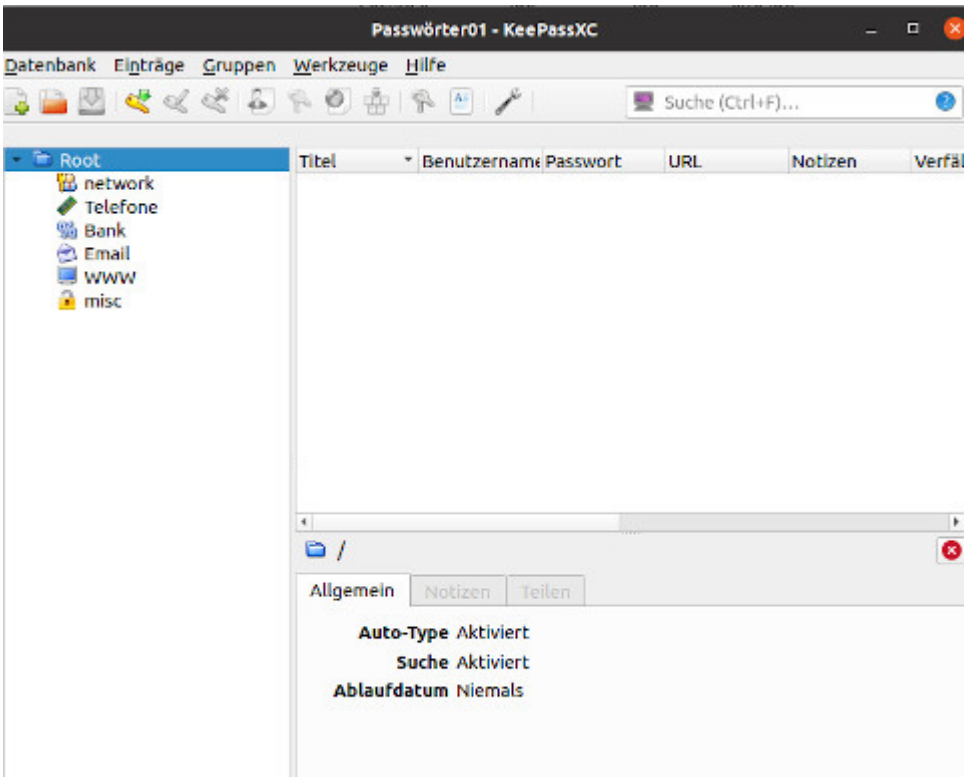
Passwörter, voller Hass



Passwort-Manager Keepass für alle Betriebssysteme

Bei Heise und auch anderswo las ich über das neue Gesetz, das sich gegen bestimmte Gefühle und Gefühlsäußerungen richtet, aber mit Technischem verknpüft ist: *Das Paket besteht aus dem „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“, das am Samstag in weiten Teilen in Kraft tritt, sowie dem ab Freitag geltenden „Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020„.*

Sie versuchen es immer wieder. Man muss wissen, dass ursprünglich geplant war, die Sache ohne richterlichen Beschluss durchziehen zu lassen. Allein schon die Chuzpe, dass das Justizministerium das versucht hat, spricht schon Bände. Interessant ist auch diese Passage: *Anbieter von Telemediendiensten wie WhatsApp, Google, Facebook, Tinder & Co. müssen sensible Daten von Verdächtigen wie IP-Adressen und Passwörter künftig an Sicherheitsbehörden herausgeben.*

Das wird natürlich lustig, wenn sich etwa Facebook weigerte. Und will das Gesetz auch auf Wechat, Weibo und Toutiao zugreifen? Die werden sich totlachen. Und was ist mit VKontakte, Odnoklassniki und Habr?

Golem schreibt: „Der nun vereinbarte Kompromiss zwischen Bundestag und Bundesländern ist 34 Seiten lang. Demnach ist die Herausgabe von Passwörtern, die in der Regel gehasht vorliegen, weiterhin an den Straftatenkatalog der Onlinedurchsuchung geknüpft."

Onlinedurchsuchung. Wenn ich allein das Wort höre, schwillt mir schon der Kamm. (Zwischenfrage: wie macht man die?) Es geht aber nicht nur um Passwörter: „Weiter kritisiert der Verband der Internetwirtschaft scharf, dass Anbieter von Telekommunikations- und Telemediendiensten gleichermaßen dazu verpflichtet werden sollen, sämtliche unternehmensinterne Daten zur Verfügung stellen, um Ermittlungs- und Strafverfolgungsbehörden Informationen zu Passwörtern und anderen Zugangsdaten zu liefern."

Ich bin mal gespannt, wie das technisch umgesetzt werden soll und was passiert, wenn ein Betroffener dagegen klagte. Ich vermute ganz stark, das Gesetz würde dann auch vom Bundesverfassungsgericht in die Tonne getreten.

