Unter Propagandisten

Jemand fragte bei Heise: „Wie genau schafft es Russland verschlüsselte Kommunikation aufzubrechen? Ich bin bisher davon ausgegangen, dass man das nur mit dem Einsatz von Trojanern auf dem Gerät des Nutzers hin bekommt. Welchen Beitrag die Kompromittierung der Netze dazu hat, ist mir nicht klar.“

Ich hatte geantwortet, dass der Autor des Artikels, Stefan Krempl, nur die „Propaganda der Sicherheitsbehörden“ wiedergebe. So war das auch beim Thema „Online-Durchsuchung“.

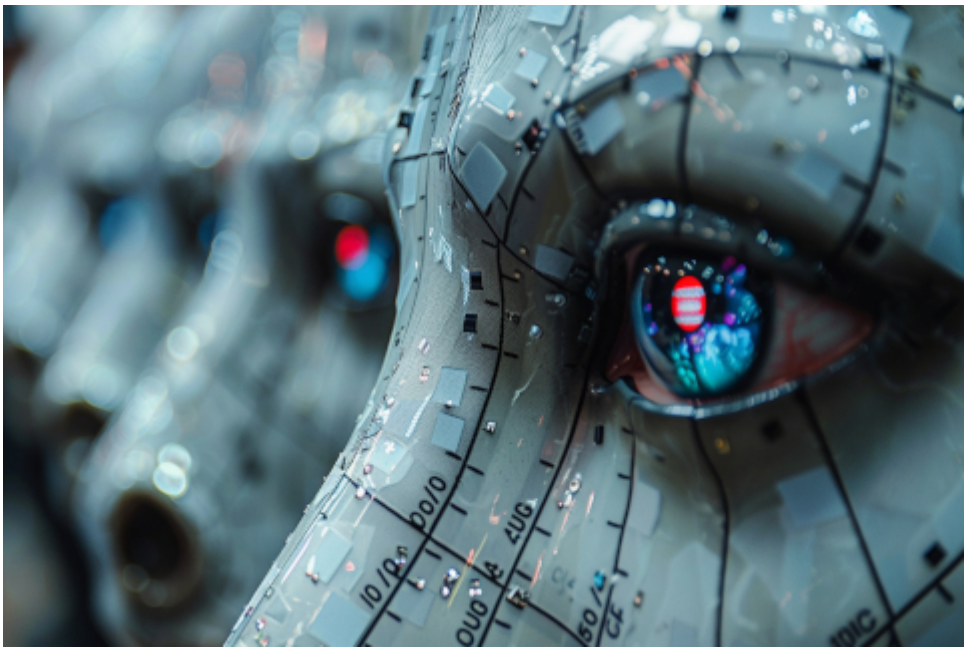
Mein Beitrag würde von Heise ~~wegen Hassrede~~ gesperrt. Die sind ganz schön dünnhäutig. Also habe ich offenbar einen Nerv getroffen.

Ich erinnere an Annette Ramelsberger in der „Süddeutschen“: „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.“

Auch das nenne ich „die Propaganda der Sicherheitsbehörden

wiedergeben“. Journalismus ist das nicht.

Bombenbauanleitungen, revisited



Midjourney macht ganz großartige Bilder mit den Befehlen „online surveillance, remote access, computer, trojan horse“ oder nur „online surveillance, remote access, computer“. Hier ein Beispiel.

Oha, es hört nie auf. Sachsens Innenminister Schuster will Rechner „online durchsuchen“ – und kein Journalist lacht ihn deswegen einfach aus:
Schuster: Die Frage ist doch, ob mehr Polizisten auf analogem Weg dieselben Daten erheben zu können. Also den Postboten abzufangen, um zu wissen, was sich ein Terrorgefährder für den Bau einer Bombe liefern lässt, ist ziemlich naiv und gefährlich. Vor allem, wenn ich im Gegensatz dazu bei einer Onlinedurchsuchung auf seinem Rechner die Bauanleitung für die Bombe finden könnte.

