
Sicherheit
im Internet und auf dem Heim-PC

Es **war**
einmal...

Ich möchte zum Einstieg eine kleine Geschichte erzählen.

Sie handelt von Stefan, einem ahnungslosen Internet- und PC-Benutzer.

- Stefan Freitagabend allein am Laptop, Frau ist im Urlaub
- E-Mail von Bank mit Bitte, er möge Online-Banking kontrollieren mit PIN und TAN
- Klick auf den Link in der E-Mail
- Alles scheint in Ordnung
- Stefan geht schlafen

- Samstagmorgen Schreiben einer Anwaltskanzlei im Briefkasten
- angeblich MP3s von Bushido in Peer-to-Peer-Netzwerk zum Download angeboten
- 650,- EUR Anwaltsgebühren bezahlen ansonsten Rechtsstreit
- Stefan kennt weder Bushido noch P2P

- Stefan stellt PC ein und sucht im Internet nach Hilfe
- Link eines Forenteilnehmers angeklickt
- Bildschirm gesperrt, Warnung der GEMA
- PC war nicht mehr benutzbar
- Wochenende gelaufen, da kein Internet
- Frau hat Zweitlaptop mit, kommt erst Sonntagabend zurück

- Montagmorgen Stefan fährt mit U-Bahn zur Arbeit
- nimmt Laptop der Frau mit um in Pause nach Trojaner zu suchen
- Laptop wird ihm gestohlen
- sämtliche privaten Fotos seiner Familie drauf, nicht extern gesichert → Frau sauer!
- wenigstens Windows-Konto mit Passwort geschützt, Dieb hat also keine Daten

- Arbeitgeber untersagt private Internetnutzung
- in Mittagspause ins Internetcafe, wg. GEMA-Meldung
- Fake, aber spezielle Software nötig, um seinen PC zu befreien
- soll 20 EUR kosten, er bestellt

- Stefan will 20 EUR überweisen
- Login bei Bank
- Konto leer
- Bank hat Mittagspause → warten

- GEMA nervt trotzdem
- anderes Konto, mit Kreditkarte
- Kreditkartendaten auf Website eingeben

- schnell noch Bestellungseingang per Mail kontrollieren
- ab zur Bank
- Rückbuchung erfolgreich

- GEMA geklärt, aber Abmahnung wartet
- Anwalt kontaktiert, Abmahnung für 200 EUR abgewehrt

- am nächsten Samstag: Rechnungen der Kreditkartenfirma
- Käufe von Waren im Ausland
- Zweitkonto bereits im Minus

- Anwalt hat Wochenende, also Mail
- Zugang wird verwehrt
- falsches Passwort
- am Montagmorgen gleich zu EDV-Kollegen
- im Büro lächeln ihn alle seltsam an

- sein Sitznachbar schaut sich gerade Stefans Frau im Bikini bei Facebook an

Publikum fragen: Was hat Stefan alles falsch gemacht?
→ Handout im Blog

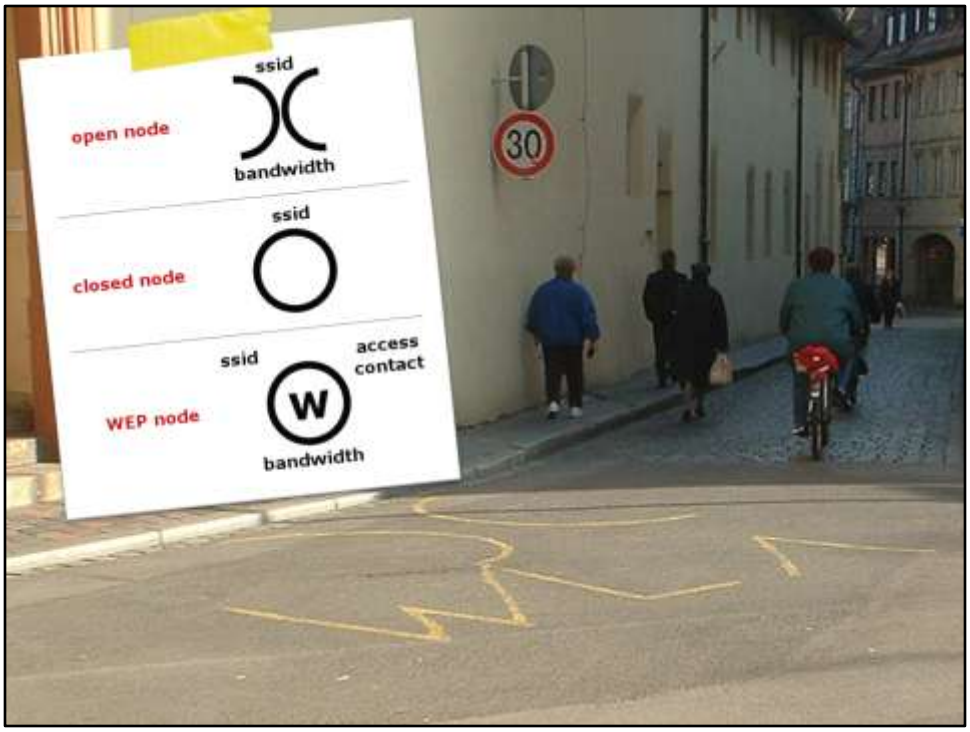
Stefan hat auf verschiedenen Ebenen Fehler gemacht: im Netzwerk, auf seinem PC/Betriebssystem und beim Browsen/Mailen.

Schauen wir uns zunächst einmal die Netzwerkebene an.
Teilnehmer fragen: Wer hat ein WLAN zuhause?

WLAN

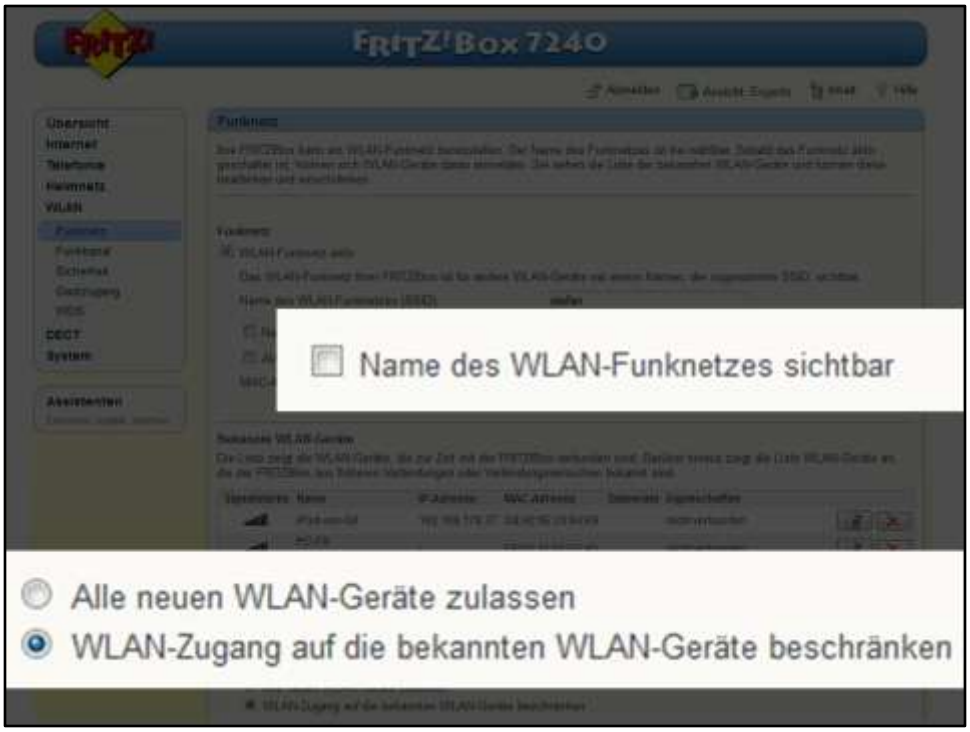
Sichere Passwörter

Firewall



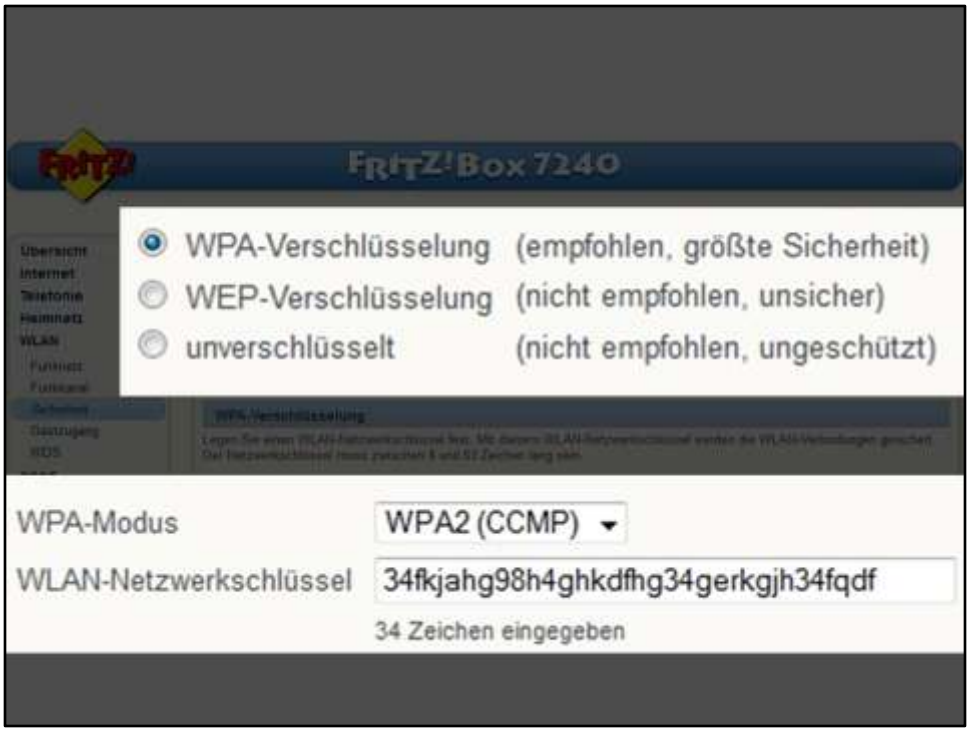
Stefan hat keine Ahnung von P2P und dennoch eine Abmahnung bekommen. Wie kann das sein? → Er hat sein WLAN gar nicht oder nicht gut genug abgesichert, sodass es von Angreifern zum Surfen genutzt werden kann. In großen Städten gibt es das sog. Warchalking, bei dem offene oder leicht zugängliche WLANs mit Kreide gekennzeichnet werden.


FRITZ!Box 7240
Abmelden
Ansicht: Experte
Inhalt
Hilfe
Übersicht
Internet
Telefonie
Heimnetz
WLAN
Funknetz
Funkkanal
Sicherheit
Gastzugang
WDS
DECT
System
Assistenten
Funknetz
Ihre FRITZ!Box kann ein WLAN-Funknetz bereitstellen. Der Name des Funknetzes ist frei wählbar. Sobald das Funknetz aktiv geschaltet ist, können sich WLAN-Geräte daran anmelden. Sie sehen die Liste der bekannten WLAN-Geräte und können diese bearbeiten und einschränken.
Funknetz
WLAN-Funknetz aktiv
Das WLAN-Funknetz Ihrer FRITZ!Box ist für andere WLAN-Geräte mit einem Namen, der sogenannten SSID, sichtbar.
Name des WLAN-Funknetzes (SSID):
stefan
Name des WLAN-Funknetzes sichtbar
AVM Stick & Surf aktivieren
MAC-Adresse dieser FRITZ!Box:
00:24:FE:A4:25:2F
Bekannte WLAN-Geräte
Die Liste zeigt die WLAN-Geräte, die zur Zeit mit der FRITZ!Box verbunden sind. Darüber hinaus zeigt die Liste WLAN-Geräte an, die der FRITZ!Box aus früheren Verbindungen oder Verbindungsversuchen bekannt sind.
Signalstärke
Name
IP-Adresse
MAC-Adresse
Datenrate
Eigenschaften
iPad-von-Gil
192.168.178.27
D8:A2:5E:33:94:E9
nicht verbunden
PC-F9-D1-11-31-D3-40
F8:D1:11:31:D3:40
nicht verbunden
Philips-BD
192.168.178.34
5C:33:8E:72:66:5C
nicht verbunden
Samsung(1)
192.168.178.27
84:07:F9:85:83:F4
26 MBit/s
WPA2, WMM
SonyEricsson
192.168.178.36
84:00:D2:A5:F8:D3
nicht verbunden
Die angezeigten WLAN-Geräte dürfen untereinander kommunizieren
WLAN-Gerät hinzufügen
Alle neuen WLAN-Geräte zulassen
WLAN-Zugang auf die bekannten WLAN-Geräte beschränken



- Unsichtbare SSID ist kein echter Schutz, aber hilft gegen Script Kiddies
- MAC kann gefälscht werden, aber dazu muss eine erlaubte MAC bekannt sein


FRITZ!Box 7240
Abmelden
Ansicht: Experte
Inhalt
Hilfe
Übersicht
Internet
Telefonie
Heimnetz
WLAN
Funknetz
Funkkanal
Sicherheit
Gastzugang
WDS
DECT
System
Assistenten
Sicherheit
Verschlüsselung
WPS - Schnellverbindung
Legen Sie hier fest, wie Ihr WLAN-Funknetz gegen unberechtigte Nutzung und gegen Abhören gesichert werden soll.
WPA-Verschlüsselung (empfohlen, größte Sicherheit)
WEP-Verschlüsselung (nicht empfohlen, unsicher)
unverschlüsselt (nicht empfohlen, ungeschützt)
WPA-Verschlüsselung
Legen Sie einen WLAN-Netzwerkschlüssel fest. Mit diesem WLAN-Netzwerkschlüssel werden die WLAN-Verbindungen gesichert. Der Netzwerkschlüssel muss zwischen 8 und 63 Zeichen lang sein.
WPA-Modus
WPA2 (CCMP)
WLAN-Netzwerkschlüssel
34 Zeichen eingegeben
Übernehmen
Abbrechen
Hilfe



- WEP ist schon geknackt
- Auch WPA kann geknackt werden, wenn das Passwort schwach ist

WLAN
Sichere **Passwörter**
Firewall

Teilnehmer fragen: Wer kennt den Computer?

- Passwörter sind sicher, wenn es sehr lange dauert, sie mit heute verfügbarer Technik zu knacken
- Sichere Passwörter sind in allen anderen genannten Bereichen wichtig!