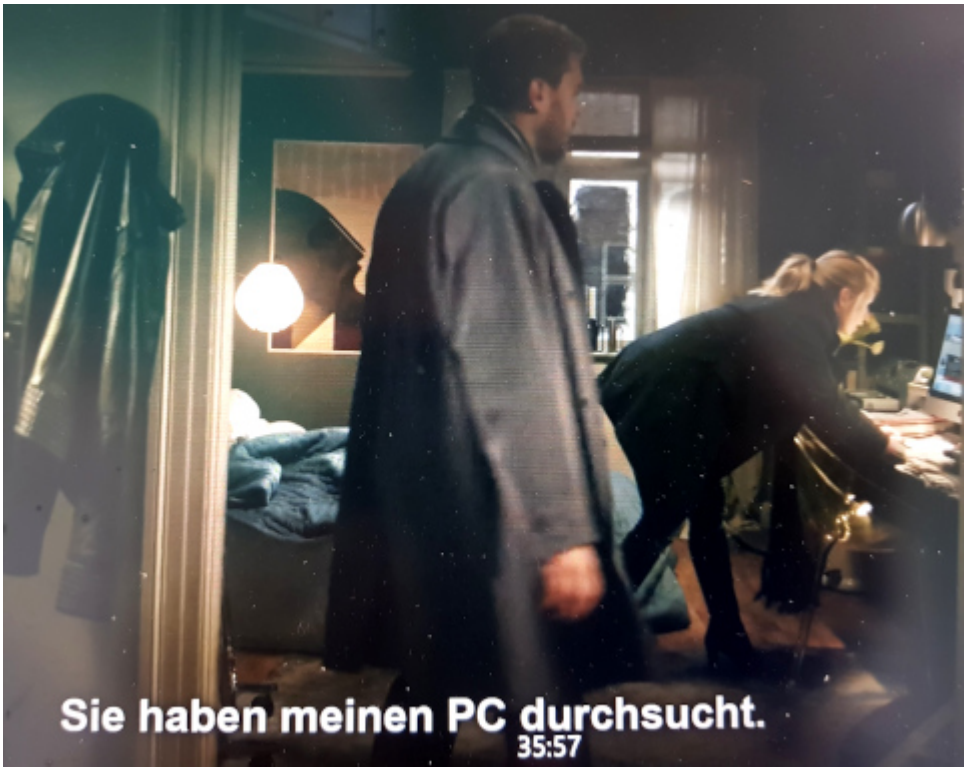
TKÜ, ick hör dir nicht trapsen

Gerade ~~schrob~~ schrieb ich in einer Arbeitspause in den ~~a~~sozialen Medien: Wer „Ungleichheit" bekämpfen, aber den Kapitalismus erhalten will, leidet an politischer Schizophrenie und hat schwer einen an der Waffel. #Grüne

Jetzt lese ich bei Fefe ein Zitat aus dem Wahlprogramm der neuen Bourgeoisie-Freundglottisschlaginnen: „…wollen wir es der Polizei ermöglichen, technische Geräte anhand einer rechtsstaatlich ausgestalteten Quellen-TKÜ zielgerichtet zu infiltrieren.“

Die haben ja noch mehr einen an der Waffel, als ich dachte. Vielleicht sollten sich mal die Wählerglottisschlaginnen trauen, mit mir eine Videokonferenz zu machen, mit Zuschauern natürlich – aus dem hiesigen Publikum, und sich für den hanebüchenen Quatsch rechtfertigen, den die ständig verzapfen? Aber vermutlich wählt die hier niemand, die habe ich schon alle vergrault…

Sie sind schon drin



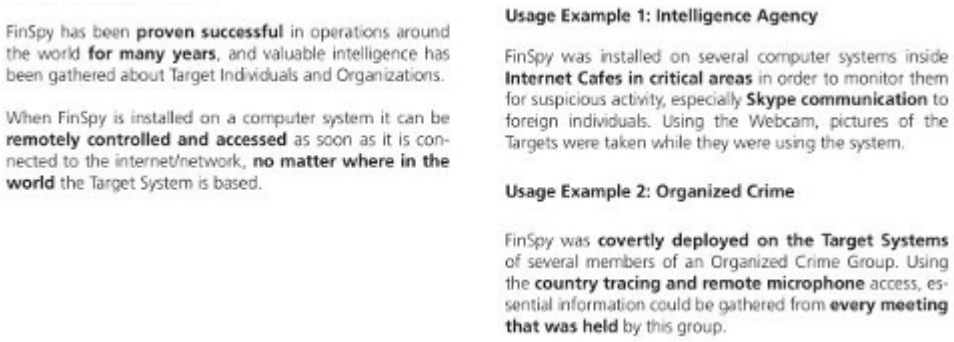
Screenshot aus Borgen, Staffel 1

Was soll man da machen? Vielleicht hätte eine ~~Cyber~~Online-

Durchsuchung geholfen? Dann hätte niemand etwas bemerkt….(Vorsicht! Ironie!)

Merke: Man muss den größten Stuss nur oft und lange genug wiederholen, bis ihn alle für wahr halten.

Cyberdurchsuchung, die 894ste



FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Manchmal habe ich bei den offenbar hingeschlampten Meldungen von Heise, insbesondere von Stefan Krempl, den Eindruck, hier werde haarscharf an einer Verschwörungstheorie vorbeigeschrieben.

Es ist eindeutig eine urbane Legende, wenn man suggeriert, irgendein Cyberpolizist säße irgendwo vor dem Monitor und „hackte“ sich irgendwo in einen privaten Rechner. So etwas zu können behauptet noch nicht einmal FinSpy.

Auch Wikipedia faselt sinnfrei herum: „handelt es sich um einen Trojaner, da die Spionagefunktionen in einer harmlos aussehenden Hülle eingeschmuggelt werden.“ (Die Diskussionsseite ist gesperrt – vermutlich nicht zufällig.)

„Harmlos aussehende Hülle“? Geht es ein bisschen konkreter? Nein, weil das Blödsinn ist! Man kann trojanische Pferde (so heißt das und nicht „Trojaner“) nur auf einem „fremden“ Rechner implementieren, wenn man entweder den physischen

Zugriff hat und der Rechner ungesichert ist oder wenn man per USB-Stick Software installieren kann, und das alles nur unter ganz bestimmten Bedingungen. Alles andere ist Voodoo und ein Hoax der allerfeinsten Sorte.

Wenn man sich die Passagen bei Wikipedia zur Quellen-Telekommunikationsüberwachung (was für ein Wort!) genauer anschaut, wird auch sofort klar, dass es sich weitgehend um heiße Luft handelt.

„Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen“, schreibt der CCC in seiner Analyse. „Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde.“ Quod erat demonstrandum. Nur wie ich oben schrieb.

In einem Internet-Cafe ginge das natürlich, falls ein Richter das anordnete. Übrigens habe ich Linux. Und man müsste schon an meinem Stangenschloss hinter der Wohnungstür vorbei und einbrechen, um an meine Rechner zu kommen. Per USB geht bei mir auch nichts, meine BIOSSE (heißt das so?) verbieten das. Keylogger funktionieren bei Ubuntu oder XFCE auch nicht oder ich würde es merken.

Aber noch mal für Krempl zum Mitschreiben: Gefährder sitzen ausschließlich und immer an demselben Platz in immer demselben Internetcafe und nutzen ausschließlich Windows.

Hide and Seek


Manchmal muss man sich über die Berichterstattung bei Heise doch wundern. Wenn jemand sachlich und richtig technische Themen im Internet dargestellt haben möchte, wer sollte sonst vernünftig aufklären?