Alle dämlichen Klischees beisammen.

Trojaner auf externen Internet-Festplatten

Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

Krempl liefert bei Heise wieder den gewohnten Bullshit ab: „Strafverfolger haben Staatstrojaner 2021 häufiger eingesetzt. Die Gerichte genehmigten 2021 55-mal das Hacken von IT-Geräten, während es 2020 48 Anordnungen gab.“

Ach ja? Wie machten die das? „Mithilfe von Staatstrojanern“ natürlich. „Dabei dürfen die Fahnder etwa auch Festplatten inspizieren und nicht nur die laufende Kommunikation mitschneiden.“ Die Internet-Festplatten sind schon seit 2006 als Textbaustein in Mode.

Ich halte das für ein fettes Lügenmärchen aus der Propaganda-Maschine der Strafverfolger, das Krempl wie gewohnt kritiklos wiederkäut. Natürlich können die üblichen Verdächtigen „Kommunikation“ in Echtzeit verfolgen, etwa bei der Telefonie. Aber sie können nicht einfach so auf externe „Festplatten“ zugreifen, schon gar nicht „von weitem“, außer der Verdächtige

ist so bekloppt, dass er vermutlich gar keinen Computer bedienen könnte.

Außerdem gab es da mal ein Urteil des Bundesverfassungsgerichts. Jemand kommentierte ganz richtig: „Zunächst mal heißt es eben nicht, daß das Instrument auch eingesetzt wurde, nur weil ein Richter die Erlaubnis erteilt hat. Und weiterführend sagt das auch nichts darüber aus, ob es erfolgreich eingesetzt wurde, ob verwertbare Informationen erlangt wurden, die sonst nicht erlangt worden wären, usw..“

Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

---

Surveillance, allüberall und nirgends [Update]

Midjourney/©Burks

Heise veröffentlicht Bullshit-Bingo für Klein-Fritzchen, natürlich von Stefan Krempl. Ich weiß nicht, was den treibt. „Polizei soll Staatstrojaner nicht mehr bei Alltagskriminalität einsetzen.“

– Erstens heißt es nicht „Staatstrojaner“. Die Trojaner waren draußen, die Griechen saßen im Pferd.

– Zweitens darf die Polizei das nicht (was sie natürlich nicht daran hinderte). Es gibt ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Oder ist die Entscheidung des Bndesverfassungsgerichts mittlerweile revidiert worden, Heise? Nein, ist sie nicht.

Midjourney/©Burks

– Drittens ist es technisch grober Unfug, auch wenn tausend juristische Pappnasen das immer wieder anders behaupten. Man sollte auch nicht die Transportverschlüsselung mit der Verschlüsselung von Inhalten auf einem Rechner verwechseln. Nur noch einmal, Krempl, zum langsamen Mitschreiben: **niemand** (in Worten: niemand) kann auf meine Rechner von „draußen“ zugreifen, selbst wenn ich einen Angriffskrieg vorbereitete. **Niemand** hat auch bisher erklärt, wie das gehen sollte. Die raunen nur alle geheimnisvoll herum und tun sich wichtig damit.

Ohne weiteres kann der Staat jedoch nicht erfassen, was auf einem Computer geschieht. Der einzige Weg ist über Sicherheitslücken in den betroffenen Systemen. Und hier muss man sich schon wundern: Statt, dass der Staat hilft, bekannte Lücken zu schließen oder zumindest auf sie aufmerksam zu machen, die letztlich alle Nutzer von Computern gefährden und

von Kriminellen ausgenutzt werden können, nutzt er sie selbst aus, um das Gerät zu hacken und „mitlesen“ zu können. (Das „schreiben Mitarbeiter der intersoft consulting, die als Experten für Datenschutz, IT-Sicherheit und IT-Forensik international Unternehmen beraten.“)

Der Staat nutzt also Lücken aus? Wie denn? Beispiele?! Das Bundesinnenministerium kauft also Zero-Day-Exploits, womöglich für Linux? Ihr spinnt doch.

