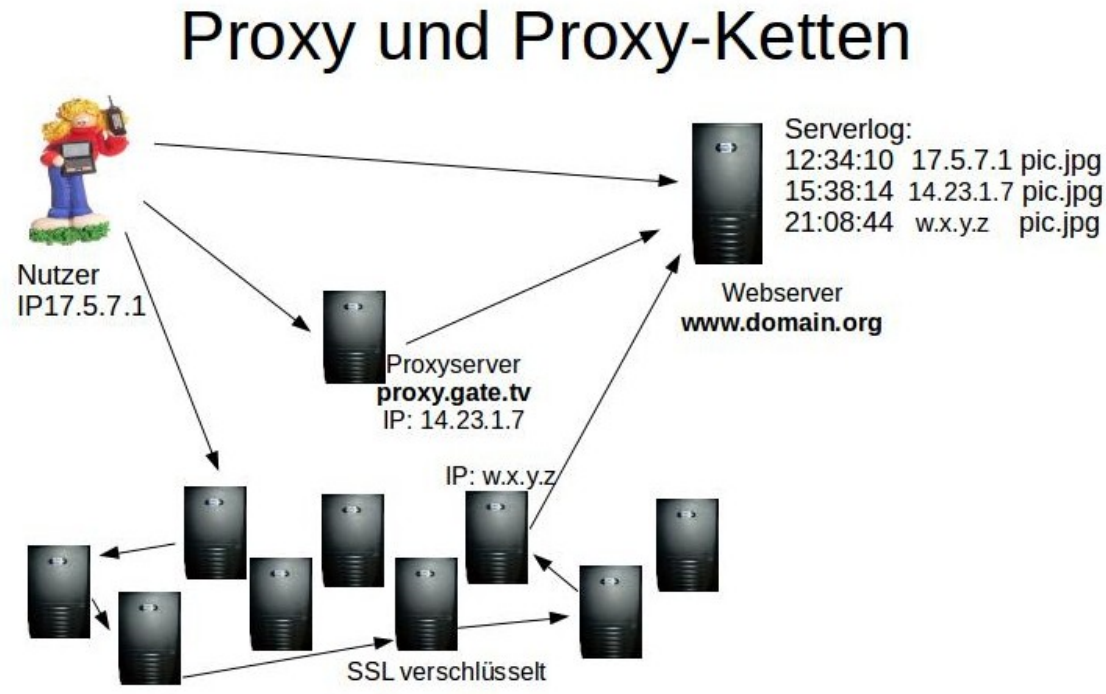
- https://www.proxyliste.com/
- https://www.workingproxies.info/proxies.shtml
- https://proxy.org/cgi_proxies.shtml
- https://www.proxywebsites.biz/
- https://www.kortaz.com/
- proxify.com
- proxeasy.com

Es bleibt das Problem, dass ich mit der Nutzung eines mir unbekannten Proxies auf dessen Ehrlichkeit vertraue.

-> Die Lösung wäre eine Reihe von Proxies, die nichts voneinander wissen.

Tor

Wir haben gesehen, dass der Umweg über einen Proxy uns zwar für den Anbieter der besuchten Webseite anonym macht, wir aber dem Besitzer des Proxies bekannt werden. Dieses Problem beheben die Dienste Tor und JAP. Für Tor (The Onion Router) muss man ein Plugin im Browser installieren, JAP (Java anonymer Proxy) ist ein eigenständiges Java Programm. Bei beiden Anwendungen wird nicht ein Proxy sondern eine ganze Kette in zufälliger und wechselnder Reihenfolge genutzt. Um zu verhindern, dass dadurch auch die ganze Kette von Serverbetreibern die Daten mitlesen können, wird der Verkehr innerhalb dieser Kette verschlüsselt übertragen. Die Kette, wie auch die Verschlüsselung tragen dazu bei, dass beide Dienste sich nicht durch Schnelligkeit auszeichnen. Der Gewinn ist dafür eine relativ hohe Anonymität, ... wenn man nicht vergessen hat vorher im Browser die Cookies der letzten Monate und andere persönliche Daten zu löschen .



Das sieht dann in der Log-Datei auf dem Web-Server so aus:

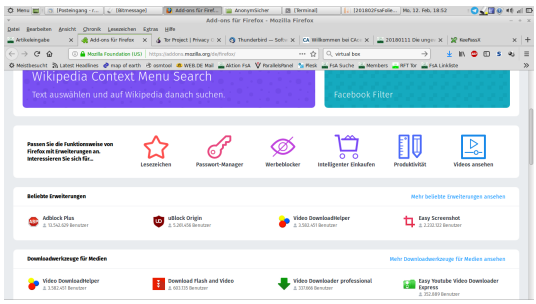
- wenn ich das Bild direkt mit seiner Webadresse aufrufe: 12:34: 1017.5.7.1 pic.jpg
- wenn ich über einen Proxy-Server gehe: 15:38: 1414.23.1.7 pic.jpg
- wenn ich eine Proxy-kette über Tor benutze: 21:08: 44 w.x.y.z pic.jpg

Infos über:

- Tor www.torproject.org
- German Privacy Foundation
- Humanistische Union Berlin
- JonDonym www.anonym-surfen.de

Bin ich im Tor Netzwerk wirklich anonym?