Aktuell: „Missing Link: Wie Staaten die Verschlüsselung im Internet per Gesetz aushebeln“. Der Artikel ist zwar lang, aber, mit Verlaub, richtig schlecht.

Erstens: Was ist überhaupt gemeint? Transportverschlüsselung oder Ende-Ende-Verschlüsselung der Nutzer? Oder gar beides?

Zweitens: Hat das irgendjemand angekündigt, die üblichen Verdächtigen hätten es gern (gähn) oder geschieht es real?

Drittens: Geht es um eine gesetzliche Grundlage, Verschlüsselung zu verbieten oder möchte man es nur umsetzen oder beides?

Viertens: Geht es um die Provider oder um die so genannten Endverbraucher oder beide?

Fünftens: Oder geht es um alles, Politiker haben aber keinen blassen Schimmer und raunen deshalb geheimnisvoll herum? „… nicht zuletzt der Einbau von Verschlüsselung in Basisprotokolle des Internets drohe den Zugriff auf kriminelle

Inhalte zu erschweren“ – großes Bullshit-Bingo!

Australiens Assistance and Access Act ist gerade hoch im Kurs bei denen, die auch für Europa ein Anti-Verschlüsselungsgesetz fordern. (…) Bei den Technical Assistance Requests (TARs), versorgen die Provider die australische Polizei sowie die verschiedene Geheimdienste mit entschlüsselten Daten von Zielpersonen.

Entschlüsselte Daten von Zielpersonen? Meinen sie die Zugangsdaten für E-Mail-Konten? (Was hülfe das?) Zugangsdaten für Websites und Social Media? Oder möchten jemand – am besten per Ferndiagnose – meine Veracrypt-Passwörter entschlüsseln? Have fun!

Australiens Regierung tritt dem Vorwurf, Hintertüren einzubauen, mit einer eigenen FAQ entgegen, in der sie über „Mythen“ spricht, die über das Gesetz verbreitet wurden.
Hintertüren? Ich will ja nicht schon wieder über die so genannte Online-Durchsuchung zetern (wenn die funktionierte, brauchte man ja keine Hintertüren). Nur für Windows oder auch für Linux Mint? Oder weiß man nichts Genaues wie immer nicht?

Oder sind andere Staaten nur neidisch über unsere schöne deutsche Sina-Box?

Guckst du hier: „Kanther fordert in seiner Rede, den Risiken, die sich aus der Technik ergeben auch mit den Mitteln der Technik zu begegnen und führt dabei unter anderem auch elektronische Wegfahrsperren als Mittel zur Verhinderung von Kraftfahrzeugdiebstählen an. Dieser Vergleich mutet seltsam unpassend an, handelt es sich dabei doch genau wie der Einsatz von kryptographischen Mitteln um ein klassisches Mittel zu Verbrechensprävention, nicht um ein staatliches Instrument zur Strafverfolgung. Eine Umsetzung von Kanthers Vorschlägen würde den Anwender von Datennetzen seiner legitimen Verteidigungsmöglichkeiten gegen Computerkriminelle berauben.
Kanther führt weiter aus, wie er sich die Kontrolle des

Staates vorstellt: “Dies kann dadurch geschehen, daß die verwendeten Schlüssel sicher hinterlegt werden. Durch eine Kombination von organisatorischen, personellen, technischen und juristischen Maßnahmen kann jedem Verdacht einer Mißbrauchsmöglichkeit begegnet werden.”

Das war am 28 April 1997! Es gibt noch andere hübsche Beispiele. Vor 20 Jahren fragte Florian Rötzer auf Telepolis: „Nichts mehr mit Pretty Good Privacy?“ Oder der Guardian (2001): „Pakistan to ban encryption software“.

Ich schrieb hier vor 12 Jahren: Der Artikel von Heise erinnerte mich an meinen Text auf *spiggel.de* vom 10.02.2007: „Geheimes Schreiben gegen Schäuble„, in dem ich Steganografie unter Linux vorstellte. Mit ein paar Befehlen kann man Texte so in Bildern verstecken, dass sie kaum gefunden werden.

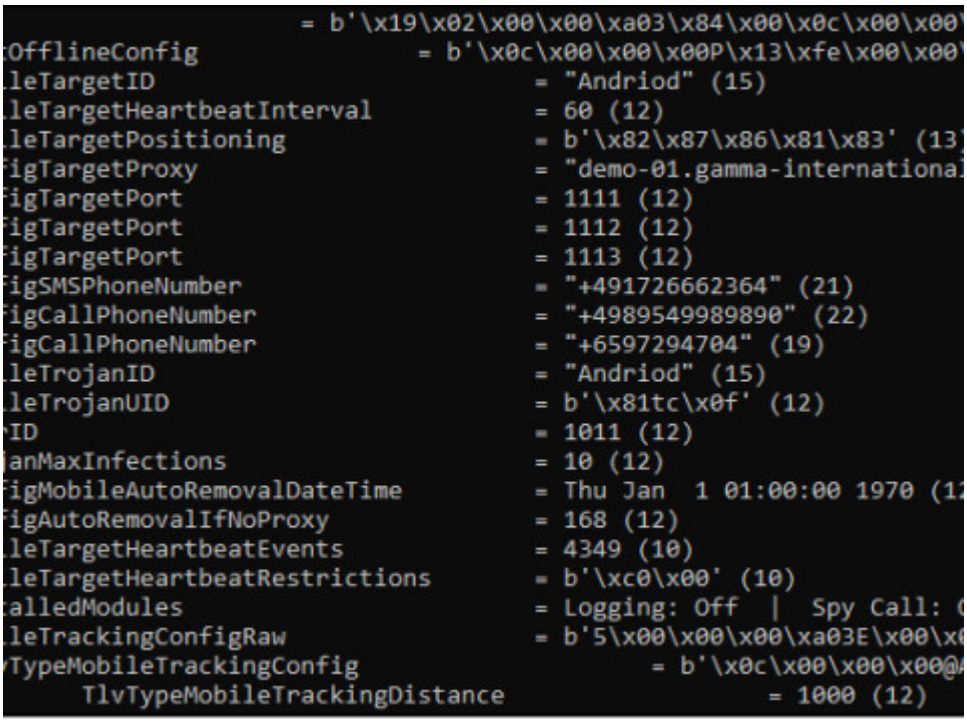
Hier ein Beispiel, die Fotos oben sind das Ergebnis: Das linke Bild ist das Original, im rechten Foto ist ein längeres Zitat aus dem Koran verborgen. Ich habe vorher nachgesehen, in welchen Passagen es um den Jihad geht.

```
burks@master:~/burksfiles/temp5$ touch osama.txt
burks@master:~/burksfiles/temp5$ echo "Und wenn die heiligen Monate abgelaufen sind, dann tötet die Götzendiener, wo immer ihr sie findet, und ergreift sie und belagert sie und lauert ihnen aus jedem Hinterhalt auf. Wenn sie aber bereuen und das Gebet verrichten und die Zakah entrichten, dann gebt ihnen den Weg frei. Wahrlich, Allah ist Allvergebend, Barmherzig;"> osama.txt
burks@master:~/burksfiles/temp5$ zip secretmessage.zip osama.txtupdating: osama.txt (deflated 36%)
burks@master:~/burksfiles/temp5$ cat 181008_2.jpg secretmessage.zip > 181008_3.jpg
```