Brute Force

Mögliche **Kombinationen**:

[Anzahl Zeichen][Anzahl Stellen]

[a-z A-Z 0-9 !$%&...] 10 Stellen

(26 + 26 + 10 + 20) ^{10}

82^{10} = 13.744.803.133.596.058.624

→ **44,6 Mio.** Jahre (10.000 Kom./s)

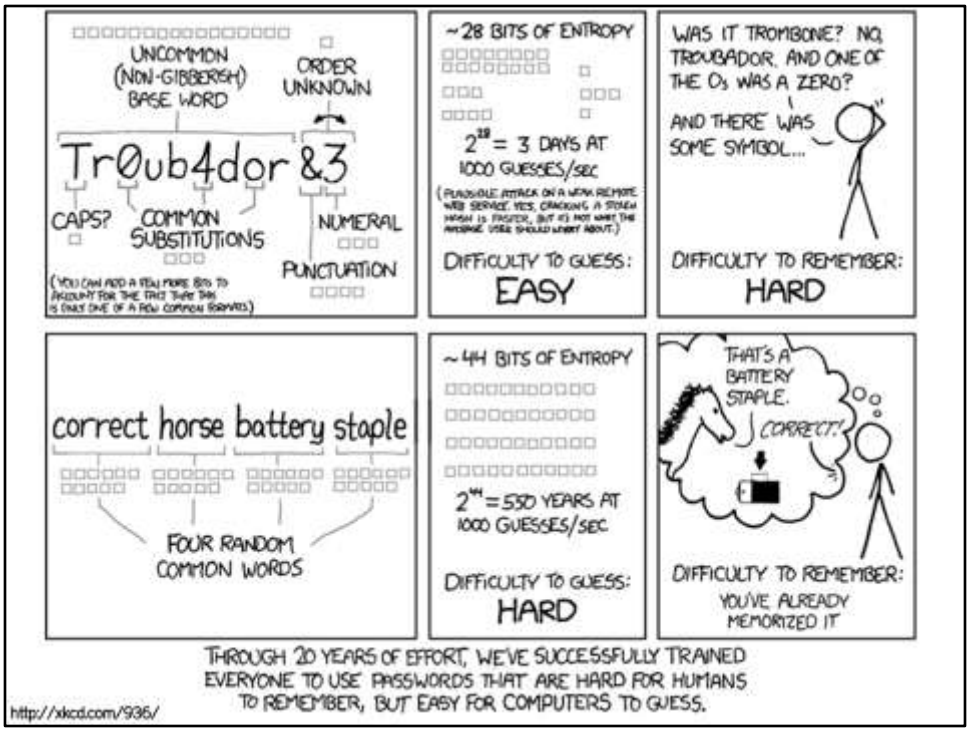
- Wörterbuchattacken: Mittel für Angreifer, Laufzeit zu verringern
- Beliebteste Passwörter 2011 laut http://splashdata.com/splashid/worst-passwords/index.htm

Passwort**sätze**

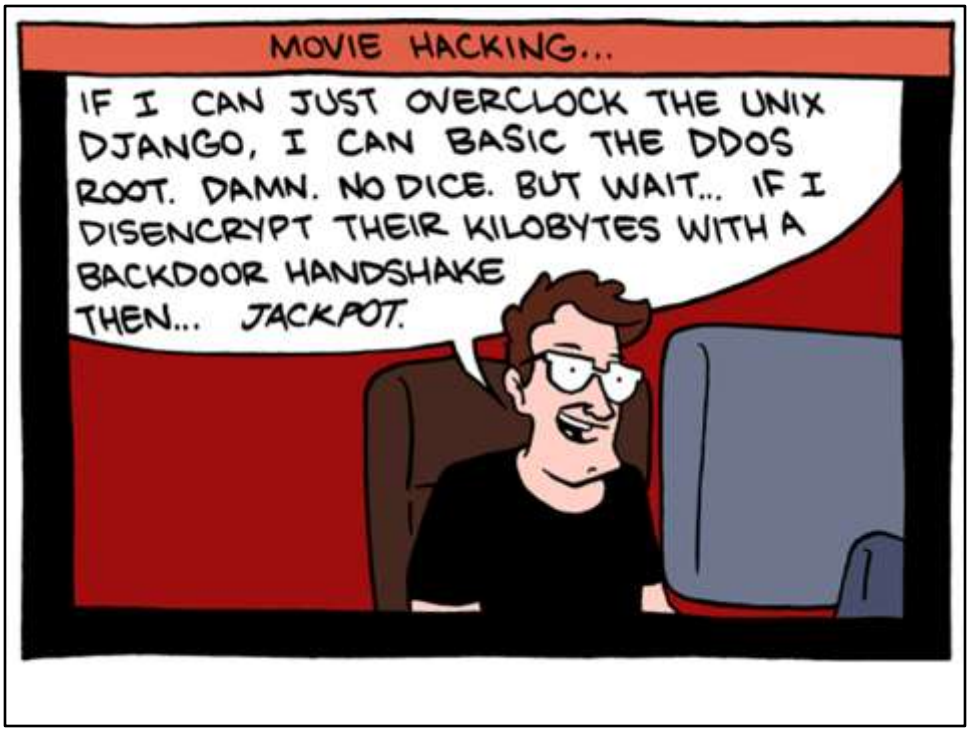
komplexes Pw.: 82^{10} = **$1{,}4 * 10^{19}$** Kombi.
vs. nur Buchstaben (52 Zeichen)

→ log(82^{10}) / log(52) = 11,15 → 12 Stellen
52^{12} = **$3{,}9 * 10^{20}$**

„diesisteingutesPasswort"
52^{23} = **$2{,}9 * 10^{39}$**


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.
http://xkcd.com/936/

„Social Engineering“ → Passwörter niemals herausgeben, auch nicht an den IT-Support

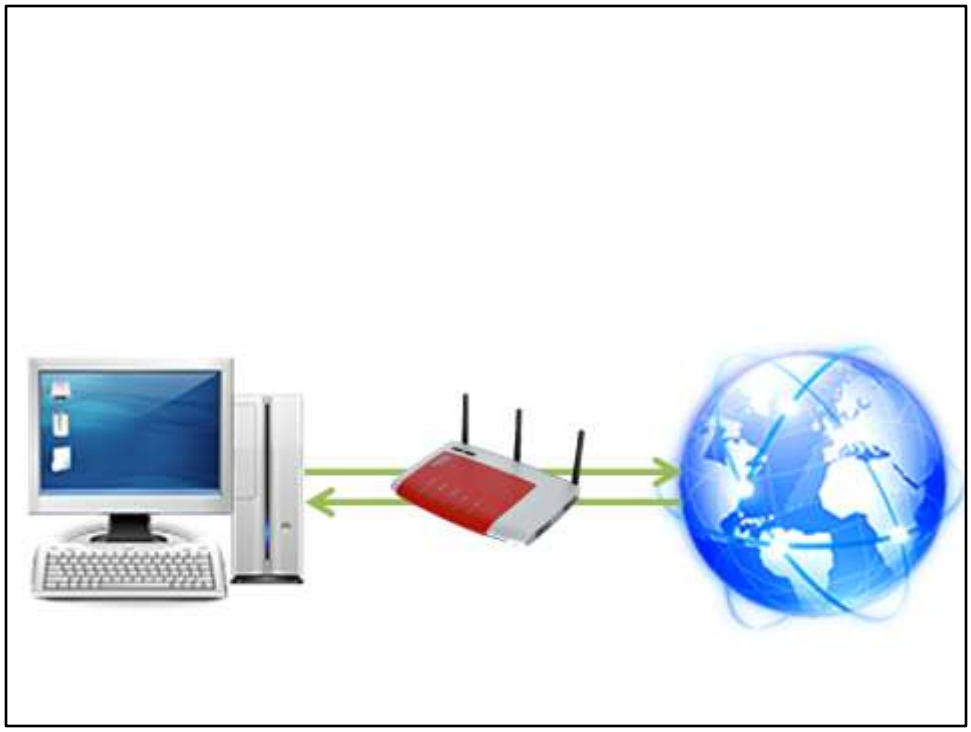

MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.

http://www.smbc-comics.com/index.php?db=comics&id=2526

WLAN

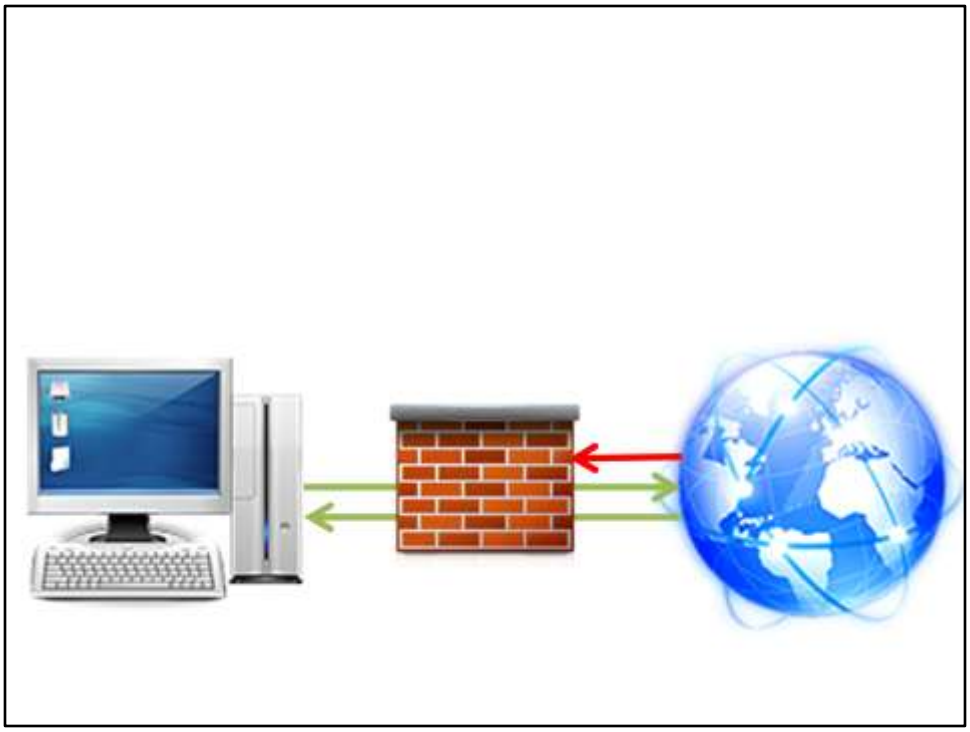
Sichere Passwörter

Firewall

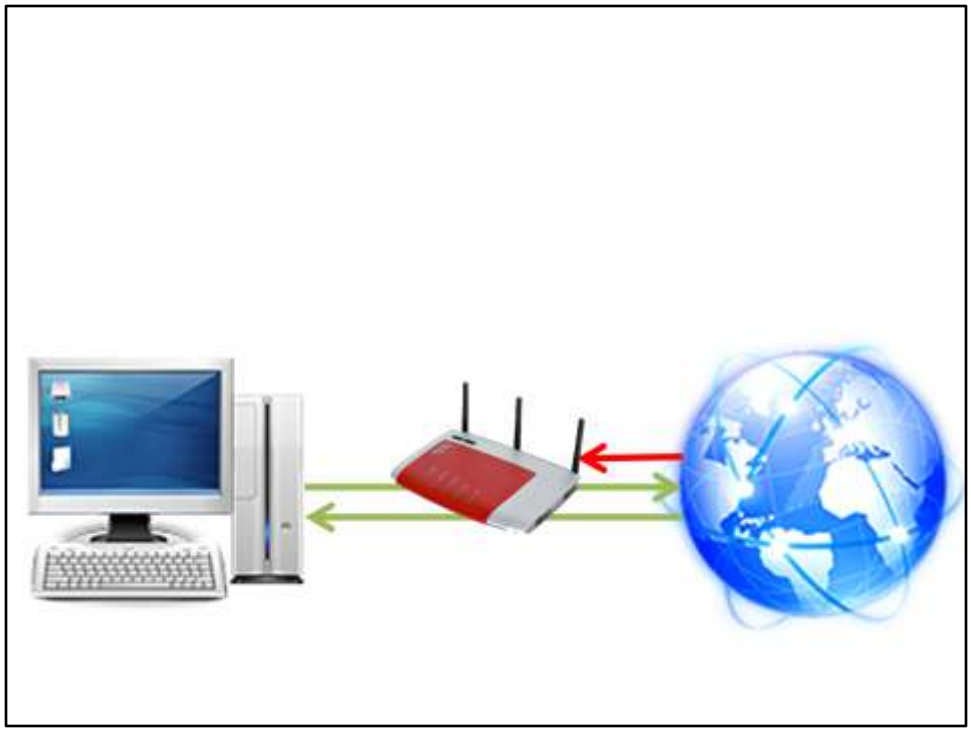


Die meisten privaten Netzwerke sehen so aus: Computer geht über Router ins Internet. Der Router lässt den ein- und ausgehenden Verkehr durch. Das ist ok, solange es nur gewünschten Netzwerkverkehr gibt.
Teilnehmer fragen: Wer hat keinen Router zuhause, sondern nutzt direkt ein (DSL-)Modem?

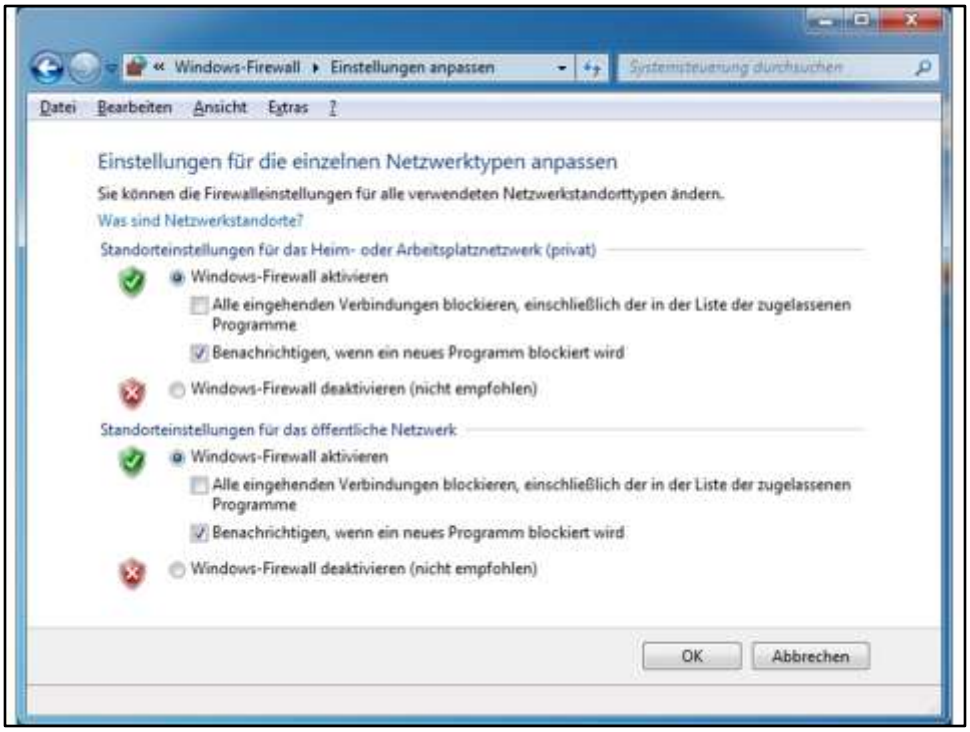
Doch was ist mit gefährlichem eingehenden Netzwerkverkehr? Dafür brauchen wir eine Firewall.
ISPs gehen von bis zu 50% Grundrauschen auf dem Netzwerk aus, von dem ein Großteil automatisierte Angriffe gegen IP-Adressbereiche sind (und natürlich Spam).