Midjourney/©Burks

– Viertens gibt es die „Online-Durchsuchung“ weder bei „Alltagskriminalität“ noch bei schweren Straftaten, nur im nachhinein, wenn die Rechner des Verdächtigen beschlagnahmt wurden und dieser auch noch ein IT-Vollidiot ist.

Was will mir dieser Artikel suggerieren? „Bei der Quellen-TKÜ geht es darum, die laufende Kommunikation per Staatstrojaner direkt auf dem Gerät eines Verdächtigen abzugreifen, bevor sie

ver- oder nachdem sie entschlüsselt wurde.“ Ach ja? Und wie soll das gehen? Krempl, du bist ein Verschwörungstheoretiker.

Dazu passt noch ein ganz ähnlicher Artikel: „Autos, Navis & Co.: Polizei will Zugriff auf alles – unverschlüsselt und sofort“. Schon klar. Ich will auch Diktator von Deutschland werden. Das ist ähnlich realistisch, selbst wenn diejenigen, die das fordern, Nachhilfeunterricht beim Chinesen nähmen.

Midjourney/©Burks

[Update] Links repariert.

Die Online-Durchsuchung mit Trojanern

/imagine a computer::3 screen::3 with a trojan horse::3 galloping out it, photorealistic, steampunk

Endlich habe ich bessere Bilder, falls ich noch einmal über die gar nicht so real existierende „Online-Durchsuchung“ schreiben sollte. Dieses Mal stammen alle Befehle ausschließlich von mir.

Unter Staatstrojanern (m/f/d)

Online-Durchsuchung und Chatkontrolle in Secondlife (2007)

Da ist sie wieder, die gute, alte Online-Durchsuchung, von der immer noch niemand zu sagen weiß, wie sie denn funktionieren soll. Jetzt hat sie sich das Kostüm „Chatkontrolle“ umgehängt und geistert geheimnisvoll raunend durch die Medien.

Durch das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ durften Behörden versteckte Schadsoftware auf Computern, Laptops und Smartphones platzieren.

Soso, lieber Kollege Jakob Schirrmacher, der nach eigenen Angaben „1987 noch nicht gelebt“ hat und, ebenfalls nach eigenen Angaben, freier Journalist, Autor, Dozent für Medien und Digitalisierung ist, also so etwas wie ich, nur ohne Zweitberuf, und, ebenfalls nach eigenen Angaben, jemand ohne PGP-Schlüssel auf der Website. Die dürfen „versteckte Schadsoftware“ auf meine Linux-Rechner beamen, womöglich von fern, wenn ich gerade nicht hingucke, warum es verdächtig ruckelt?

Ich habe da mal eine Frage: Wie machen „die“ das? Vielleicht darf man das gar nicht fragen, weil es supergeheim ist? Und hatte das Bundesverfassungsgericht die so genannte TKÜ (Quellen-Telekommunikationsüberwachung) nicht 2008 verboten? Da warst du doch schon geboren, lieber Kollege?!