Oder wünscht das Publikum, weil es besorgt ist, dass ich hier einen Online-Lehrgang über Steganografie anbiete? Gehe ich richtig in der Annahme, dass niemand mehr Windows 3.11

benutzt?

Bundestrojanische Gäule



Mit großem Interesse habe ich den Heise-Bericht über den „Spionage-Trojaner FinFisher“ gelesen. (Das heisst nicht „Trojaner“, sondern „Trojanisches Pferd“ – die Trojaner waren in Troja, und die Griechen saßen im Pferd.)

Schade, dass die Analyse des CCC „Evolution einer privatwirtschaftlichen
Schadsoftware für staatliche Akteure“ noch nicht erschienen war, als ich mein Buch veröffentlichte – es hätte Die Online-Durchsuchung gut ergänzt. Jetzt können wir „Butter bei die Fische“ tun. Kann die Frage: Wie fange ich mir so etwas ein? beantwortet werden?

Metzpolitik.org hatte schon vor vier Jahren geschrieben: „Die Begrenzung auf Windows 7 und Vista erscheint veraltet. Bereits

vor zwei Jahren haben wir berichtet, dass FinSpy Mobile auch für alle mobilen Systeme (also iOS, Android, BlackBerry, Windows Mobile und Symbian) existiert. Und letztes Jahr haben interne Folien bestätigt, dass FinSpy alle großen Betriebssysteme (Windows, Linux und Mac OS X) infizieren kann."

Der wichtigste Satz: „Über den Infektionsweg sagt das Team um Morgan Marquis-Boire wenig. Nur: Falls die Trojaner die mobilen Betriebssysteme nicht direkt angreifen, **benötigen alle untersuchten Exemplare eine Interaktion des Nutzers, wie dem Klicken auf einen Mail-Anhang oder eine Webseite**."

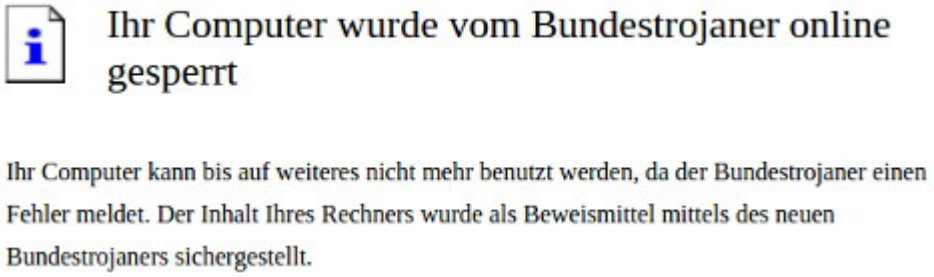
Genau das – und nur das! – habe ich immer behauptet, während fast alle Medienberichte entweder das Problem, wie die Spionage-Software zu installieren sei, vornehm ignorierten oder zu Magie – der Hacker hackt und ist irgendwann drin – greifen mussten.

Aber wie soll das funktionieren, wenn das Zielobjekt nicht total bekloppt ist? Klicken auf einen Mail-Anhang? Oha! Oder gar auf einer Website? Mit oder ohne Javascript erlaubt? Selbst wenn ein unerfahrener Windows-Nutzer Virustotal nicht kennt: Leben wir denn noch in Zeiten des Loveletter-Virus, als Outlook (wer nutzt das??) Anhänge nicht korrekt anzeigte?

Netzpolitik.org wies noch auf drei weitere Schwachstellen hin: Windows 7 SP1 – Acrobat Reader PDF Exploit, Windows 7 SP1 – Browsers Exploit, Windows 7 SP1 – Microsoft Office 2010 DOC-XLS Exploits. Schon klar. Das erinnert mich an 2003: „UK government gets bitten by Microsoft Word".

Hilfe, jemand wollte einen Bundestrojaner bei mir installieren! (25.06.2011) Nur gut, dass ich immer wachsam bin und die zunehmende Radikalisierung und Extremismusierung der E-Mail-Attachments bekämpfe!

Remote Communication Interception Software, reloaded [Update]



„Online-Durchsuchung bei Tätern, die nicht übers Internet kommunizieren“- großartige Zwischenüberschrift von Heise. Passt zum Niveau und zu den üblichen Textbausteinen, die seit 1993 zum Thema abgesondert werden.

In den Verhandlungen mit den Grünen zur anstehenden Verschärfung des Polizeigesetzes in dem südlichen Bundesland

hatte Strobl bei der Online-Durchsuchung nachgeben müssen. Bei dem Instrument geht es um das heimliche Durchsuchen von Festplatten von Computern, um beispielsweise Terrorpläne zu vereiteln.

Immer diese Festplatten! 2006 ging es um die berüchtigten „Internet-Festplatten, wahlweise auch ohne Internet.

Man kann natürlich auch ersatzweise Harry Potter lesen. Magie ist bei beiden Themen im Spiel. Ceterum censeo: Wie wollt ihr das anstellen, wenn das auszuspähende Objekt die Minimalstandards des sicherheitsbewussten Online-Verhaltens einhält? (Mal abgesehen davon, dass man zuerst die IP-Adresse des Zielrechners kennen müsste.)