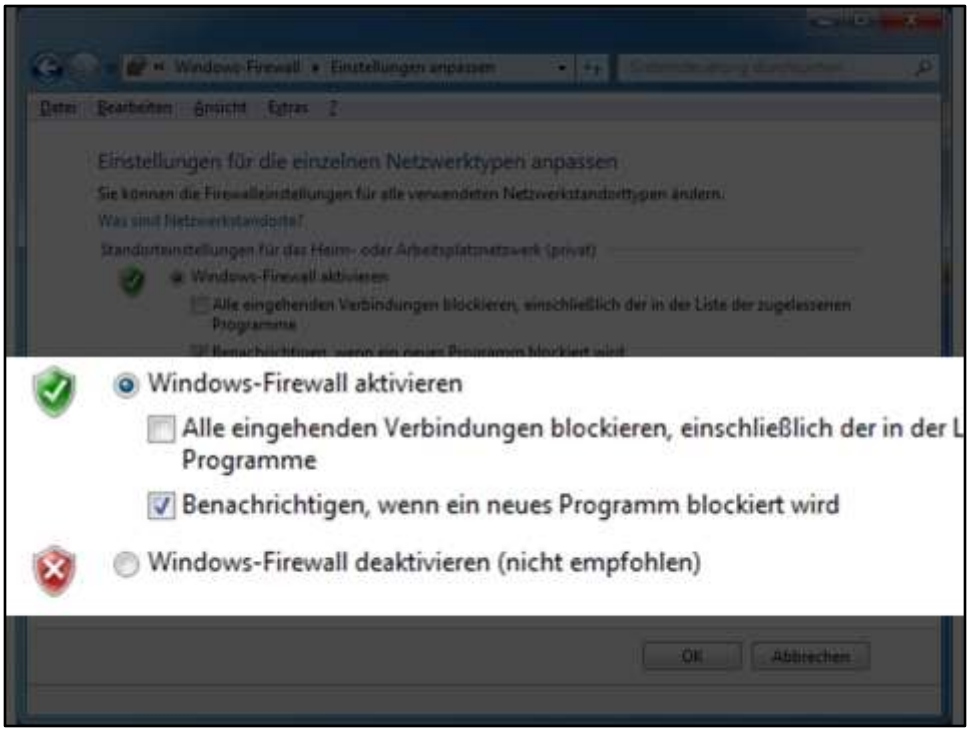


Eine Firewall blockiert unerwünschte Zugriffe von innen/außen, aber lässt gewünschte Verbindungen zu.



- Alle Router haben eine Firewall bereits eingebaut, sie muss nur aktiviert werden.
- Ansonsten reicht die Windows-Firewall
- Eigentlich nur nötig, wenn direkt im Internet und nicht hinter Router
- Vorsicht bei öffentlichen WLAN-Zugängen


« Windows-Firewall ▸ Einstellungen anpassen
Systemsteuerung durchsuchen
Datei Bearbeiten Ansicht Extras ?
Einstellungen für die einzelnen Netzwerktypen anpassen
Sie können die Firewalleinstellungen für alle verwendeten Netzwerkstandorttypen ändern.
Was sind Netzwerkstandorte?
Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)
Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)
Standorteinstellungen für das öffentliche Netzwerk
Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)
OK
Abbrechen

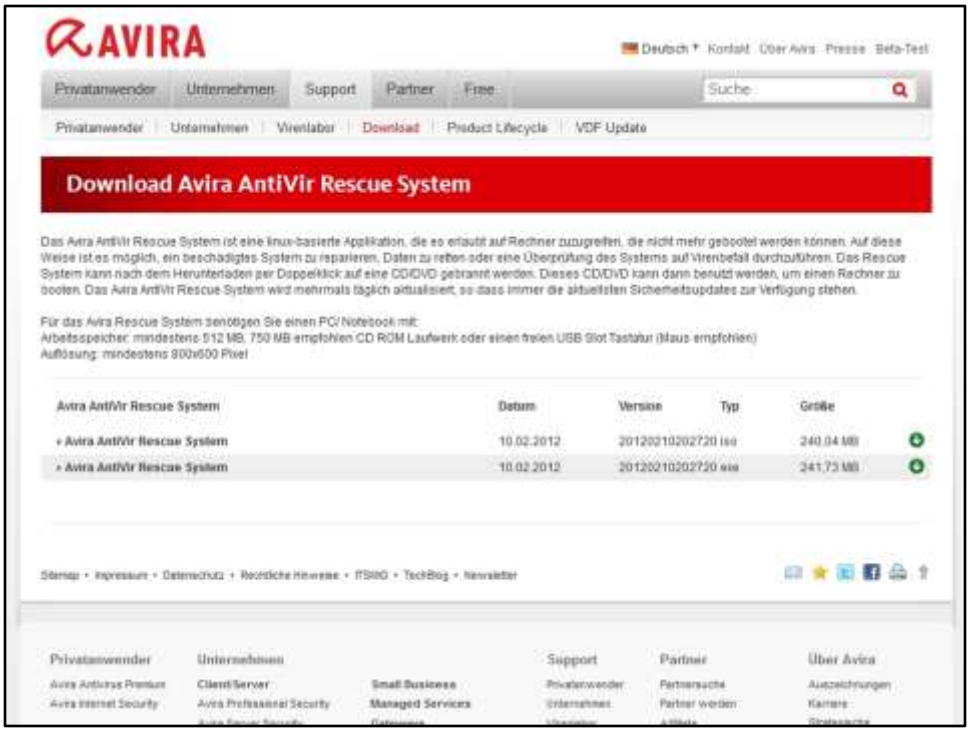

Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der L
Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)

Kommen wir nun zur Ebene des PCs/Betriebssystems.

Kommen wir nun zur Ebene des PCs/Betriebssystems.

- Virenscanner ist Geschmackssache
- einer reicht, nicht zwei gleichzeitig
- das Wichtigste sind die regelmäßigen Updates

Auf http://www.testvirus.de kann man die korrekte Funktionsweise seines Virenscanners testen.

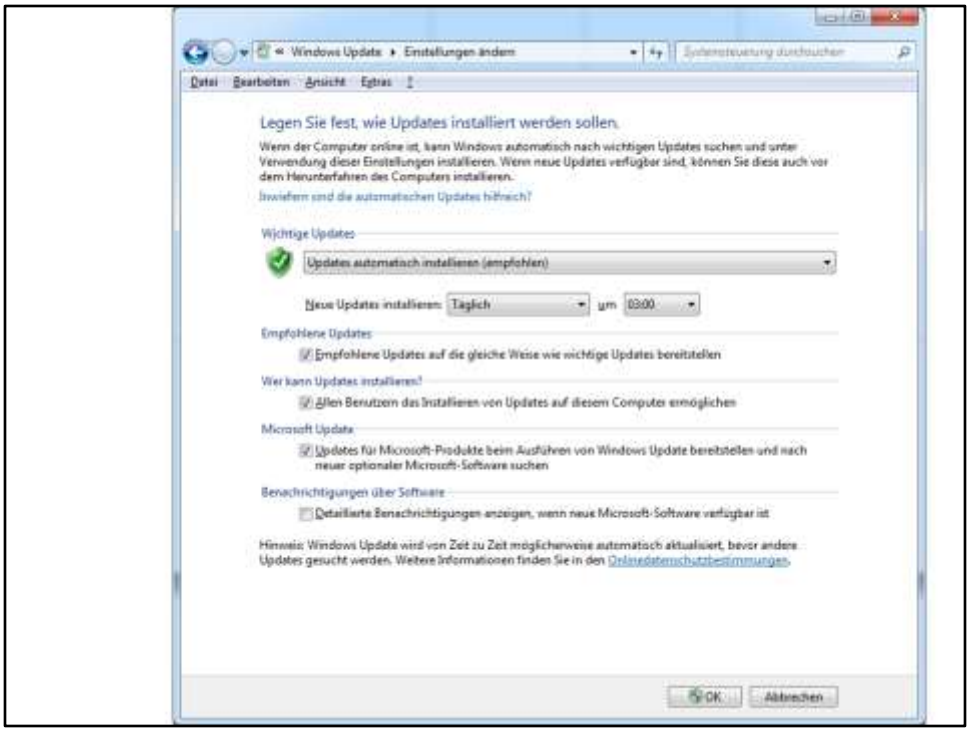


Und als Vorbereitung auf den Ernstfall sollte man eine Live-CD mit Virenscanner bereithalten, wie zahlreiche Hersteller sie anbieten.
http://www.avira.com/de/support-download-avira-antivir-rescue-system

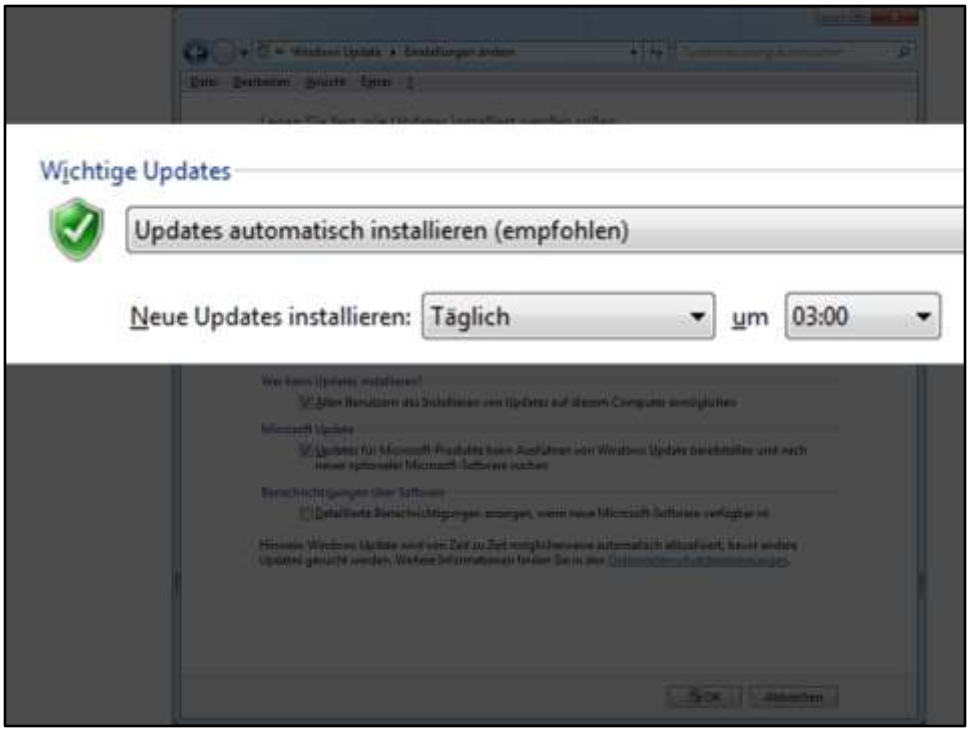
Virenschutz

Softwareupdates

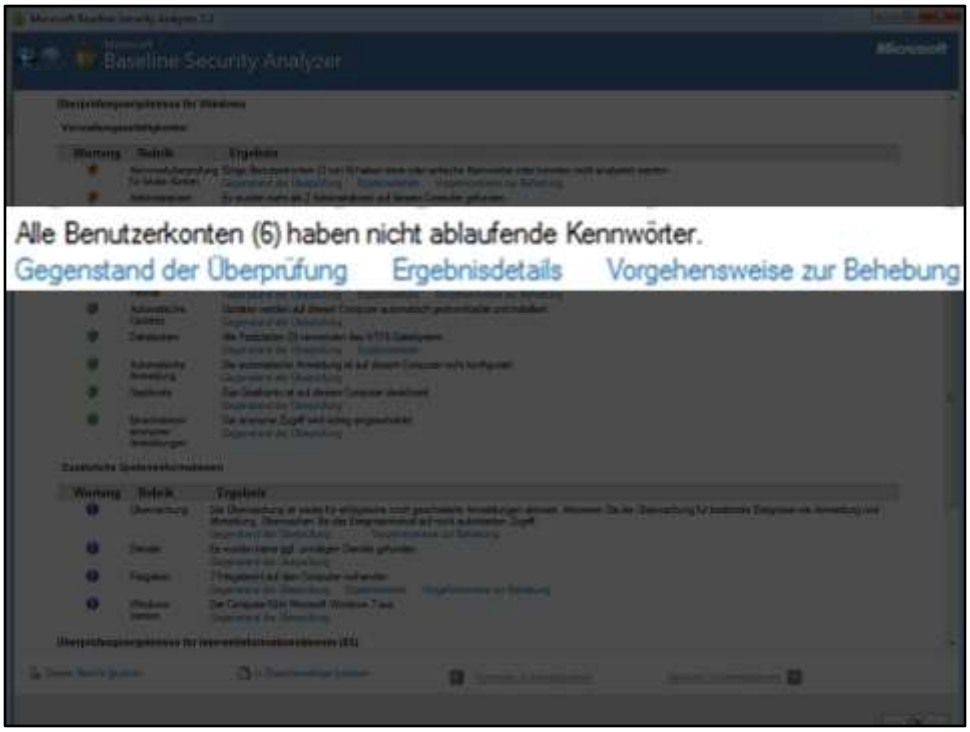
Datensicherheit



Die Windows Updates sollten konfiguriert sein. Windows ohne Updates am Netz → in wenigen Minuten mit Schädlingen befallen.


Wichtige Updates
Updates automatisch installieren (empfohlen)
Neue Updates installieren:
Täglich
um
03:00

Der MBSA prüft einige grundlegenden Sicherheitseinstellungen…



…und zeigt sie verständlich beschrieben an, damit sie behoben werden können.