- der Eingangsproxy kennt meine IP
- der Ausgangsproxy weiß wohin ich will
- wenn ich nur http nutze, sehen beide auch den Inhalt
- der Zielrechner denkt, ich komme vom Ausgangsproxy
- der Zielrechner erfährt aber von mir
    - den Browsertyp,
    - meine Zeitzone,
    - mein Betriebssystem,
    - durch (Java-) Skripte auf den Webseiten können weitere Informationen erlangt werden
- -> Also im Browser NoScript, AddBlockPlus u.ä. nutzen



Anonym trotz Vorratsdatenspeicherung?

Ist das noch legal, wenn der Staat Hunderte von Millionen Euro pro Jahr für eine Vorratsdatenspeicherung ausgibt und ich mich ganz einfach mit Tor und JAP unsichtbar machen kann?

JAP wurde an der Universität Dresden mit Mitteln des Wirtschaftsministeriums gerade auch zum Schutz für deutsche Unternehmen entwickelt. Server für JAP werden in Deutschland unter anderem auch vom Unabhängigen Landesamt für Datenschutz (ULD) 17 in Kiel vom Datenschutzbeauftragten Schleswig-Holsteins betrieben. Das ULD konnte sich in mehreren Verfahren bescheinigen lassen, dass der Dienst im Einklang mit den deutschen Gesetzen steht.

Wer sich die Installation und Konfiguration der oben genannten Programme ersparen möchte kann auch eine für verschlüsselte E-Mail, VoIP-Telefon und anonymes Surfen mit Tor fertig konfigurierte CD mit einem Linux Live-System aus dem Internet herunterladen und nutzen.

Die CD wurde von der dänischen IT Gewerkschaft "IT-Politisk Forening" erstellt und ist auch mit deutscher Anleitung als ISO Image im Internet kostenlos erhältlich. ((https://www.aktion-freiheitstattangst.org/de/articles/419-polippix-cd-21-download-zur-umgehung-der-vorratsdatenspeicherung-120709.htm Die CD ist inzwischen leider veraltet!)

Grundsätzlich hat jedoch die Vorratsdatenspeicherung die Möglichkeit eingeschränkt sich anonym im Internet zu bewegen. Jeder Verbindungsaufbau und -abbau wird beim eigenen Internetprovider und jede verschickte oder empfangene E-Mail wird mit Absender- und Empfänger-Adresse und Uhrzeit beim E-Maildienst für sechs Monate gespeichert. Ein E-Mail-Provider außerhalb Europas kann also durchaus von Nutzen sein.

Verhalten in sozialen Netzwerken

Wozu?

- Kontakt im Freundeskreis
- Bloggen, eigene Meinung öffentlich kundtun

Was sollte man nicht tun?

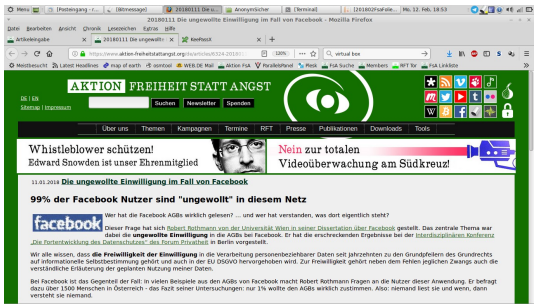
- eigene persönliche Daten öffentlich stellen
- Menschen auf Fotos mit persönlichen Daten markieren

Welche Netzwerke sind empfehlenswert?

- Diaspora (dezentral, Open Source, Profil löschbar)
- Comyuno (Freundeskreis bleibt unter sich, komplett löschbar)

Welche nicht?

- Facebook (AGBs verlangen vollständige Unterwerfung)
- WhatsApp (gehört Facebook)
- Instagram (einige Privacy-Einstellungen sind möglich)
- Snapchat (einige Privacy-Einstellungen sind möglich)
- u.v.a. (Youtube, Vimeo, Flickr, …)



Zum Thema Facebook verweisen wir gern auf die Dissertation „Die Rechtswirklichkeit der informierten Zustimmung“ von Robert Rothmann (Uni Wien), der darin festgestellt hat, dass 99% der Nutzer dieses Dienstes sich nie dort angemeldet hätten, wenn sie gewusst hätten, welchen Bedingungen sie damit zustimmen. Wir empfehlen dazu unseren Artikel „Die ungewollte Einwilligung im Fall von Facebook“.