Die so genannte Remote Communication Interception Software gibt es auch für Linux?! Und vermutlich funktioniert sie *ohne* physischen Zugriff (USB! USB!) auf den Zielrechner? Das will ich sehen. Bisher hat noch *niemand* etwas darüber gesagt, auch wenn der CCC manchmal geheimnisvoll herumraunte:
Zu den konkreten Methoden macht das Bundeskriminalamt keine Angaben – ‚aus kriminaltaktischen Gründen', wie ein Sprecher sagte. Zwar gebe es keine speziell geschulten ‚Online-Durchsucher', jedoch Spezialisten, die herangezogen würden. Es handele sich um Beamte, die ‚versiert auf dem Gebiet' seien. (…) Berichten zufolge haben die Sicherheitsdienste inzwischen auch Spionageprogramme entwickelt, die über das Trojaner-Prinzip hinausgehen. (…) Trojaner nutzen Sicherheitslücken, die nur mit großer Sachkenntnis gestopft werden können. ‚Der Privatnutzer kann sich dagegen kaum schützen', sagt Constanze Kurz, Sprecherin des Chaos Computer Clubs, einer Lobby-Organisation, die für möglichst wenig staatliche Überwachung im Internet eintritt.(FAZ.net, 05.02.2007)

Man kann sich nicht schützen? Das sagt der CCC? Was rauchen die da? Ich bin auch versiert, gefragt hat man mich aber noch nicht.

Jaja. Phishing E-Mails im Behördenauftrag?! Da kann Netzpolitik.org gern den Vertrag mit FinFisher veröffentlichen. Ich halte das für höheren volksverdummenden Blödsinn.

„Man könnte von ‚Durchsuchungssoftware' sprechen; bei bei Software für die Quellen-TKÜ von Remote Communication Interception Software (RCIS). De Facto ist es aber nichts anderes als Schadsoftware, die das Rechnersystem infiltriert und seine Funktion manipuliert."

Wie? Wie? Wie? Der Kaiser ist nackt! De facto ist das ein Meme.

Legendär immer noch Annette Ramelsberger (Süddeutsche, 07.12.2006): „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau."

Nein, das war mir bisher nicht klar, und wenn ich ehrlich sein soll, wurde es auch seitdem nicht klarer. Alle schreiben voneinander ab. Fakten werden sowieso überschätzt.

[Update] Ich habe *nie* behauptet, dass man keine Mal- oder Spionagesoftware auf fremden Rechnern installieren könne. Es funktioniert aber *nicht* so, wie sich das fast alle vorstellen: Von fern und weil irgendjemand das so will. Man braucht a) mindestens den (physikalischen) Zugriff auf den Zielrechner (um z.B. einen Keylogger oder per USB etwas aufspielen zu können) und b) muss sich der Nutzer selten dämlich anstellen (leider ist das wohl eher die Regel als die Ausnahme). Alles andere ist Humbug.

Online durchsuchen

Heise: „Wie Geheimdienste Cyberattacken durchführen – Ein Ex-FBI-Agent spricht über staatliche und nichtstaatliche Cyberangriffe, deren Zuschreibung und den Sony-Pictures-Hack.“

Komisch. Der spricht gar nicht über das Von-fern-auf-fremde-Rechner-zugreifen-und-online-durchsuchen!? Woran kann das nur liegen?

Online-Durchsuchung, revisited

Reporter ohne Grenzen (ROG) warnt vor Plänen des Bundesinnenministeriums, wonach deutsche Geheimdienste Medien im In- und Ausland künftig digital ausspionieren könnten. Einem Referentenentwurf zufolge sollen deutsche Inlands- und Auslandsgeheimdienste Server, Computer und Smartphones von Verlagen, Rundfunksendern sowie freiberuflichen

Journalistinnen und Journalisten hacken dürfen.

Dann hackt mal schön. Das ist doch wieder ein großer Schmarrn. Aber unsere „Online"-Journalisten werden das alle nachbeten.

Ich schrieb im Oktober 2009: Der Kaiser ist bekanntlich nackt und Online-Durchsuchungen hat es nie gegeben und wird es nie geben. Jedenfalls nicht so, wie sie der Volksmund und Klein Wolfgang verstehen: Da sitzt ein Ermittler irgendwo in einer Behörde und sucht und findet die IP-Adresse des Computers eines Verdächtigen, spielt dem dann „online" und unbemerkt ein Spionageprogramm auf und liest dann mit? Vergesst es. Keep on dreaming. Die real gar nicht existierende Online-Durchsuchung ist der einflussreichste Medien-Hoax, den ich kenne, ein hübsches urbanes Märchen, das vom Wünschen und Wollen ahnungsloser Internet-Ausdrucker und noch mehr vom ahnungslosen Geraune der Medien am Leben erhalten wird. Nicht

ich muss beweisen, dass es bisher *keine* „Online-Durchsuchung gab, sondern diejenigem, die behaupten, so etwas würde gemacht, müssen Fakten, Fakten, Fakten liefern – wer, wie und womit.

Wenn der Nutzer sich total dämlich anstellt, dann ginge es – und nur mit physischem Zugriff auf den Rechner. (Und welchen? Hackt ihr auch meinen Router und mein Intranet?)

Und kommt mir jetzt nicht mit FinFisher: *…Spionageprogramme, die bislang unbekannte Sicherheitslücken von Smartphones und Computern ausnutzen, um sämtliche Aktivitäten der Nutzer auszuspionieren: Mail-Korrespondenz, Adressbücher, Chat-Programme, Telefonanrufe – sie schalten sogar Kamera und Mikrofon nach Belieben ein, ohne dass der Nutzer dies merkt.*

Ach ja? PGP ist jetzt auch „gehackt“? Meine Mail-Korrespondenz, falls unverschlüsselt, wird doch schon durch die SINA-Box mitprotokolliert. Wozu jetzt noch mal draufsatteln? Meine Kameras schaltet niemand ein. Nur damit ihr’s wisst.

[Update] Fefe hat was über die Cyberpläne vom Cyberheimathorst.