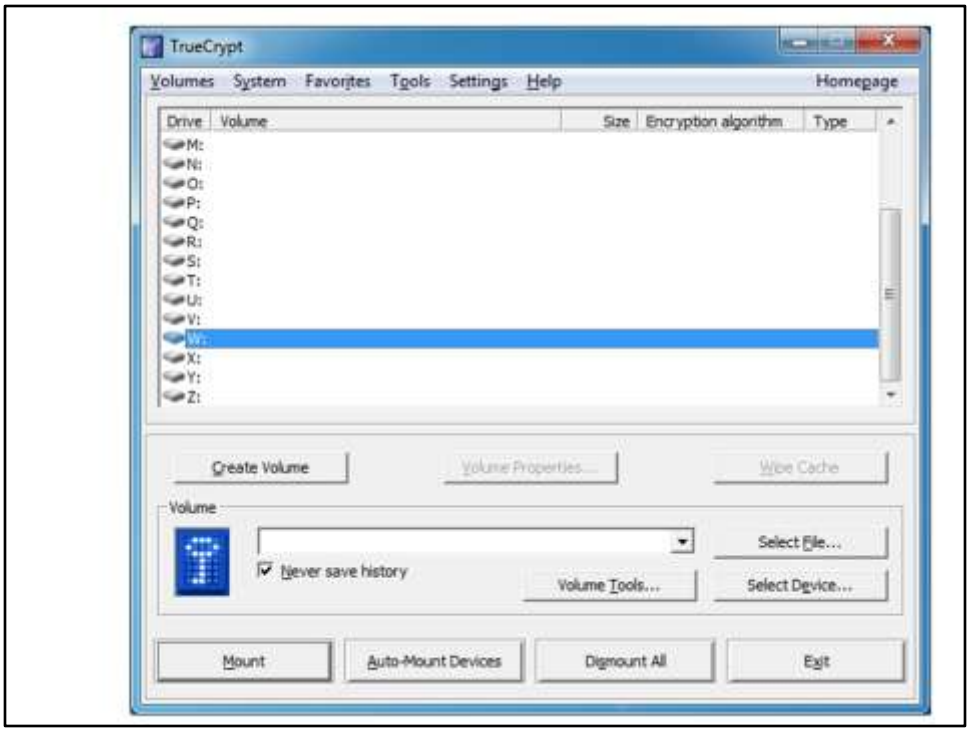
Ein großes Problem gerade in letzter Zeit waren Sicherheitslücken in Java → Updates aktivieren!

PSI scannt für alle anderen installierten Programme nach Updates…

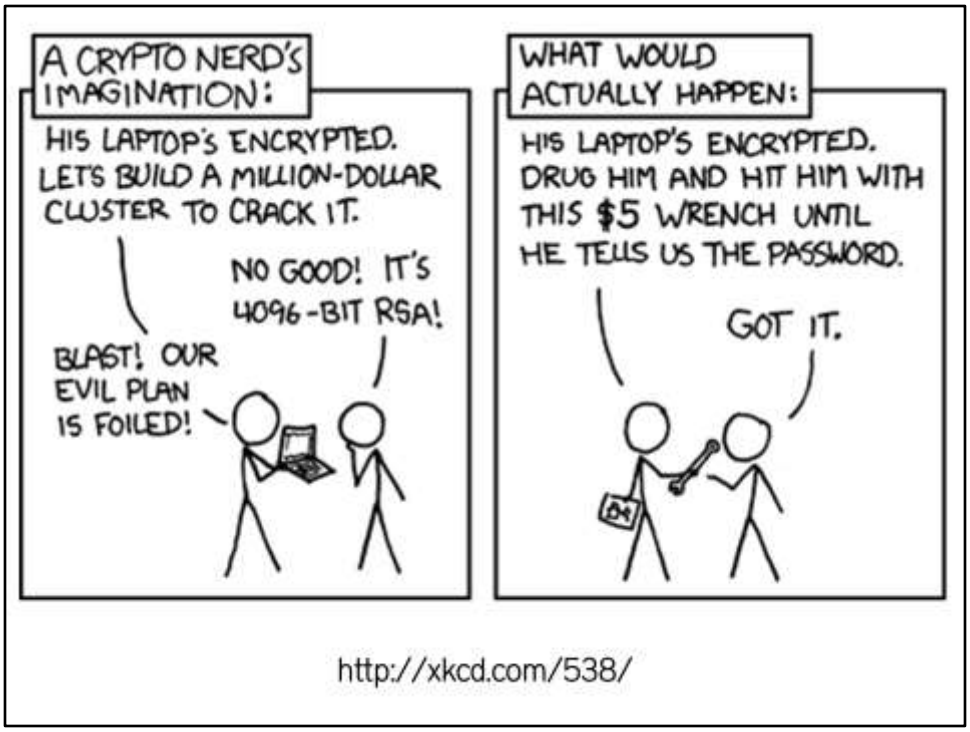
…und installiert sie auf Knopfdruck.

Virenschutz
Softwareupdates
Datensicherheit

- Windows-Kennwort hilft nicht bei Diebstahl der Hardware → Zugriff auf Hardware



- Nur Verschlüsselung der Daten hilft



http://xkcd.com/538/

Festplatten halten ca. 5, DVDs ca. 10 Jahre

- Datenverlust vorbeugen durch Backup, z.B. mit SyncToy

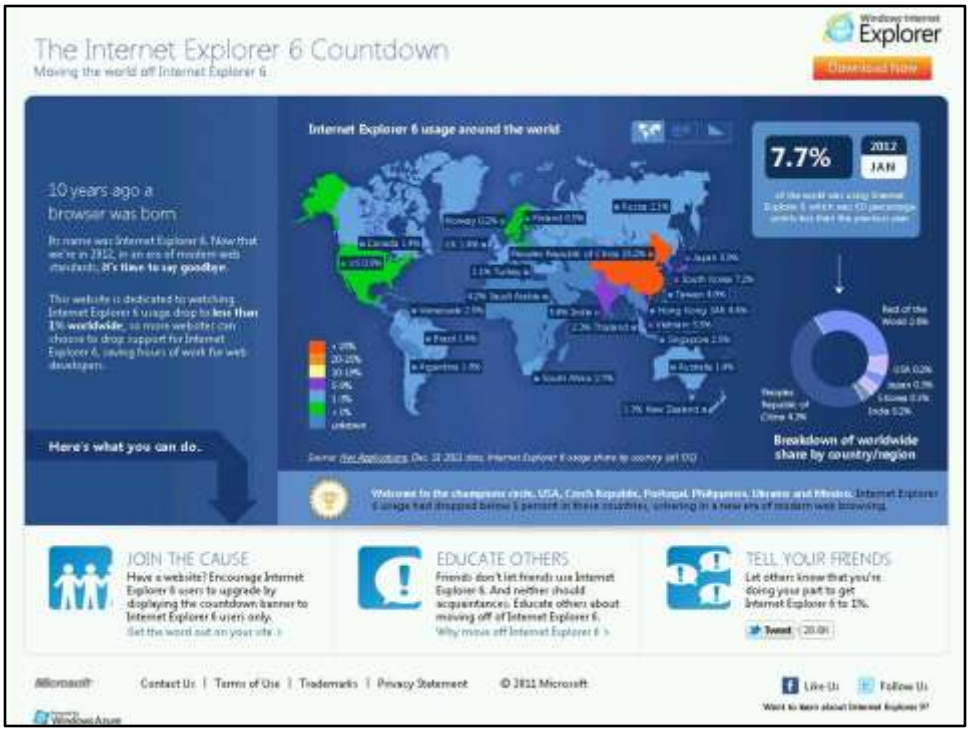
- Vorsicht beim Verkauf alter Datenspeicher
- Einmal mit Nullen überschreiben reicht allerdings aus, um keine Daten wiederherstellen zu können

Kommen wir nun zur Ebene des Webbrowsers.

Kommen wir nun zur Ebene des Webbrowsers.

Teilnehmer fragen: Wer benutzt welchen Browser?

- Browser sind alle recht sicher
- Firefox hat viele AddOns
- Chrome hat Sandbox



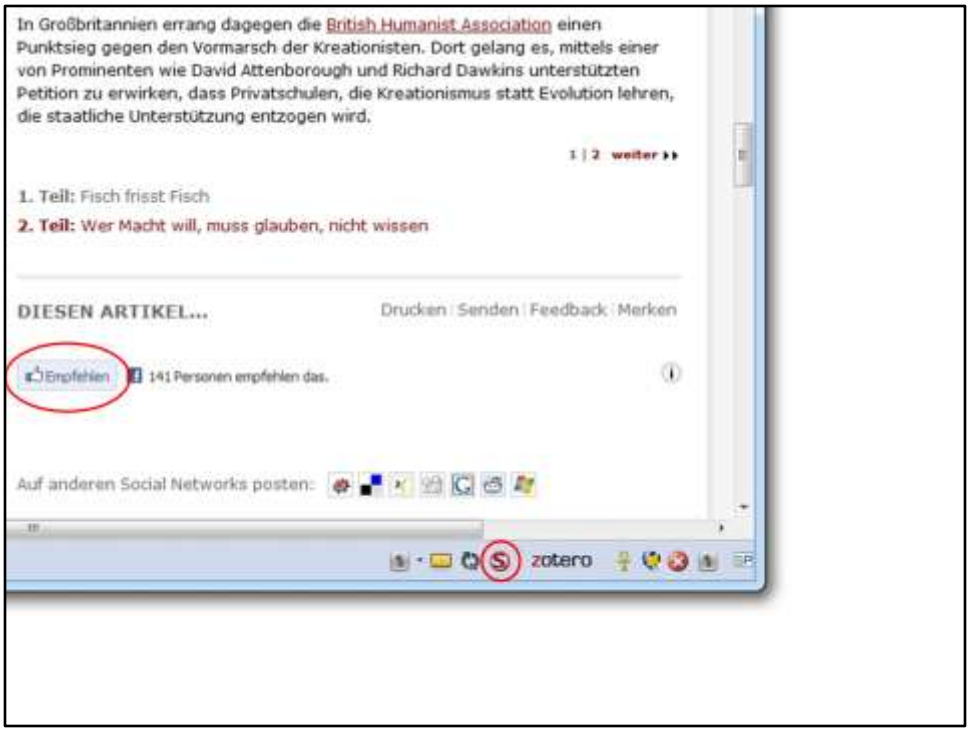
Wichtig ist ein aktueller (!) Browser

Browser warnen vor bekannten bösartigen Websites → man darf es nur nicht ignorieren.

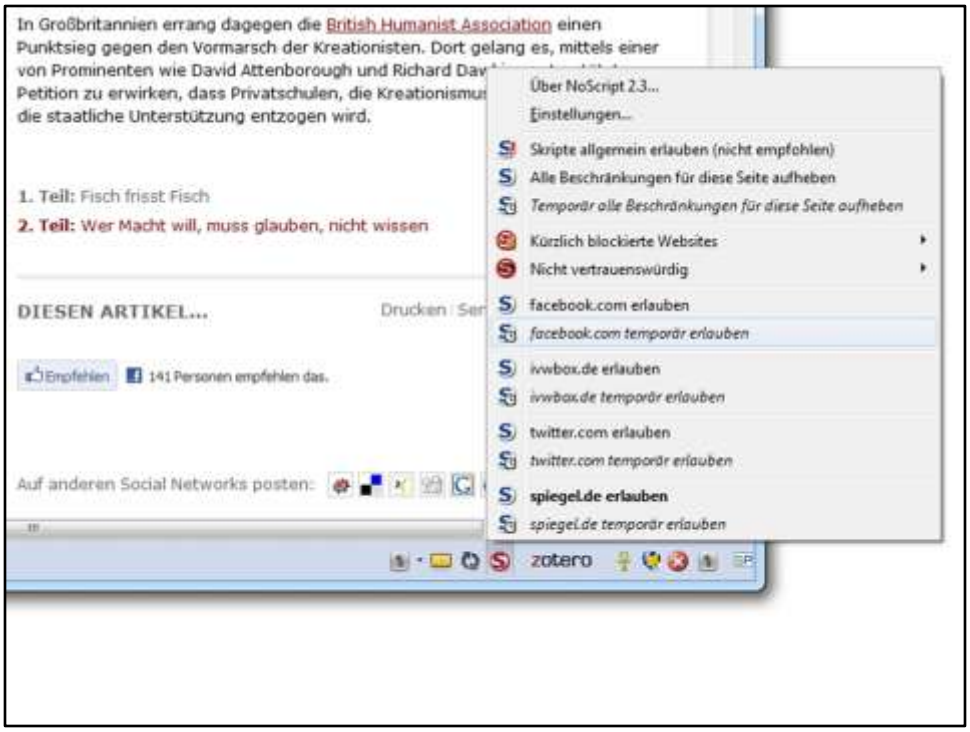
- Browser-Updates immer sofort einspielen
- Auch wenn AddOns vielleicht nicht mehr laufen

Wer ganz sicher gehen will, installiert sich ein separates Windows in einer VM. Sollte die zerschossen werden, kann sie einfach zurückgesetzt werden.


Registrieren Sie sich neu oder melden Sie sich an
ADD-ONS
ERWEITERUNGEN | PERSONAS | THEMES | SAMMLUNGEN | MEHR...
» Erweiterungen » NoScript
NoScript 2.3
von Giorgio Maone
Zusätzlicher Schutz für Ihren Browser!
+ Zu Firefox hinzufügen
Datenschutzerklärung
EMPFOHLEN



- NoScript deaktiviert alle Scripts, z.B. die Facebook-Buttons



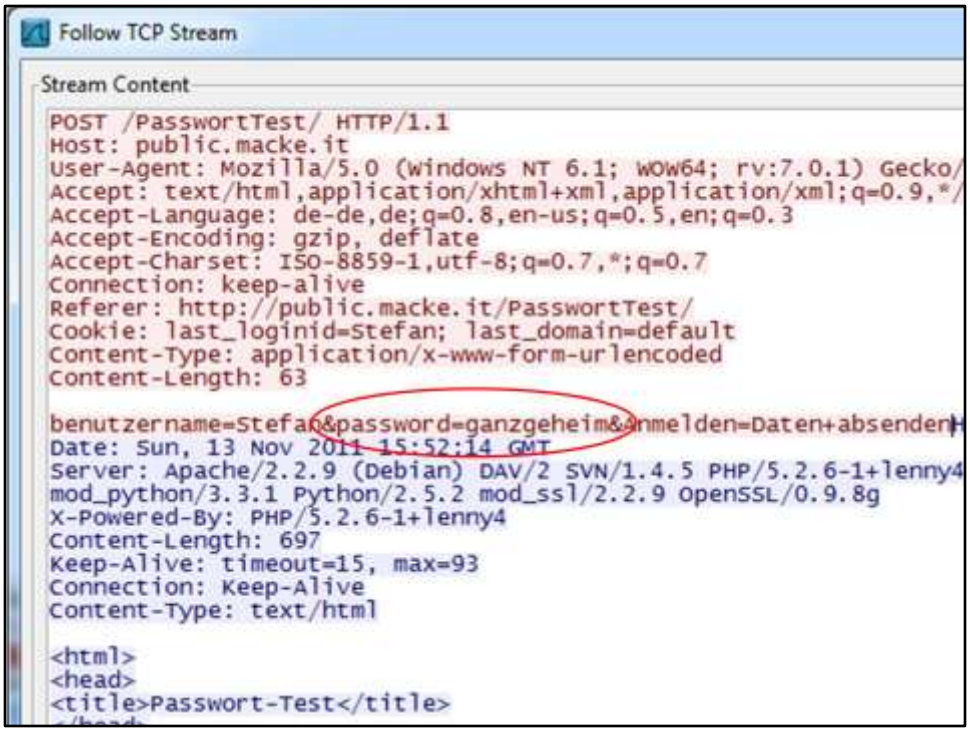
- Man kann dann gezielt die Scripts aktivieren, die man wirklich benötigt