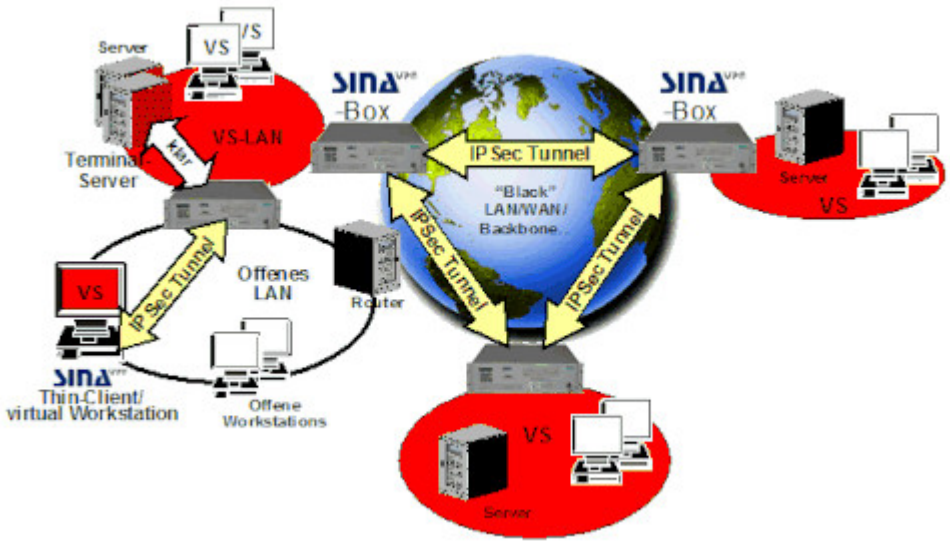
> Was auffällt: Die Überwachungsmaßnahmen kommen dem Bürger näher und näher: vom Auto in den Wohnraum, hin zum Telefon und schließlich bis hin in die tiefste Gedankenwelt. Dies gelang beispielsweise durch die später eingeführte Quellen TKÜ (Quellen-Telekommunikationsüberwachung), die 2017 ihre Vollendung feierte. Durch das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ durften Behörden versteckte Schadsoftware auf Computern, Laptops und Smartphones platzieren.
>
> Der sogenannte Staats Trojaner ermöglichte es Behörden, Messenger Chats und SMS mitzulesen, sowie Kameras und Mikrofone zu benutzen. Der Gesetzestext dazu lautet: „Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“.

Mir ist eine „drohende“ Chatkontrolle übrigens völlig schnurzpiepegal. Ich mache das so, wenn ich nicht ohnehin das quelloffene Signal benutze: Ich rufe irgendein IRC-Programm auf. Vorher habe ich mich per verschlüsselter E-Mail mit meinen Mitverschworenen (m/f/d) verabredet, dass wir uns auf irc.brasirc.com.br treffen und dort einen passwortgeschützten Kanal eröffnen. Und dann chatten wir und tauschen Daten aus.

Nein, ich habe eine bessere Idee. Wir loggen uns mit halbnackten Avataren in Secondlife ein und treffen uns in einem Adult-Segment (irgendwas mit Porn) oder treffen uns auf meiner Sim, umbraust von virtuellen Sandstürmen und die virtuellen Waffen immer griffbereit, um Chatkontrolleure virtuell abzumurksen.

Ich finde ein Gesetz zur Chatkontrolle gut und richtig. Dann befassen sich die, die jetzt noch zum Thema ahnungslos herumfaseln, endlich mit Sicherheit und Datenschutz. Oder halten die Kresse, was auch nicht schlecht wäre.

Sonstige Rechte



Credits: BSI

Netzpolitik.org: *Das geplante Gesetz gegen digitale Gewalt handelt von weit mehr als digitaler Gewalt. Justizminister Marco Buschmann will umfassend Auskunftsansprüche ausweiten: auf Urheberrechtsverletzungen, Messenger und private Inhalte.* (Fefe dazu.)

Das Ministerium Für Wahrheit informiert: Urheberrechtsverletzungen sind jetzt „digitale Gewalt“. Warum nicht gleich „Hassrede“? (Wer hat diese bescheuerten Begriff eigentlich erfunden?)

Das geplante Gesetz gegen digitale Gewalt zielt aber nicht nur auf digitale Gewalttäter. Es regelt „alle Fälle einer rechtswidrigen Verletzung absoluter Rechte“. Unter absolute Rechte fallen „sonstige Rechte“, unter anderem auch Immaterialgüterrechte wie „geistiges Eigentum“.