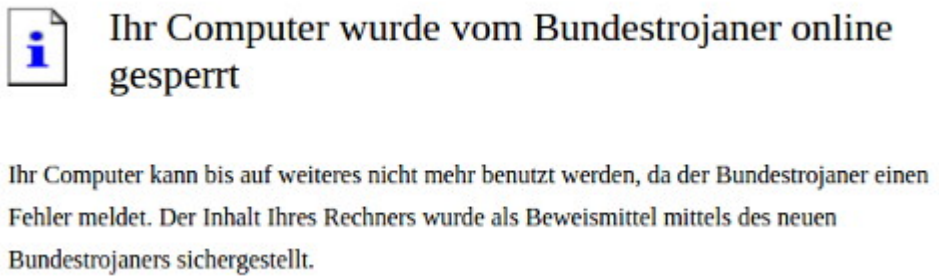
Embedded Journalism

Telepolis: „Wie der BND die deutschen Medien steuerte“. – „Geheimdienstexperte Erich Schmidt-Eenboom über Verbindungen der geheimen Dienste, die bis in die Chefredaktionen der größten deutschen Medien reichen“ Der Artikel wird aber nichts nützen.

Interessant ist, dass meine Vermutung über die Ramelsberger

von der „Süddeutschen“ geteilt wird. Da sind wir dann wieder bei der „Online-Durchsuchung.“

Bitte durchsuchen Sie mein Gerät!



Ich habe eine kleine und unmaßgebliche Frage, die bekanntlich niemanden interessiert: *Wie will man Computer „heimlich“ durchsuchen?*

„…ist es nötig, die Geräte der Betroffenen mit Schadsoftware in Form sogenannter Staatstrojaner zu infizieren.“

Wie? Wie? Wie?

Bundestrojanisches Pferd oder: Technisch dürfte es

dabei Probleme geben

Heise: „Generell bleibt es dabei, dass Strafverfolger die Möglichkeit erhalten, Internet-Telefonate etwa per Skype und die Kommunikation über Messenger wie WhatsApp, Signal, Telegram oder Threema zu überwachen.“

Ach ja? Signal kann man also überwachen? Wie denn? Hat sich Edward Snowden geirrt? Oder ist das nur eine Verschwörungstheorie? Ich kriege schlechte Laune, wenn ich diesen Schwachfug lese.

„Mit dem derzeitigen Bundestrojaner, den IT-Experten vom BKA innerhalb von drei Jahren entwickelt hatten, können Messenger-

Programme nicht abgehört werden. Berichten zufolge ist damit nur eine Quellen-TKÜ von Voice over IP (VoIP) über Skype auf Desktop-Rechnern mit Windows möglich.“

Sonst nix. Was ist mit Skype für Linux? Fragen über Fragen. Und niemand macht sich die Mühe, das Publikum aufzukären. Nur geheimnisvolles Herumgeraune.

Berichten zufolge war schon vieles möglich. Wahr wird es dadurch nicht. Warum übernimmt der Autor Stefan Kremp die Terminologie derjenigen, die auf Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme missachten?

Wenn man sich ältere Berichte zum Thema anschaut: Wir kommt der Mist auf einen Rechner? Ja? Ich höre?!

Sind eigentlich alle irre? Soll das Journalismus sein?

Die Details entscheiden oder: Abhören leicht gemacht

Kaiserwetter, die letzten Tage meine Urlaubs. Da muss ich eine kleine Radtour machen, um ein Café zu finden, in dem ich in Ruhe einen Milchkaffee trinken kann (und in dem es auch einen gibt, nicht nur „Latte“ irgendwas). Schön. Aber trotz der Sonnenstrahlen, die sogar wärmen, pfeift ein Wind mir störend meine Frisur kaputt nzw. die Haare ins Gesicht. Das Fahrrad hat trotz angeblich „unplattbarer“ Reifen einen Platten, aber natürlich erst an dem Ort, der von meiner Wohnung am weitesten entfernt liegt. Manchmal sind eben die Details wichtig. das kenne ich aus Südamerika: Das schönste Panaroma wird manchmal uninteressant, wenn man keinen Platz zum Kacken findet, aber muss.

Und ich muss wieder im gedruckten „Spiegel“ von Praktikanten geschriebene Verschwörungstheorien lesen, die kein Journalist, der sein berufliches Ethos – falls vorhanden – ernst nähme, so schlampig formulieren würde.

Das Bundesinnenministerium will eine neue Sicherheitsbehörde aufbauen.
Nun gut, die „wollen“ immer viel. Wer den „Spiegel“ gebrieft hat über das Wollen, wollte auch etwas. Haben wir nicht schon einige Behörden mit einem „Cyber“ drin? Ein Cyberabwehrzentrum

zum Beispiel? Eine Allianz für Cybersicherheit? „Bundesinnenminister Wolfgang Schäuble und die Gewerkschaft der Polizei (GdP) drängen auf eine verstärkte Inspektion der Kommunikationsströme im Internet, um online vorangetriebene Terrorplanungen und Hetzpropaganda zu verhindern. ‚Wir müssen die Kontrolle des Internets verstärken.'“. Ach so, das sagte er schon 2006. Manche Dinge kann man eben nicht oft genug sagen.

Mit deren Hilfe soll Internetkommunikation besser überwacht und Verschlüsselung geknackt werden.
Das, lieber „Spiegel“, ist kein Journalismus, das ist Propaganda. „Besser“ ist suggestiv und stammt garantiert nicht von eurem Praktikanten, sondern ist die Wortwahl des Briefings durch eben diesen Informanten aus dem Ministerium, das etwas will. Und starke Verschlüsselung kann man eben *nicht* knacken. Was soll also diese heiße Luft? Wenn ihr wieder mal Verschlüsselung der Inhalte und Transportverschlüsselung durcheinanderwürfelt, klärt das nicht auf, sondern verdummt das Volk, weil das Volk sich angesichts dieser lancierten Meldung fürchtet und ängstigt nach dem Motto: Die sind schon drin, man kann eh nichts tun. Und das war so gewollt von denen, wie wieder einmal etwas wollen und euch das sagten.