Webbrowser

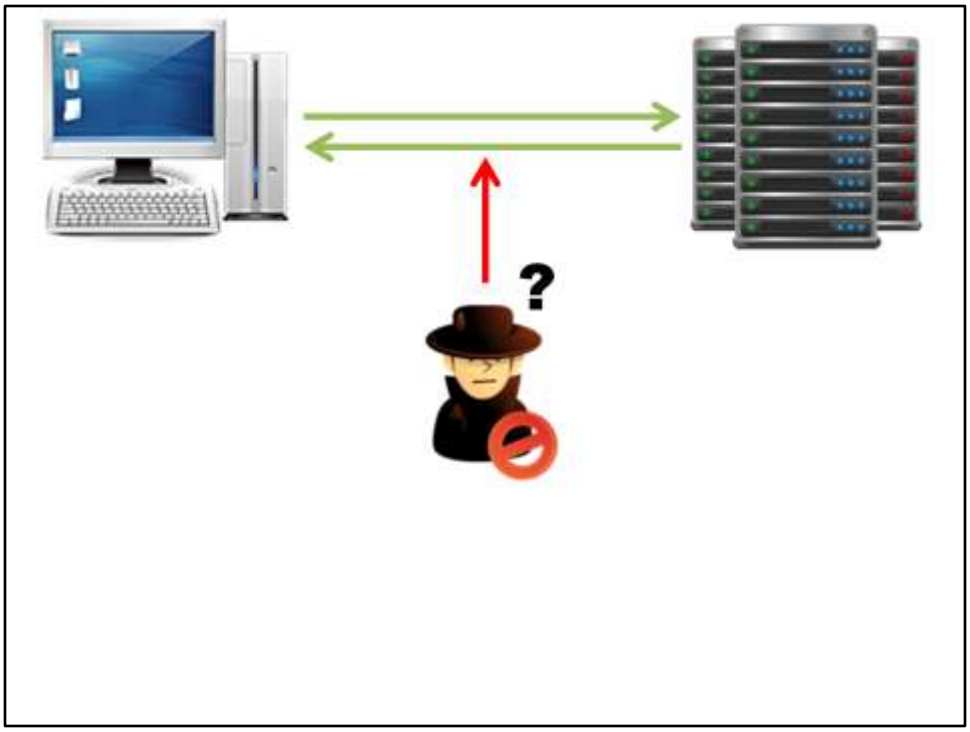
HTTPS

Sichere E-Mails

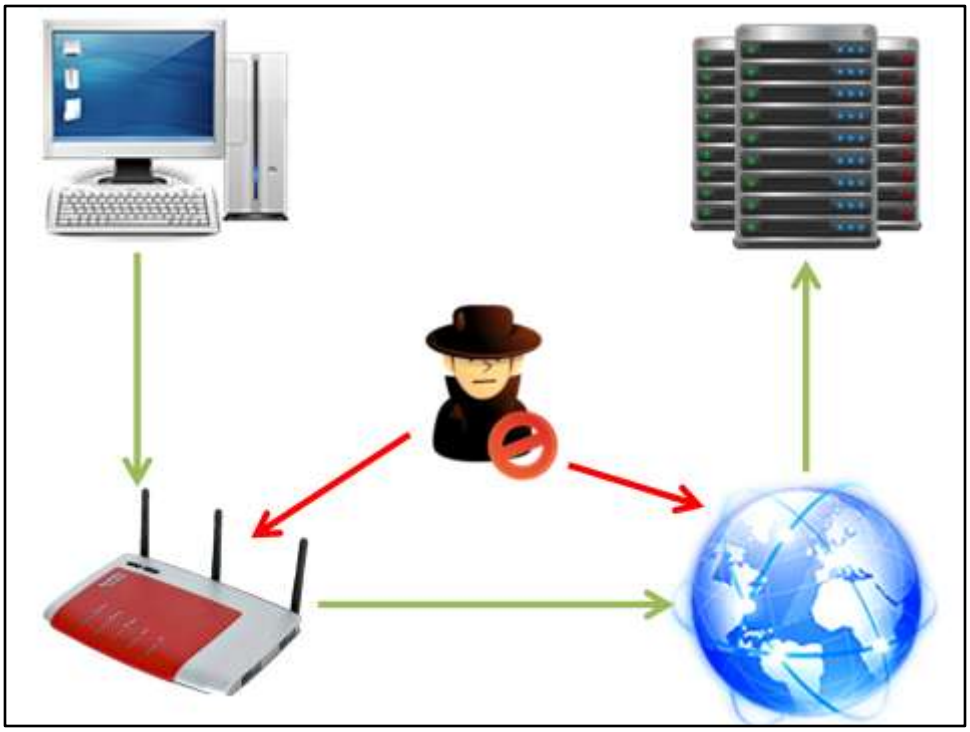
Dateidownloads



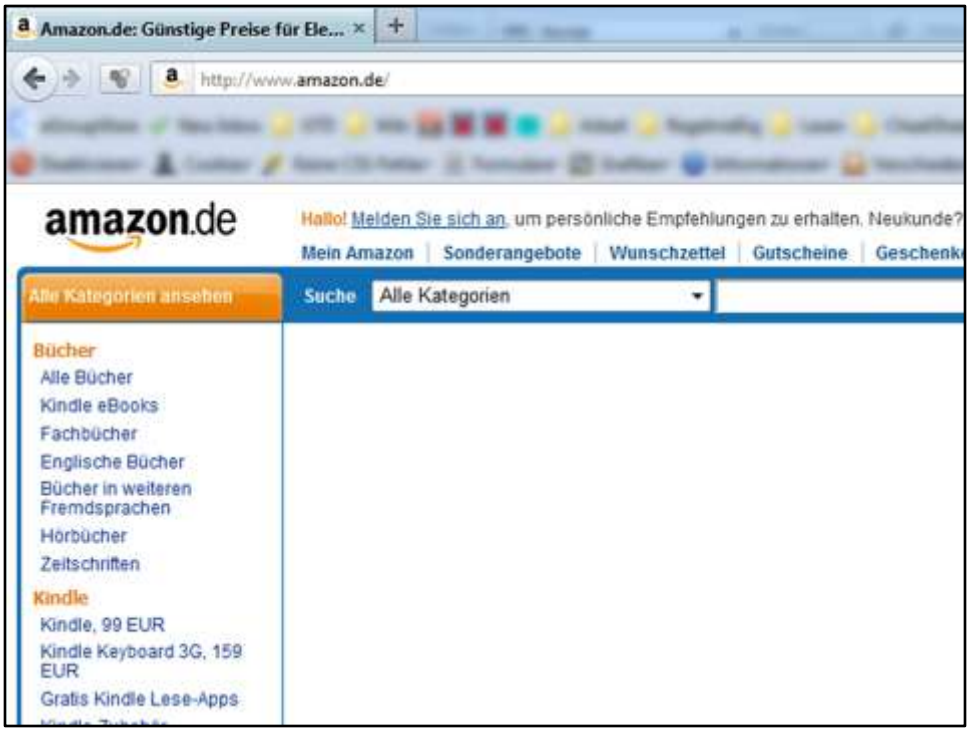
Daten werden bei HTTP unverschlüsselt übertragen



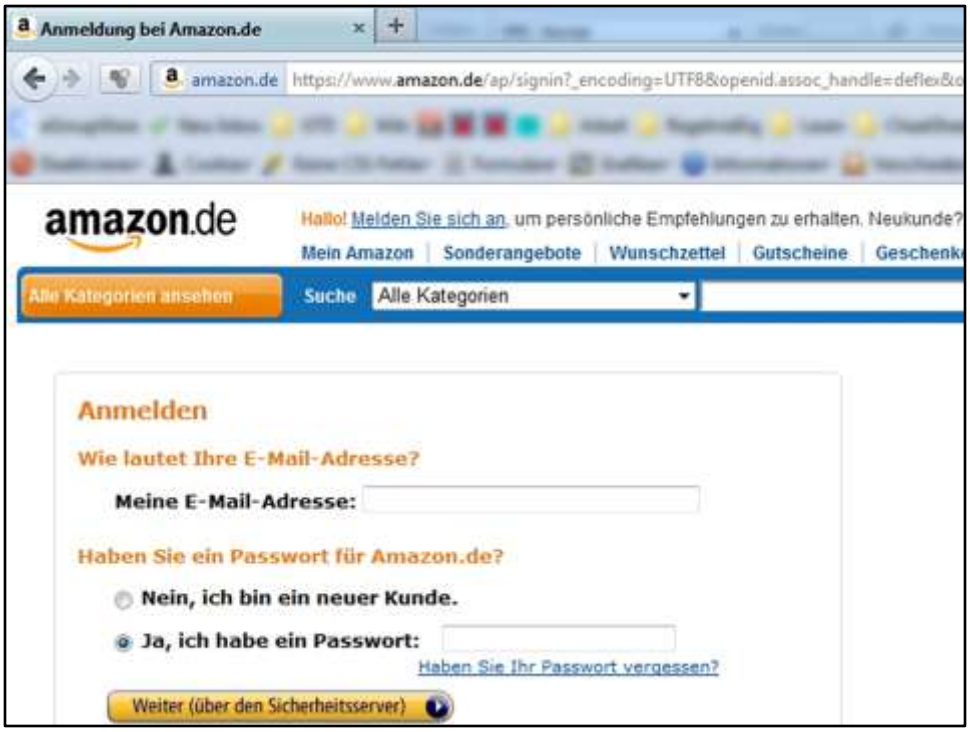
Das wäre kein Problem, wenn Client und Server direkt miteinander kommunizieren würden.



Doch das ist nicht so. Vielmehr gibt es eine Reihe an Zwischenstationen, die die Datenpakete passieren müssen.
An all diesen Zwischenstationen kann ein Angreifer die Daten problemlos auslesen.
Die Daten müssen also zwischen Client und Server verschlüsselt werden.

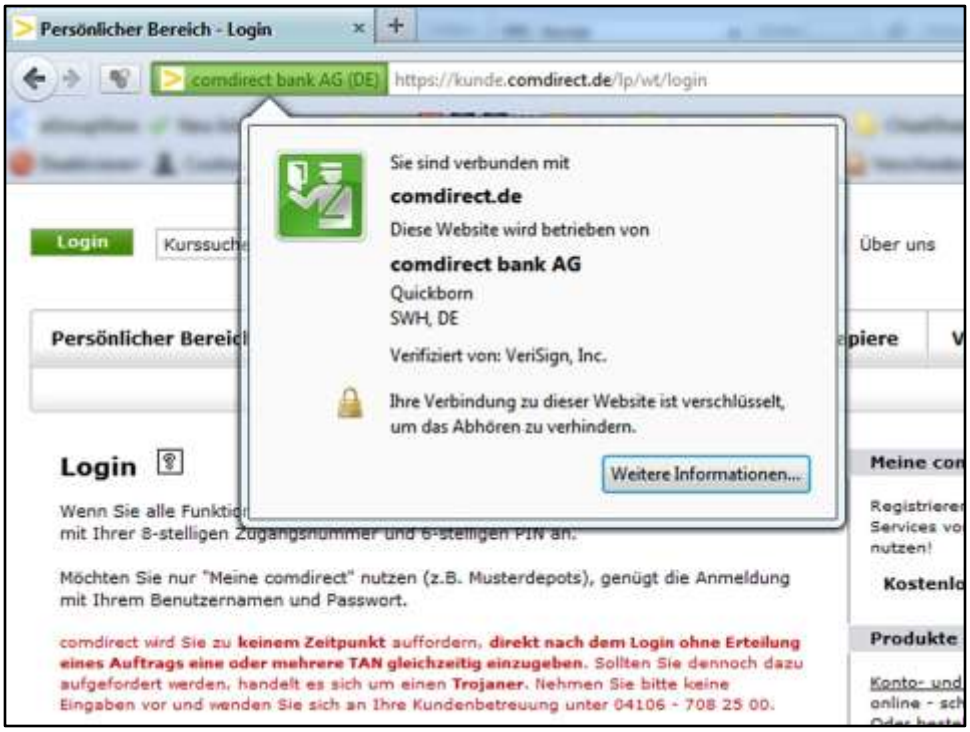


Wie erkennt man nun, dass man verschlüsselt unterwegs ist? → Adresszeile des Browsers



Alle modernen Browser färben die Adresszeile ein, wenn die Verbindung verschlüsselt ist.

Mit einem Klick auf die Adresszeile bekommt man dann Informationen zum Zertifikat angezeigt.

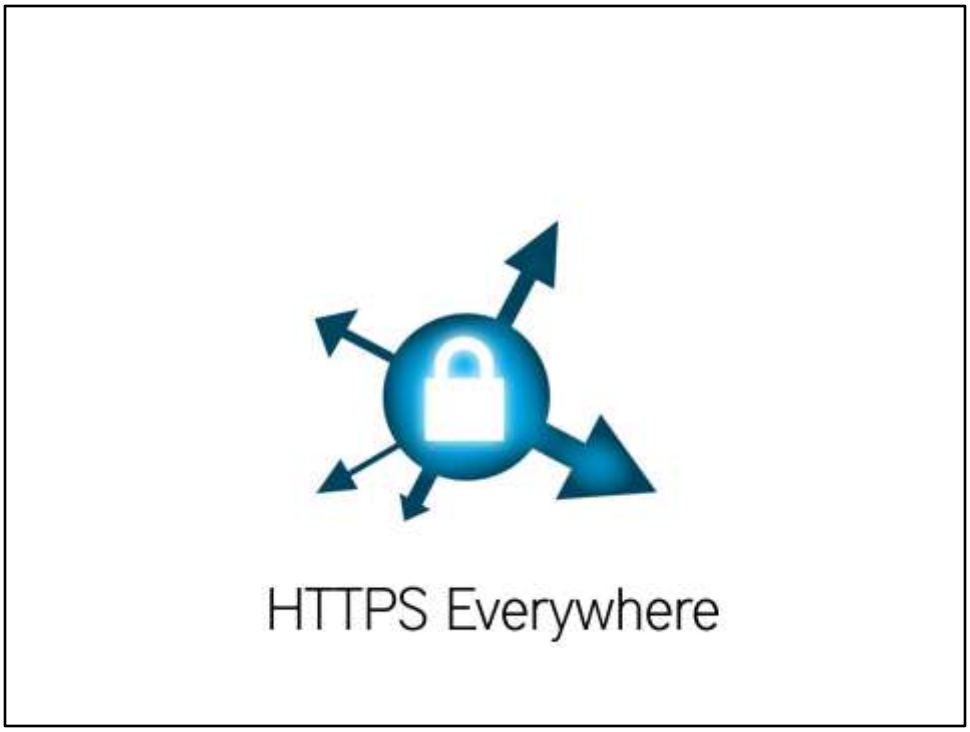


Grün bedeutet, dass der Inhaber der Website intensiv geprüft wird (z.B. mit Telefonanruf und Prüfung der Adresse).