Es wird wieder so sein wie immer und wie schon bei der so genannten „Online-Durchsuchung“. Diejenigen, die jetzt Gesetze mit immer öfterem Komparativ fordern, haben keinen blassen Schimmer, worum es technisch überhaupt geht und wie das durchzusetzen sei. Und die anderen, die das wissen, jammern über die pöhse Politik, statt die auszulachen und ihnen mitzuteilen, dass sie damit höchstens Klein Fritzchen kriegen, aber sonst niemanden.

Natürlich sind die neuen Gesetze gegen das Böse im Internet wie eine Schrotflinte. Man schießt blind drauflos und hofft, dass jemand getroffen wird.

Im Gesetzentwurf steht der wunderschöne Satz: *Die Identität des Verfassers einer rechtswidrigen Äußerung kann aber regelmäßig nur ermittelt werden, wenn zuerst der Telemedienanbieter die IP-Adresse herausgibt und der Internetzugangsanbieter dann in einem zweiten Schritt Auskunft gibt, wem diese IP-Adresse zum Zeitpunkt der Äußerung zugeordnet war.*

Quod erat demonstrandum: Die Vorratsdatenspeicherung, reloaded, revisited. Sie versuchen es so oft, bis es irgendwann versehentlich durchkommt.

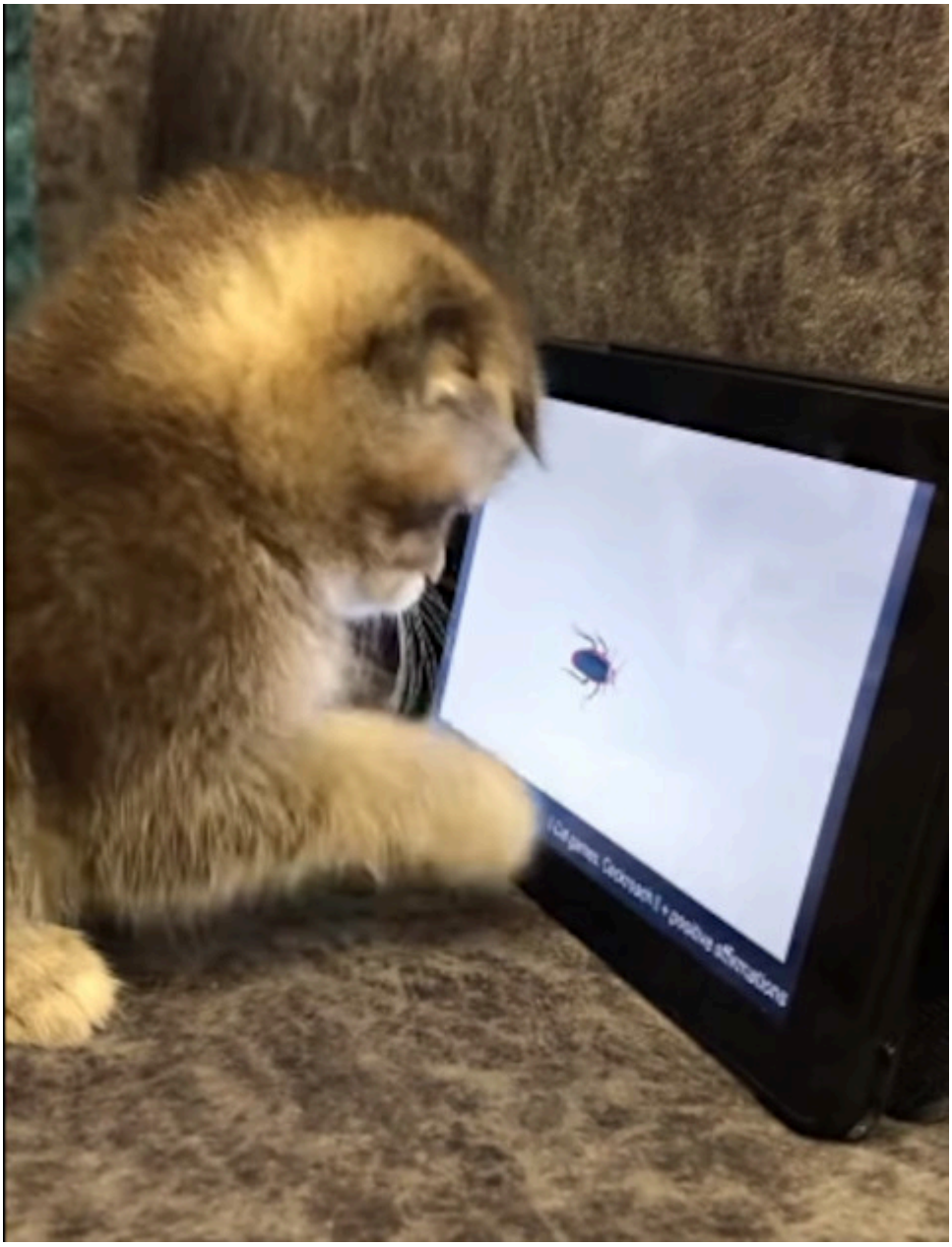
Bei offensichtlichen [!] Rechtsverletzungen soll das Gericht den Diensteanbieter bereits durch eine einstweilige Anordnung verpflichten können, Auskunft über die Bestands-und