Aufgabe der Behörde sei es unter anderem, neue Methoden zu entwickeln, um in verschlüsselte Kommunikation, etwas bei Messenger Diesten [im Original fehlt hier ein Komma] eindringen zu können, heißt es in Regierungskreisen.
Oha! Wenn die Kreise in der Regierung meinen, das funktionierte, dann muss es ja wahr sein. By the way: Was halten diese Kreise denn von Signal, von Snowden empfohlen und abhörsicher? Gefällt denen das nicht? Wie wäre es, wenn der „Spiegel“ neue Methoden entwickleln würde, um bei Intenet- und Computerthemen nicht mehr auf dem Niveau von Richterin Barbara Salesch zu berichten?

Auch bei der Onlinedurchsuchung, bei der der Rechner einer Zeilperson infiltiert wird, sowie beim Abhören von Gesprächen

könnte die Behörde neue technische Werkzeuge entwickeln.
Sie könnte? Warum? Weil eine Behörde immer besser ist beim Bullshit-Bingo als Gamma International aka FinFisher Intrusion? Und wie kriegt man Finspy auf einen Rechner? Das wollte ich immer schon mal wissen. Aber niemand antwortet mir, auch nicht Wikipedia oder der CCC. Ist vermutlich alles geheim.

Die Pläne sind allerdings regierungsintern umstritten.
Der oberflächliche Quatsch, den ihr da verbreitet, ist journalismusintern auch umstritten.

Lukratives Geschäft mit Schnüffel-Tools

Heise: „Nachdem Hacker über 400 Gigabyte an internen Dokumenten von Hacking Team entwendet haben, versucht der Hersteller von Überwachungssoftware, den Schaden zu begrenzen."

Hahahahaha. Geschieht ihnen recht.

Übrigens, für unsere Online-Durchsuschungs"-fans hat ein kluger Mensch einiges bei Heise notiert: „Wie der RemoteDesktop-Server aufs Zielsystem kommt, wurde bisher als Problem des Anwenders angenommen worden."

Es ist wie gehabt: Die wichtigste Frage stellt niemand (das darf doch nicht wahr sein?): Wie kommt das Zeug auf einen Rechner?

Cyber-[bitte selbst ausfüllen]

Wie macht man einen Cyber-Bankraub? Die Antwort wissen die Experten in den Medien schon seit der so genannten „Online-Durchsuchung“:
Die Angreifer verschicken E-Mails mit gefährlichem Dateianhang an Adressen, hinter denen sie Bankmitarbeiter vermuteten. Sobald die den Anhang öffnen, zum Beispiel ein infiziertes Word-Dokument, installiert sich das Schadprogramm von selbst und öffnet den Angreifern eine Hintertür ins Banknetzwerk.

Einmal mit Experten arbeiten. Unverschlüsselte Mails. Attachments (für Linux?) Word. WTF?!

Aber man muss sich das Geheule und Zähneklappern anhören, wenn man in einem Fortbildungsseminar den Teilnehmern sagt: „E-Mails verschlüsseln. Keine Word-Attachments usw.“.

Trojanisches Pferd liegt noch nicht vor

Jochen Kuri (Heise): „…bei der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) werden unter anderem VoIP-Gespräche vor der Verschlüsselung beim Sender beziehungsweise nach der Entschlüsselung beim Empfänger durch einen eingeschleusten Trojaner abgehört. Die Regelung sei derzeit unverhältnismäßig, weil eine derartige Software noch

gar nicht vorliege und der Gesetzgeber sie daher nicht genau kennen könne, sagte Gerichtspräsident Winfried Schubert.“

Die Software gibt es noch gar nicht? Ach so. Die bauen daran noch – offenbar seit 2006. Aber man kann ja trotzdem behaupten, dass täglich onlinedurchsucht wird. Hört sich einfach besser an.

Secret Manuals oder: Emulating an access point

3 Install the agent on the target device with the selected methods.
See "List of installation vectors" on page 138 .

List of installation vectors

Operating systems supported by agents

Operating systems supported by the various desktop and mobile devices are listed b

Device	*Operating System*
Desktop	• Windows • OS X
Mobile	• Android • BlackBerry • Windows Mobile • Symbian • IOS

The Intercept: „Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide – Hacking Team manuals, dated September 2013, provide step-by-step instructions for technicians, administrators, and analysts on how to infect a device and set up spying.“

„The spyware installer might lay in wait in a hotel, or a Starbucks, and gain access to your computer by ‚emulating an

access point‘ – in other words, pretending to be a free wifi hotspot to which the victim connected previously.“

Ich weiß ja nicht, aber wer ist denn so blöde, darauf hereinzufallen? Ich habe mir mal einige dieser Handbücher durchgesehen, vor allem das rcs-9-technician-final.pdf ist interessant. Auf keinen Fall kann die Spionage-software zum Erfolg kommen, wenn der Nutzer sich vernünftig verhält. Und bei Linux auch nicht. Wen wollen sie also ausspionieren? Klein Fritzchen?

Als er einmal auf die cipav.exe klickte

Heise über das FBI, das einen Artikel fälschte, um Malware auf dem Rechner eines Verdächtigen zu installieren:

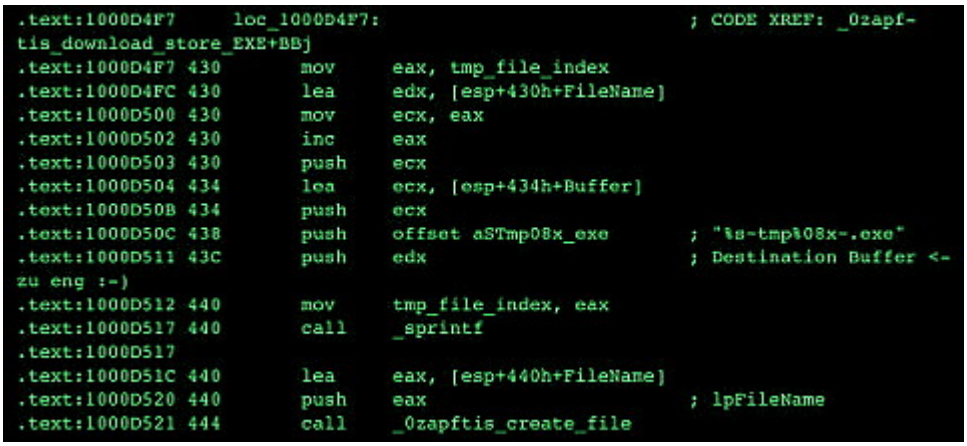
Dafür fälschten sie einen angeblich von der Nachrichtenagentur AP stammenden Artikel über Bombendrohungen und verschickten einen Link darauf an einen MySpace-Account. Als der Verdächtige darauf klickte, sei ihm die Software „Computer and Internet Protocol Address Verifier“ (CIPAV) auf dem Rechner installiert worden“.