Unser Dienstleister, die ivv, entschlüsselt alle Verbindungen, um sie mitlesen zu können. Daher ändert sich auch die Farbe von grün in blau.

Zertifikatsfehler ab jetzt nicht mehr wegklicken, sondern genau lesen, was die Ursache ist!

- Abgelaufen?
- Unbekannter Aussteller?
- Falsche URL?



Leitet den Benutzer automatisch auf HTTPS um, wenn verfügbar.


Firefox
Webbrowser
HTTPS
Sichere **E-Mails**
Dateidownloads


MYTH: COMPUTERS SUCK BECAUSE THEY DON'T DO WHAT YOU SAY.
NO! I DON'T DOWNLOAD THAT FILE! IT'S A VIRUS! NO! NOOO!

http://www.smbc-comics.com/index.php?db=comics&id=1801

Von: DHL <info@packstation.de>
An:
Cc:
Betreff: Ihre neue Goldcard

Falls der Newsletter nicht richtig dargestellt wird, klicken Sie bitte hier.

DHL

Ihre neue Goldcard

07.07.2011

PACKSTATION

Sehr geehrter PACKSTATION Kunde,

vielen Dank für Ihre kürzliche Anmeldung zum PACKSTATION Service von DHL. Wie Sie vielleicht schon aus dem Newsletter erfahren haben, wurden sämtliche PACKSTATIONEN deutschlandweit aktualisiert. Nun ist eine Goldcard unabdingbar geworden.

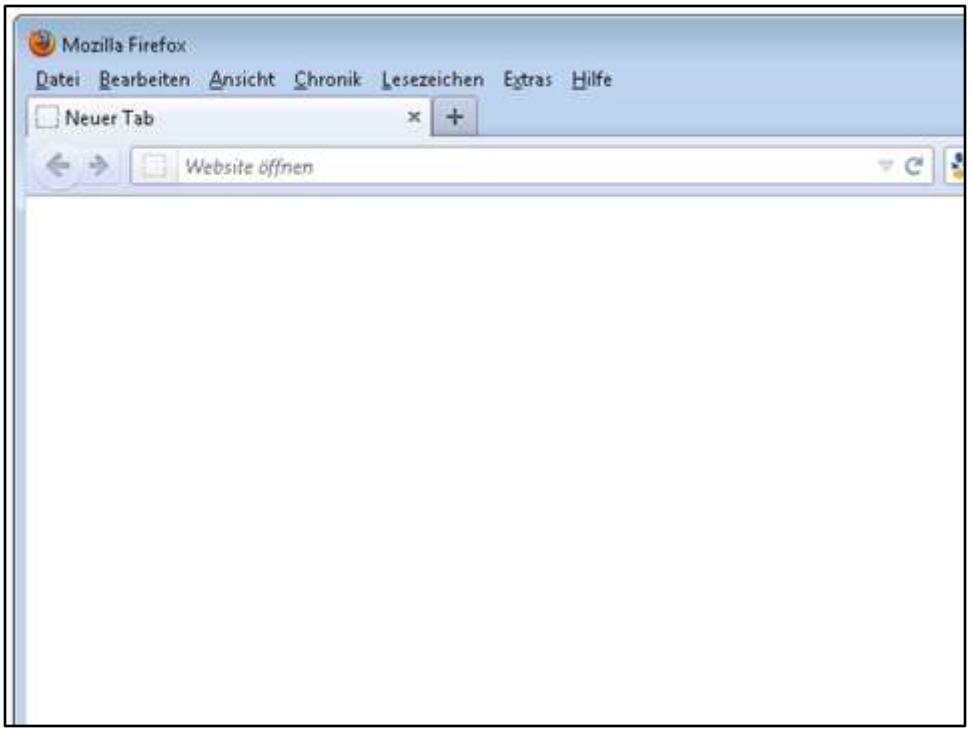
Fordern Sie jetzt Ihre neue Goldcard an, und profitieren Sie von vielen Neuerungen, wie z.B dem eingebauten RFI-Chip, mit dem sich verlorene oder gestohlene Kundenkarten orten lassen. So können Sie problemlos den PACKSTATION Service nutzen und sich gleichzeitig einige Überraschungen sichern - und das alles völlig kostenlos und unverbindlich.

Jetzt kostenfrei anfordern!

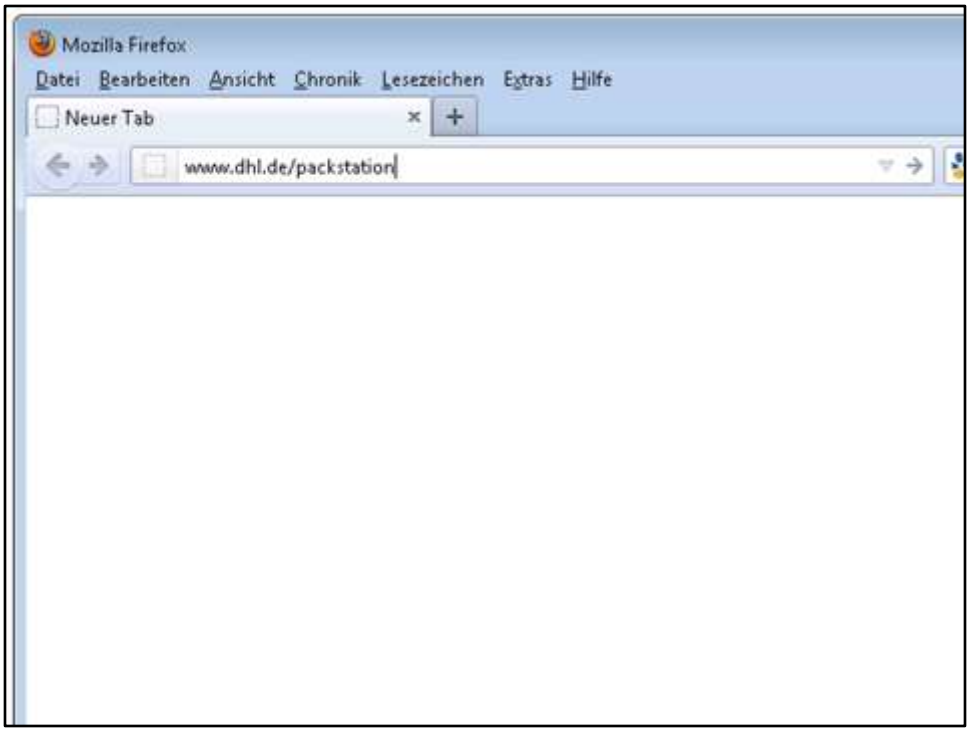
Und so einfach geht's:

- Vermerken Sie die PostNummer, Online-Passwort sowie **Ihre PIN: Die**

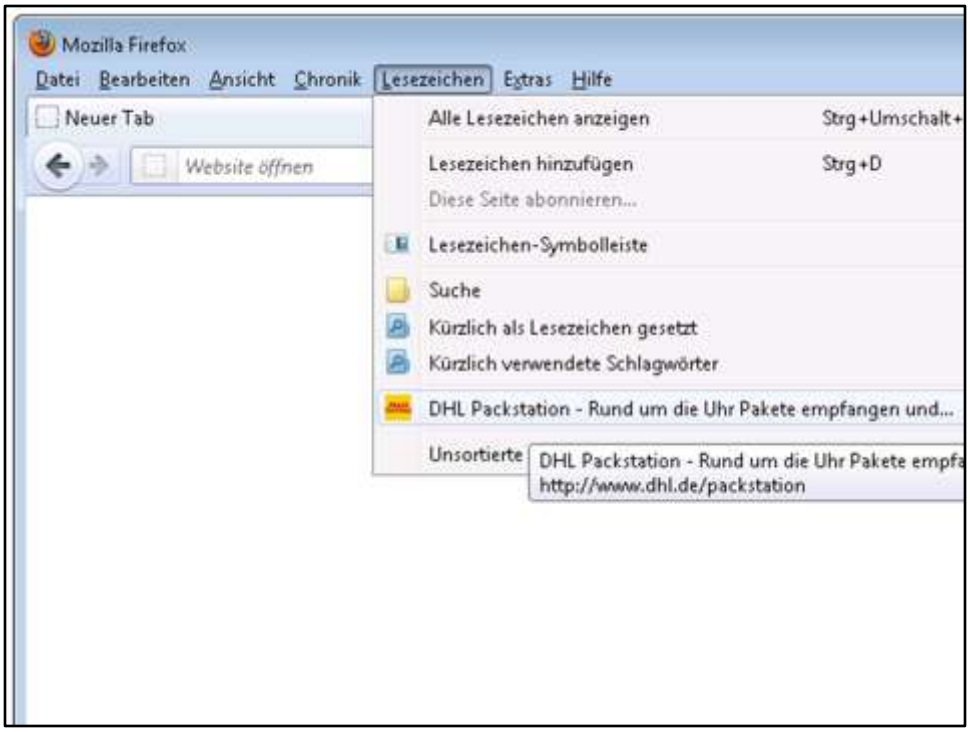
Teilnehmer raten lassen: Ist die Mail echt oder gefälscht?
nie Links aus Mails direkt öffnen…