Wenn es mir nur um synchrones Chatten geht, dann gibt es viele weitere Messenger, insbesondere für Smartphones aber auch für Laptops.

Wer wegen des Abziehen von privaten Daten, wie z.B. um meine privaten Kontakte, um WhatsApp einen Bogen machen möchte, muss

1. eine Alternative suchen und
2. seine Kommunikationspartner davon überzeugen sich diese App ebenfalls runterzuladen.

Wir haben eine Liste von Privatsphäre-schützenden Apps gesammelt.

Vor der Benutzung von Facebooks Produkt WhatsApp können wir nur warnen. Trotz seiner angeblichen Ende-zu-Ende Verschlüsselung aller Nachrichten ist die App ständig auf der Suche nach den persönlichen Daten auf dem Handy (Kontakte, E-Mail Adressen, Standort, …).

Deutsche Gerichte und die Datenschutzbeauftragten mehrerer Bundesländer haben eindeutig festgestellt, dass die Nutzung von WhatsApp in der Regel sogar rechtswidrig ist, weil man damit

die Privatsphäre, explizit die Mailadressen und Telefonnummern seiner Freunde unerlaubt, d.h. ohne deren Einwilligung weitergibt. (https://www.aktion-freiheitstattangst.org/de/articles/6390-20180304-99-aller-whatsapp-nutzer-sind-datenhehler.htm)

Neben der proprietären Verschlüsselung nutzt WhatsApp Server in den USA. Was es alles sonst noch an Facebook zu kritisieren gibt steht hier https://www.aktion-freiheitstattangst.org/de/articles/2532-20111130-facebook-privatsphaere-leitfaden.htm

Privatsphäre-schützende Messenger

Die folgende Tabelle enthält Alternativen für Messenger-Dienste, die meist Privatsphäre-schonender mit den Daten ihrer Nutzer umgehen.

Tabelle: **Privatsphäre-schützende Messenger**

App	+	-
Briar Beta	Ende-zu-Ende verschlüsselt, Kontakte müssen sich einen persönlichen Qrcode zeigen	Kontakte erzeugen geht nur, wenn man sich trifft und ist manchmal auch noch schwierig. Die Version ist noch im Beta-Stadium.
ChatSecure	Open Source XMPP kann mit OTR Ende-zu-Ende verschlüsselt werden	Im Original nur SSL/TLS-Verschlüsselt zwischen den Servern, dort aber unverschlüsselt
Conversations	Ende-zu-Ende verschlüsselt	Installation schwierig, fehlerhaft auf Linux Desktop (heißt dort gajim)
Signal	Open Source Client Ende-zu-Ende verschlüsselt, von Edward Snowden empfohlen,	geht nicht auf Samsung Tab A, SM T580
Telegram	Open Source Client Anleitung https://telegram.org/faq/de	Geheime Server-Software, Desktop Version kann nicht verschlüsseln, Verschlüsselung geheim, zentralisierte US-Server, Kontakt- und Metadaten werden gespeichert
Threema	Open Source Client	Geheime Server-Software, Verschlüsselung geheim,
Tigase	XMPP Messenger	Messenger mit offenem Protokoll
Xabber, ….	Open Source XMPP kann mit OTR Ende-zu-Ende verschlüsselt werden	Im Original nur SSL/TLS-verschlüsselt zwischen den Servern, dort aber unverschlüsselt
Yaxim	XMPP Messenger	Messenger mit offenem Protokoll

Fazit

Was ist zu tun?

- Kommunikation im Internet verschlüsseln
- Surfen möglichst SSL-verschlüsselt (https://...)
- E-Mails lesen und schreiben mit Thunderbird und Enigmail Plugin
- GnuPG und/oder X.500/OpenSSL installieren
- Firewall und Virenschutz
- Aktuelle Virenschutz Software installieren und regelmäßig updaten
- Firewall auf dem Rechner verstehen und benutzen
    - (eigene strikte Regeln je nach Bedarf einsetzen)
- Die eigenen Daten sicher aufbewahren
- Daten und Programme auf dem Rechner trennen
- Ordner mit wichtigen persönlichen Daten verschlüsseln (TrueCrypt)
    - regelmäßige Datensicherung/BackUp
- Anwendungen trennen
- verschiedene (virtuelle) Rechner für verschiedene Anwendungen (Surf-PC, Bankrechner, Spiele-PC, ...)
- Virtualisierung mit VirtualBox, VMware, Xen, ...