Merke: Der Verdächtige hatte Windows (sonst hätte es nicht funktioniert). Der Verdächtige las unverschlüsselte E.Mails.

Der Verdächtige las unverschlüsselte E-Mails von fremden Personen. Der Verdächtige klickte auf Links in E-Mails (er verhielt sich grob fahrlässig, weil er HTML-E-Mails empfing und sie auch so anzeigen ließ). Der Verdächtige war grob unvorsichtig und hatte Javascript *nicht* verboten (nur so ginge das). Der Verdächtige surfte vermutlich übr einen Admin-Account und wurde nicht beim Installieren eine Software gefragt. Der Verdächtige verhielt sich denkbar bescheuert.

Übrigens stammt die Geschichte aus der Wired aus dem Jahr 2007: „The software was sent to the owner of an anonymous MySpace profile linked to bomb threats against Timberline High School near Seattle. The code led the FBI to 15-year-old Josh Glazebrook, a student at the school, who on Monday pleaded guilty to making bomb threats, identity theft and felony harassment."

Der Kaiser ist nackt!



Heise meldet, dass die Bundesregierung behaupte, die Software zur Online-Durchsuchung sei einsatzbereit. Das ist aber nicht neu. Wie man der von mir erstellten Chronik der Medienberichte über die so genannte „Online"-Durchsuchung sehen kann, soll das schon vor acht Jahren möglich gewesen sein. Der

Tagesspiegel titelte am 08.12.2006: „Die Ermittler surfen [sic!!] mit“:

“Das System der sogenannten „Online-Durchsuchung“ sei bereits in diesem Jahr mehrfach angewandt worden und sei Teil des 132 Millionen Euro schweren Sonderprogramms zur Stärkung der inneren Sicherheit. Die Ermittler sollen sich dabei auf richterliche Anordnung unbemerkt via Internet in die Computer von Privatpersonen einloggen können, gegen die ein Strafverfahren läuft.

(Viele Links funktionieren nicht mehr, aber anhand des genauen Titels kann man sie noch finden, teilweise über archive.org)

Manchmal fühle ich mich wie allein gelassen unter lauter Irren. Was nützt mir ein derartiger Bericht wie der aktuelle bei Heise, wenn niemand fragt, wie die Überwachungssoftware auf den Rechner des „Zielobjekts“ gekommen ist? Das ist doch – jenseits der empörten Attitude – eine der wichtigsten Fragen überhaupt? Es braucht doch mindestens den physischen Zugriff (und dann müssen bestimmte Voraussetzungen gegeben sein), oder das „Opfer“ muss Malware wie Skype schon installiert haben.

Es geht aber mitnichten so, dass jemand „von fern“ irgendwas installiert. Außerdem müsste man ja auch die IP-Adresse wissen und eventuell noch den Router austricksen. (Jetzt fange hier niemand davon an, etwas von „Mail-Attachments“ zu faseln oder von „Websites, auf die man „gelockt“ werden soll. Ich kann es nicht mehr hören.) Christian Rath schrieb in der *taz* am 11.12.2006:

Denkbar sind verschiedene Wege. So kann die Polizei versuchen, ein „Trojanisches Pferd“ (kurz Trojaner) auf den Computer des Betroffenen zu schleusen. Ein Trojaner ist ein Programm, das heimlich Aktionen auf dem Computer ausführt, ohne dass der Benutzer dies bemerkt. Der Trojaner kann zum Beispiel als Anhang mit einer getarnten E-Mail auf den Rechner gelangen. Vorsichtige Computernutzer öffnen aber keine unbekannten

Anhänge oder schützen ihren Computer mittels Firewall oder Filter schon vor dem Zugang solcher Spionagesoftware.

Soll ich das jetzt noch kommentieren?

Am 08.10.2011 berichtete Heise:
Dem Chaos Computer Club (CCC) ist nach eigenen Angaben die staatliche Spionagesoftware zugespielt worden, die allgemein unter dem Begriff „Bundestrojaner“ oder in bundeslandspezifischen Versionen beispielsweise auch als „Bayerntrojaner“ bekannt wurde.

In der Analyse des CCC (LESEN!) heisst es: „Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Ach so. Dann gibt es den „Trojaner“ nicht für Linux? Das ist aber schade.

Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten. Andere mögliche Verfahren wären ähnliche Angriffe, wie sie von anderer Malware benutzt werden, also E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Es gibt auch kommerzielle Anbieter von sogenannten Infection Proxies, die genau diese Installation für Behörden vornehmen

E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Und so etwas schreibt der Chaos Computer Club?! OMG.

Ceterum censeo: Der Kaiser ist nackt!

Skypekit

Ich habe die Skype-Software schon seit langem von meinen Rechnern geworfen, weil Skype bekanntlich Malware ist. Meinen Skype-Account nutze ich via Trillian. Das ging aber nicht mehr. (Ich nutze Skype eigentlich nur, um als Warlord virtuelle Hauereien in Secondlife zu koordinieren.)

Am 12. Juli 2013 wurde durch von Edward Snowden geleakte Informationen bekannt, dass den amerikanischen Geheimdiensten durch Microsoft tatsächlich direkter Zugriff auf den gesamten Skype-Verkehr gewährt wird und sowohl Textchats als auch Telefonate und Videotelefonate nach Belieben von der NSA mitgeschnitten und ausgewertet werden können, da es dem Geheimdienst mit Hilfe des direkten Zugriffs auf die Skype-Server möglich ist, die Skype-Verschlüsselung zu umgehen.

Jetzt habe ich eine Lösung für Windows 7 gefunden: „Skypekit in Trillian noch eine Weile weiter nutzen“.

Ich möchte die technikaffinen Leserinnen und sicherheitbewussten Leser auffordern, mir die Risiken des älteren Skypekit via Trillan aufzuzählen.