…sondern sie selbst im Browser eingeben

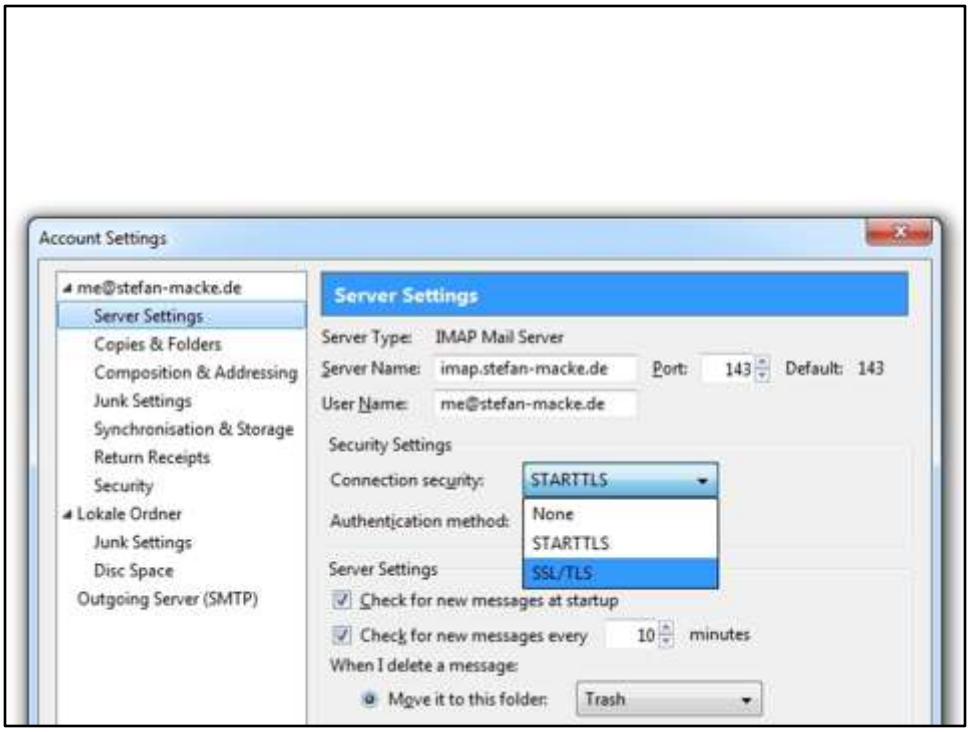


…sondern sie selbst im Browser eingeben

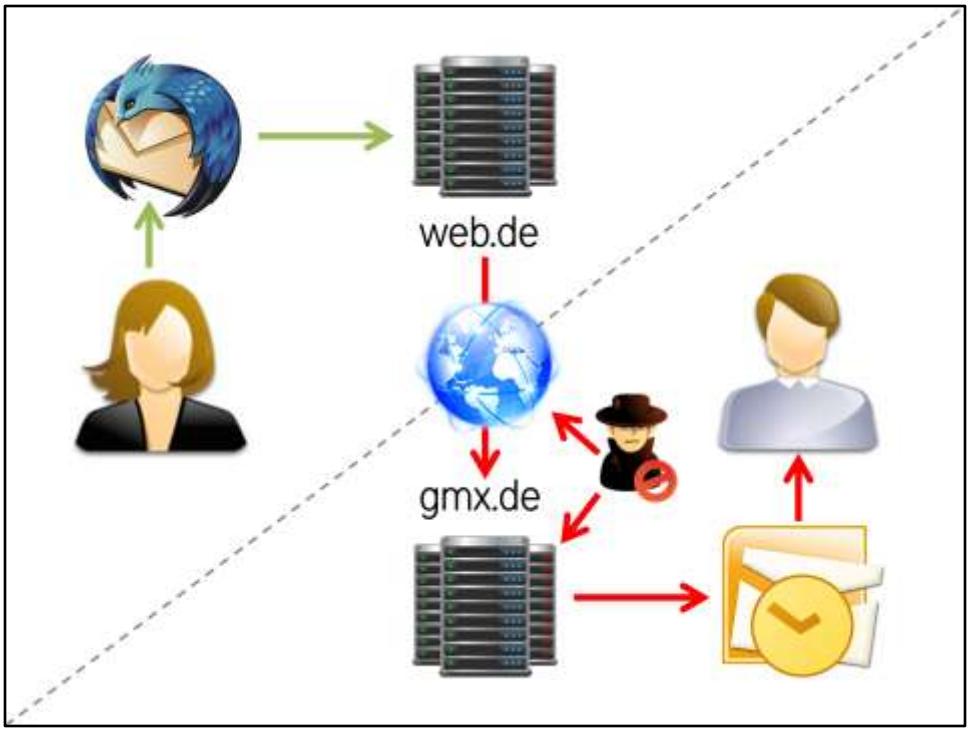


…sondern sie selbst im Browser eingeben

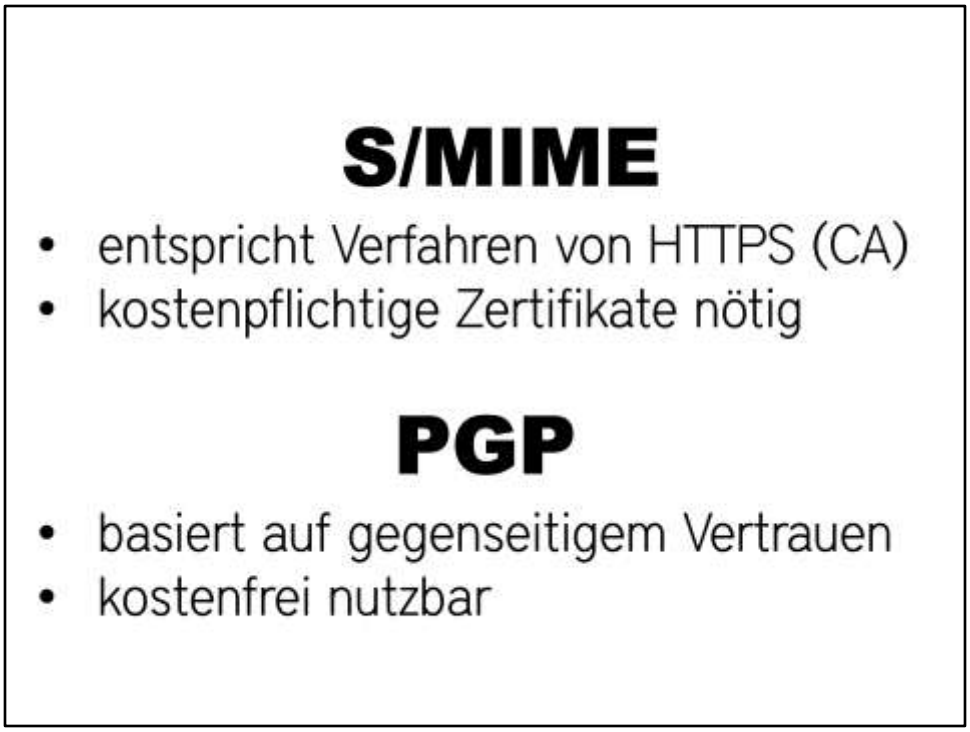
…sondern sie selbst im Browser eingeben



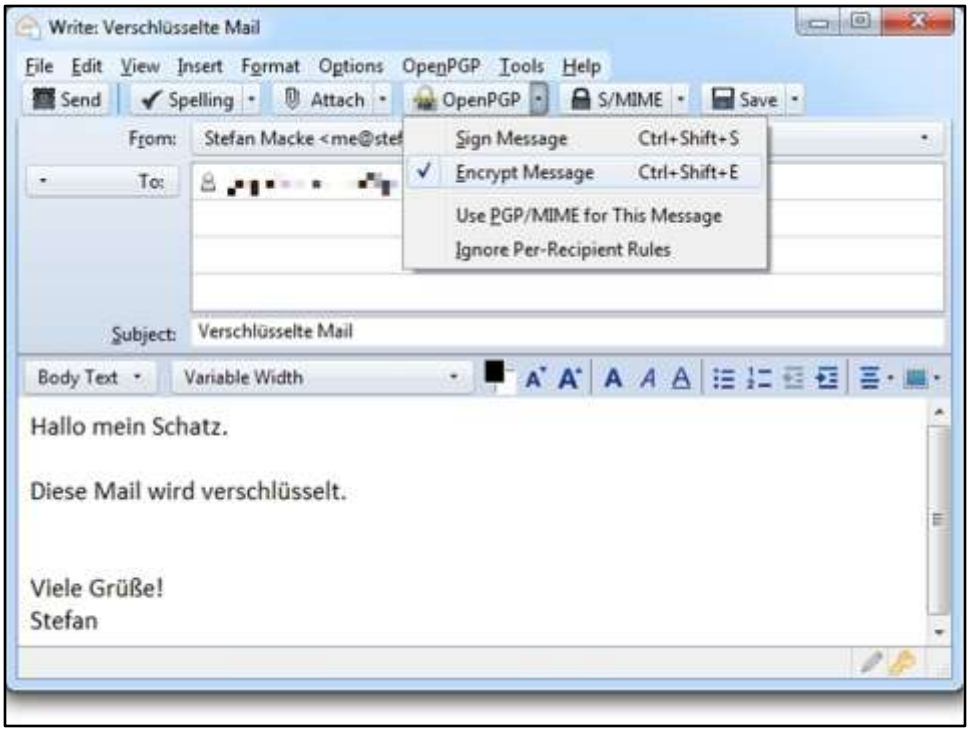
- Was für das WWW gilt, gilt genauso für E-Mails: alles wird unverschlüsselt übertragen.
- Nur verbindet man sich üblicherweise nur mit einem einzigen Server.



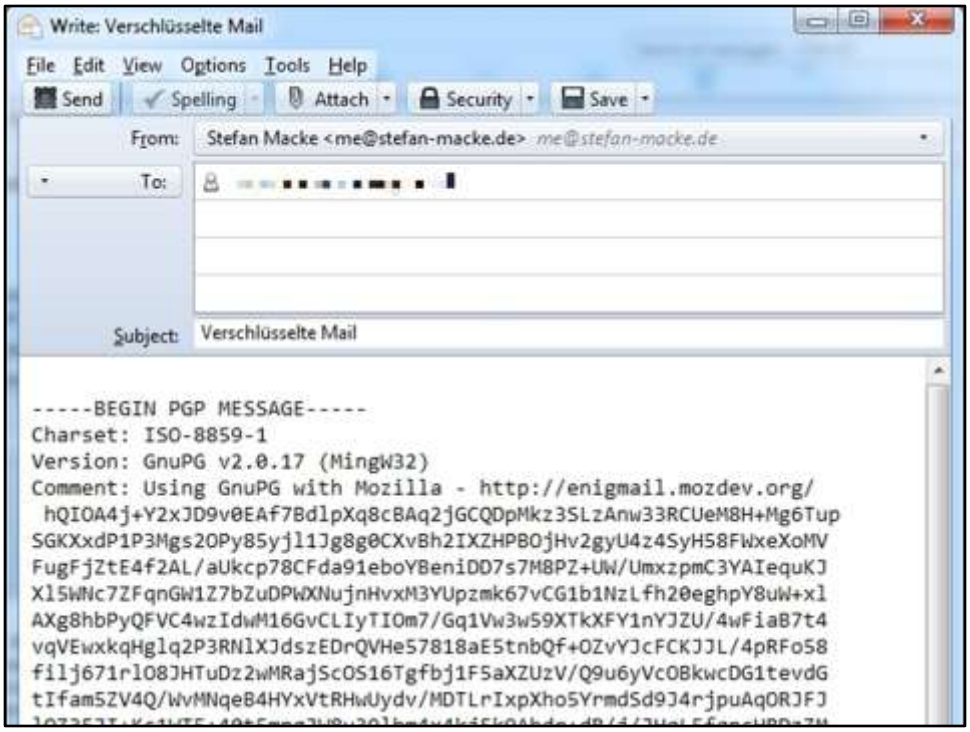
- SMTPS verschlüsselt nur die Daten zwischen Mailclient und eigenem Mailserver
- Nicht zwischen den Mailservern über das Internet



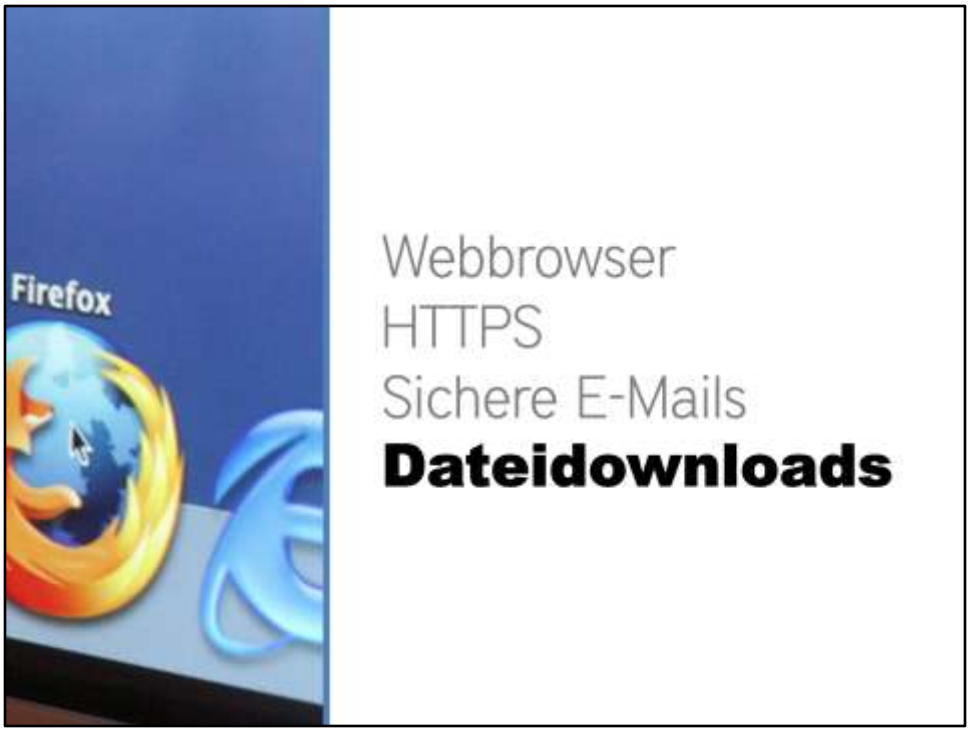
Um die Mailinhalte zu verschlüsseln kann PGP oder S/MIME verwendet werden.



Beispiel: Enigmail



Beispiel: Enigmail

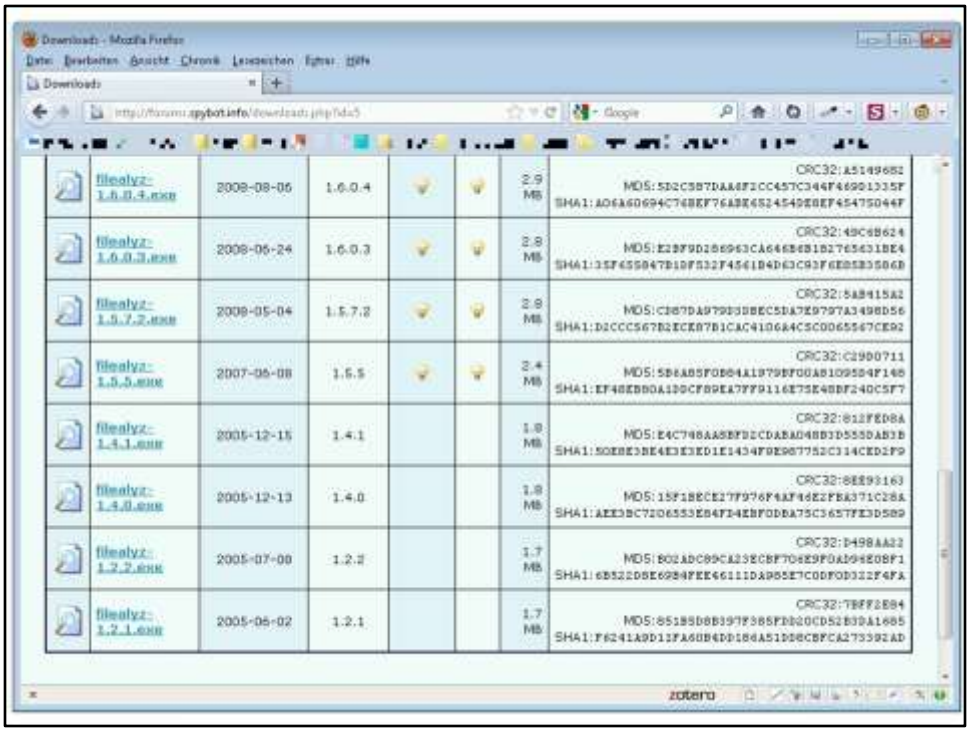

Firefox
Webbrowser
HTTPS
Sichere E-Mails
Dateidownloads

Woher weiß man, dass heruntergeladene Dateien nicht manipuliert wurden?

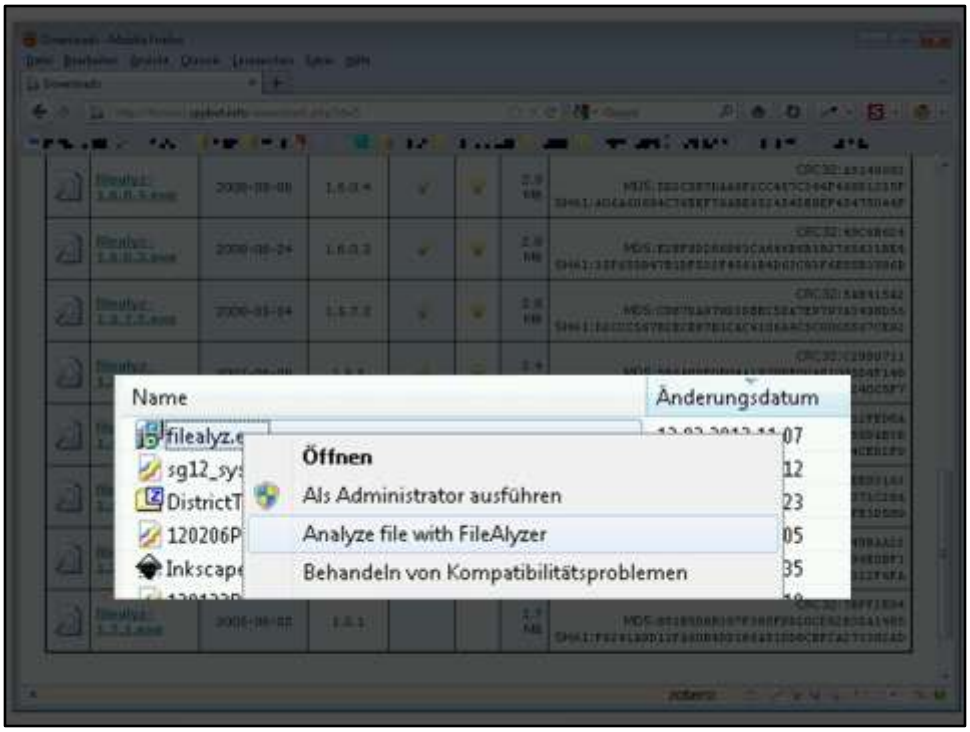
- Trojaner drin?
- Hintertürchen bei Verschlüsselung?