Nutzungsdaten eines Verfassers zu erteilen.

Das ist schiere Willkür und natürlich auch fehlende Normenklarheit, wird also vom Bundesverfassungsgericht in die Tonne getreten werden. Technisch allerdings geht das – die Infrastruktur mussten die Provider auf eigene Kosten anschaffen.

Man darf also Hausdurchsuchungen zum Beispiel wegen einer Restaurant- oder Hotelkritik erwarten, die dem Besitzer nicht gefällt.

Sie sind mit dem Internet verbunden.



Das technische Problem, ein Insekt zu fangen, wurde in diesem Fall nicht zufredenstellend gelöst.

Verehrtes Publikum: Ich verneige mich in Ehrfurcht vor den versierten Beiträgen, die meine technischen Probleme weitgehend lösten. Weitgehend.

1. VPN via WireGuard geht jetzt auf allen Betriebssystemen. Warum ist man (zx2c4 und Edge Security) darauf nicht schon früher gekommen?
Keep in mind, though, that „support“ requests are much better suited for our IRC channel. Har har. I love it. Old school.

So gaaaaanz einfach war es unter Linux nicht. Heiko Richter hat es dankenswerterweise relativ volkstümlich erklärt.

In die Datei /etc/wireguard/wg0.conf fügen wir die Konfiguration ein, die wir von der Fritz!Box erhalten haben. Die Datei, die einem die Fritzbox vorher – bei der Einrichtung von WireGuard – geruhte zu überreichen, heisst wg_config.conf und funktioniert sowohl für Windows und Linux (sudo gedit

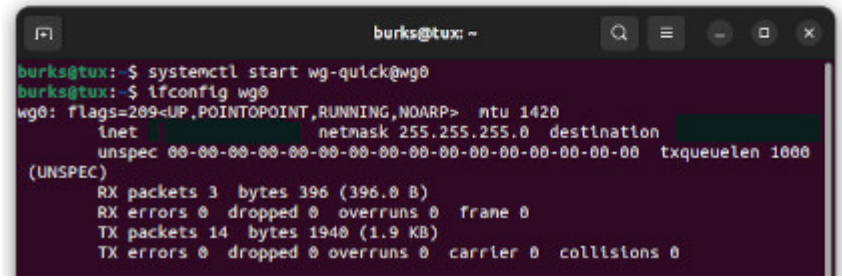
usw.)