Es gilt das Prinzip der abgestuften Sicherheit. Genauso wie ich die Leistungsfähigkeit meines PCs skalieren kann und entscheiden muss, was ich mit welchen Mittel angehe, so muss ich auch entscheiden, welche Mittel ich für die Sicherheit meiner Daten einsetze.

Ganz wichtig bleibt auch, dass ich mich beim Surfen im Internet nicht selbst verleiten lasse persönliche Daten Preis zu geben, denn die Datensammelwut von privaten und staatlichen Stellen ist ungebremst. Jeder Bundesbürger ist mit seinen persönlichen Daten ohne sein Wissen schon jetzt in über 50 Datenbanken erfasst [20].

Das Bundesverfassungsgericht hat mehrfach festgestellt, dass die Informationelle Selbstbestimmung ein Grundrecht ist. Wie jedes Grundrecht muss es aber auch von jedem Einzelnen verteidigt und durchgesetzt werden.

Nach den Datenskandalen im letzten Jahr (Telekom, Lidl, LBB Bankdaten, ...) und den wachsenden Begehrlichkeiten an unseren Daten von staatlicher Seite wurde uns versprochen, den Datenschutz, in Deutschland also das BDSG, an den Stand der Zeit anzupassen. Das steht nun ab Mai 2018 mit dem Inkrafttreten der EU Datenschutzgrundverordnung (DSGVO) an.

Verweise

1 Die-Wegwerf-Mail-Adresse http://www.sofort-mail.de/
2 Mozilla Thunderbird Mail http://www.mozilla-europe.org/de/products/thunderbird/
3 Enigmail-Verschlüsselung http://enigmail.mozdev.org/
4 VMware http://www.vmware.com/de/
5 Parallels http://www.parallels.com/de
6 Virtual Box http://www.virtualbox.org/
7 True Crypt http://www.truecrypt.org/
8 Firewall Builder http://www.fwbuilder.org/
9 Suchmaschinen http://www.suchmaschinen-online.de/
10 Mozilla Firefox http://www.mozilla-europe.org/de/firefox/
11 freie Proxies http://www.proxyliste.com/
12 Open SSH http://www.openssh.com/de/
13 Freegate http://de.wikipedia.org/wiki/Freegate http://www.dit-inc.us/
14 TOR http://www.torproject.org/
15 JAP http://anon.inf.tu-dresden.de/
16 Tor Plugin für Firefox https://addons.mozilla.org/de/firefox/addon/5833
17 ULD http://www.datenschutzzentrum.de/
18 Polippix http://itpol.polcast.dk/sager/polippix/polippix-den-politisk-cd-privatlivets-fred/
19 dt. Polippix CD ISO Image http://a-fsa.de/d/17u
20 Datenmissbrauch http://www.welt.de/webwelt/article2328711/Die-Daten-aller-Deutschen-sind-im-Umlauf.html

Weitere Links

Freiheitsrechte:

Deutsches Institut für Menschenrechte www.institut-fuer-menschenrechte.de
Humanistische Union www.humanistische-union.de
Statewatch www.statewatch.org
Abgeordnetenwatch ; www.abgeordnetenwatch.de
Informationsstelle Militarismus www.imi-online.de

Online-Freiheitsrechte:

Chaos Computer Club www.ccc.de
European Digital Rights Initiative www.edri.org www.unwatched.org
ULD Schleswig-Holstein www.datenschutzzentrum.de
Electronic Frontier Foundation www.eff.org/issues/eff-europe

Verschlüsselung:

www.gnupg.org
www.thunderbird-mail.de
www.openssl.org
enigmail.mozdev.org
www.truecrypt.org

Weitere Infos bekommt man hier:

Sicherheit beim Surfen https://wiki.ubuntuusers.de/Sicherheit/Anonym_Surfen
Mögliche Gefahren in Tor Netzwerken https://wiki.ubuntuusers.de/Tor/Gefahren
Was sieht das Internet über mich beim Surfen https://www.heise.de/netze/tools/ip/
E-Mail- und Festplattenverschlüsselung https://computergruppe.h48.de/
Vorteile von Linux https://computergruppe.h48.de/index.php?n=Links.WarumLinux?
Anonym und sicher im Internet http://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-2018/sid-veranstaltungen-2018/berlin-anonym-amp-sicher-im-internet/
und https://www.aktion-freiheitstattangst.org/de/articles/1004-sicher-im-internet.htm
und "was kann ich tun" https://www.aktion-freiheitstattangst.org/de/articles/4185-privatsphaere-schuetzen-was-kann-ich-tun.htm
und "technische Hinweise" https://www.aktion-freiheitstattangst.org/de/articles/4238-technische-hinweise-um-der-ueberwachung-zu-entgehen.htm