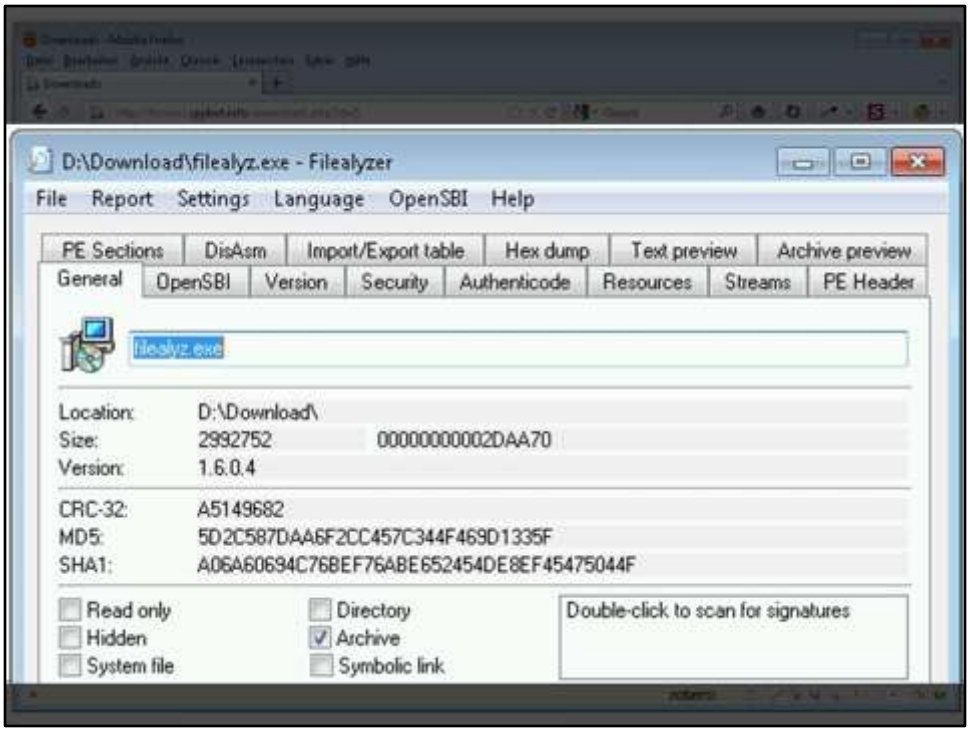

Download
Gpg4win 2.1.0
Gpg4win 2.1.0 enthält:
SHA1-Prüfsumme (für gpg4win-2.1.0.exe):
f619313cb42241d6837d20d24a814b81a1fe7f6d gpg4win-2.1.0.exe

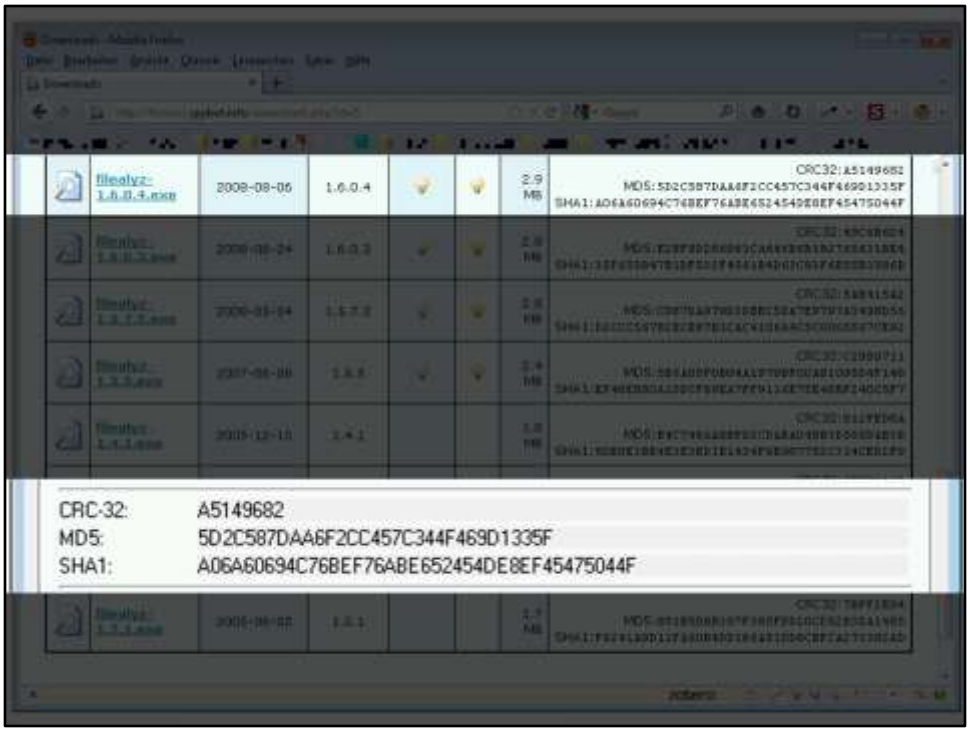

Hash-Funktion
Einbahnstraße
e462ab94e3dc2309712baac834472eddfff9923
fixe Länge



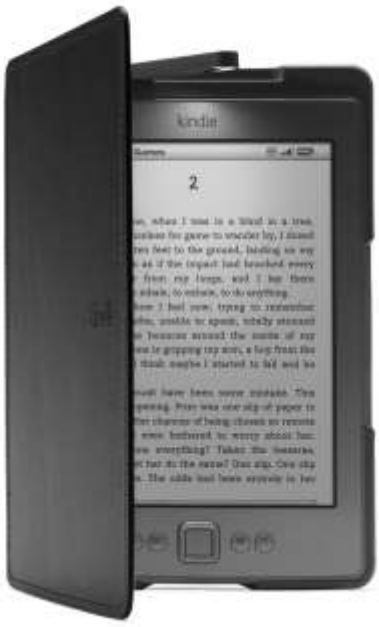
Ein Tool zum überprüfen der Hashes von Downloads ist FileAlyzer.


Name
Änderungsdatum
Öffnen
Als Administrator ausführen
Analyze file with FileAlyzer
Behandeln von Kompatibilitätsproblemen


D:\Download\filealyz.exe - Filealyzer
File Report Settings Language OpenSBI Help
PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview
General OpenSBI Version Security Authenticode Resources Streams PE Header
filealyz.exe
Location: D:\Download\
Size: 2992752 00000000002DAA70
Version: 1.6.0.4
CRC-32: A5149682
MD5: 5D2C587DAA6F2CC457C344F469D1335F
SHA1: A06A60694C76BEF76ABE652454DE8EF45475044F
Read only
Hidden
System file
Directory
Archive
Symbolic link
Double-click to scan for signatures


filealyz-
1.6.0.4.exe
2008-08-06
1.6.0.4
2.9 MB
CRC-32: A5149682
MD5: 5D2C587DAA6F2CC457C344F469D1335F
SHA1: A06A60694C76BEF76ABE652454DE8EF45475044F
CRC-32: A5149682
MD5: 5D2C587DAA6F2CC457C344F469D1335F
SHA1: A06A60694C76BEF76ABE652454DE8EF45475044F

Zeiten
ändern sich...



Ich möchte zum Abschluss noch einmal die kleine Geschichte vom Anfang erzählen, aber an die heutige Zeit angepasst.

Stefan ist nun kein ahnungsloser Internet- und PC-Benutzer mehr, denn er hat einiges über Sicherheit gelernt.

Anstatt die Links in seinen Mails direkt anzuklicken, lädt er die Seite manuell im Browser und schaut nach dem Rechten.

Angreifer auf sein WLAN können ihm nichts mehr anhaben…

…denn er hat seinen Router mit WPA2 und einem sicheren Kennwort abgesichert.

Und selbst wenn er sich auf zwielichtigen Seiten rumtreibt, warnt ihn sein Virenscanner rechtzeitig vor Schadsoftware.

Stefan hat alle Daten auf externen Medien und seinen tragbaren Geräten mit TrueCrypt verschlüsselt, sodass Diebe nichts mit ihnen anfangen können.

Wenn Stefan im Internetcafé oder sonstigen öffentlichen Netzwerken unterwegs ist…

…achtet er darauf, nur verschlüsselte Verbindungen zu benutzen.

Daher muss er sich auch keine Sorgen um seinen Kontostand machen.

Egal ob Online-Bezahlvorgänge…

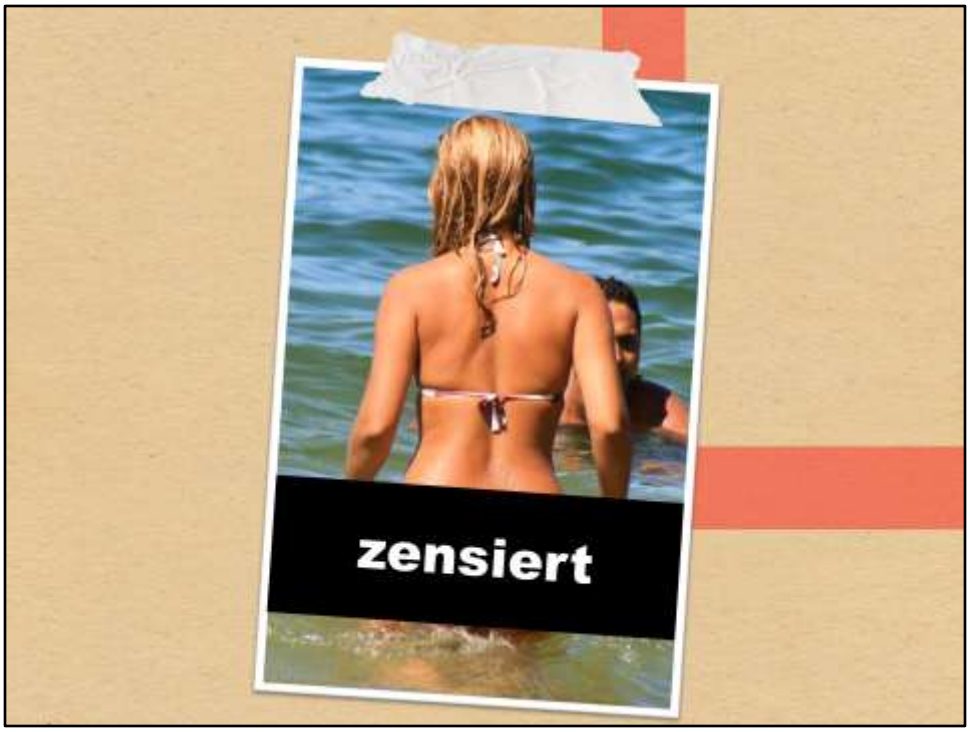
…oder der Webmail-Zugang, immer achtet Stefan auf die blaue/grüne Adresszeile.

Seinen Anwalt muss Stefan jetzt nur noch selten anrufen.

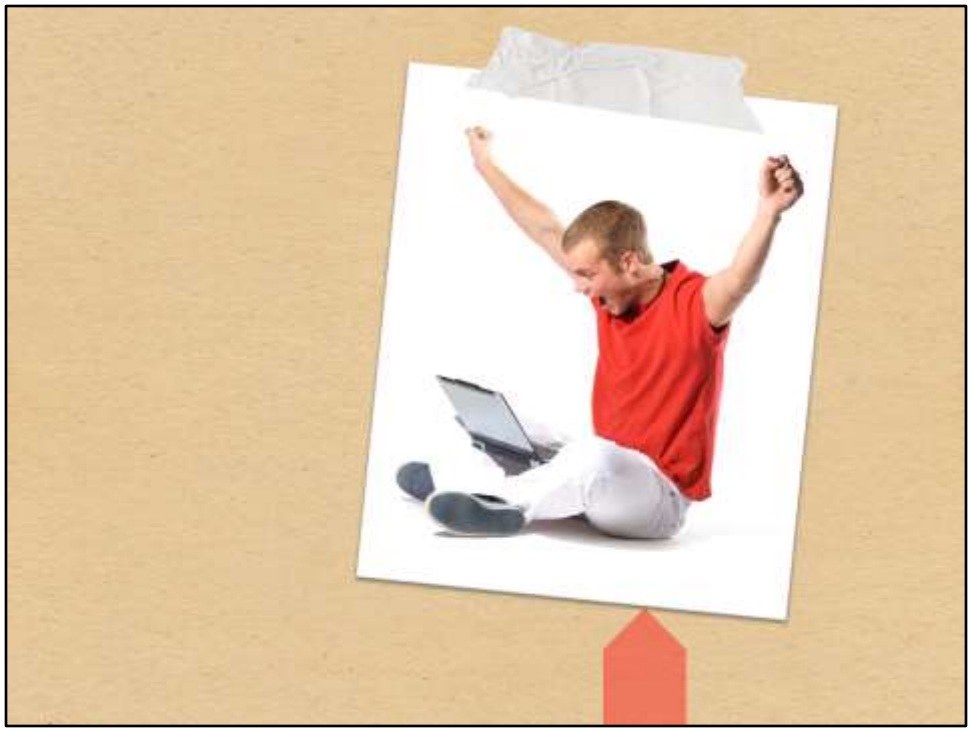
Anstatt seltsamer Rechnungen…

…bekommt Stefan jetzt nur noch Postkarten von Freunden, denen er Tipps zum Thema Sicherheit im Internet gegeben hat.

Und wenn die GMX-Meldung kommt, hat er sich tatsächlich vertippt.



Und Stefans Urlaubsfotos bleiben nun auch privat.



Stefan ist rundum zufrieden und lebt fröhlich und sicher bis an sein Lebensende.


Fazit

Die Tipps sind zwar einfach, aber bedeuten auch Einschränkungen: Hier ein Klick, dort ein Schritt mehr…

Sicherheit ist ein ganzheitliches Konzept. Einzelne Maßnahmen reichen nicht aus.

Mit den paar einfachen Tipps kann sich nun jeder sicher im Internet bewegen! ;-)


END

David Ritter
www.sxc.hu/photo/603585

Andrzej Pobiedzinski
www.sxc.hu/photo/1318896

Glen Jeffreys
www.sxc.hu/photo/228778

Thad Zajdowicz
www.sxc.hu/photo/623446

Ante Vekic
www.sxc.hu/photo/1237883

Alex Fiore
www.sxc.hu/photo/197626

s_falkow

www.flickr.com/photos/safari_vacation/6257284524

Sarah Gilbert

www.flickr.com/photos/cafemama/718939603/

c.alberto

www.flickr.com/photos/cacobeto/3212630910/

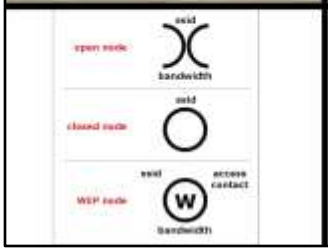
Simon Cataudo
www.sxc.hu/photo/116120

Philippe Ramakers
www.sxc.hu/photo/250528

Shawn McCullough
www.flickr.com/photos/shawnmichael/4302375313/

Gary Scott
www.sxc.hu/photo/746494

Maha
www.flickr.com/photos/maha-online/62811764/



Isaac Mao
http://www.flickr.com/photos/isaacmao/191604830/

Sebastiaan ter Burg

www.flickr.com/photos/ter-burg/5520210028/

Alchemist

de.wikipedia.org/wiki/Datei:Hard_disk_head_crash.jpg

Antonio Jimenez Alonso

www.sxc.hu/photo/779951

Metro Centric
www.flickr.com/photos/16782093@N03/3642988815/

Guglielmo Losio
www.sxc.hu/photo/1356926

Johanna Friedman
www.sxc.hu/photo/403571/


Sicherheit
im Internet und auf dem Heim-PC