Sehr geehrte Damen und Herren Nerds aka Thomas Niedermeier ! Manuals wie Ubuntu Desktop als WireGuard VPN Client konfigurieren lese ich nur, wenn mich eine attraktive nackte Frau dazu auffordert. Ich bin mir auch nicht sicher, ob ich das Thema verstanden habe: VPN *ohne* Fritzbox o.ä.? Wer tut sich so etwas an?

```
# systemctl start wg-quick@wg0
```

Nach erfolgter Einwahl gibt es ein neues Interface mit entsprechenden Routen:

```
# ifconfig wg0
wg0: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1420
        inet 10.10.10.201  netmask 255.255.255.255  destination 10.10.10.201
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 296 (296.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      0.0.0.0         255.255.254.0   U     0      0        0 wg0
```



So sieht das dann unter Jammy Jellyfish aus.

Auch Detailprobleme (Wie permanent einschalten? Wie ausschalten? Ist es überhaupt an?) kriegte ich nach einiger Zeit hingefummelt.

[x] Problem gelöst.

2. Mit WireGuard kann ich mich auch von nah und fern mit meiner Fritzbox verbinden. Wer hätte gedacht, dass das so einfach funktioniert! Was geschieht aber im Oktober?

Bei der Ausreise vom Flughafen Ben Gurion aus kann es zur Einbehaltung von elektronischen Geräten, insbesondere Laptops, durch die israelischen Sicherheitsbehörden kommen. In diesen

Fällen werden die Computer eingehend untersucht und dann nach ein bis drei Tagen an den Aufenthaltsort des Reisenden nachgesandt.

Hurra! Endlich eine „Online-Durchsuchung“! Das will ich sehen. Aber mein fettes Linux-Laptop nehme ich sowieso nicht mit… Und wenn sie meine Veracrypt-Container nicht aufkriegen, behalten sie den Rechner? Da entwickele ich sportlichen Ehrgeiz… ~~Aber ich hätte gar nichts zu verbergen.~~

Das technische Problem, sich zu entfesseln, wurde hier nur halbherzig gelöst. (Credits: Schockwellenreiter)

Unter Veracryptern und tugendhaften Klempnern

Wie das der Kryptografie kundige und des Verschlüsselns digitaler Dinge erfahrene Publikum schon bemerkte, kann man geschützte Speichermedien fünf Jahre lang untersuchen und doch nichts finden. Ich weiß, wovon ich rede. Das wird die üblichen Verdächtigen aber nicht daran hindern, wie gewohnt zu verfahren.

Ich will aber eure Herzen nicht vergiften wie Madame de Staël, die in ihrem Buch über Deutschland, das Napoleon höchstpersönlich ins Feuer warf, schrieb, dass die Deutschen zu wenig unabhängig seien und dass sie „durchaus nicht das haben, was man Charakter nennt. Sie sind tugendhaft und rechtschaffen, als Privatleute, als Familienväter, als Staatsbeamte; aber ihr gefälliger und zuvorkommender Diensteifer gegenüber der Macht verursacht ein schmerzliches Gefühl.“

Jetzt zu wichtigen und aktuellen Themen: Ich muss für den

Garten meiner Mutter einen neuen Wasserhahn besorgen, weil der alte tropft und vermutlich die halbe Hauswand einstürzt, wenn ich ihn versuche zu reparieren. Ich hatte bei der Großbourgeoisie schon einen gekauft (1/2 und 3/4 Zoll Anschluss), aber der passt nicht. Frage: Wo wird denn der Durchmesser festgestellt? Am Gewinde oder woanders? Wie ~~groß~~ dick muss er sein?

Ein Teller bunten Quatsch

Was gibt es so?

– Noch mehr Vereinsmeierei. Also noch mehr Schriftführer, Kassenwarte und Beisitzer, Ämter, um die sich Leute bewerben, die sonst nichts auf die Reihe kriegen. Braucht dieses Land nicht.

– Nein. Ich kann den Quatsch nicht mehr hören. Dann doch lieber irgendeinen russischen Propagandakanal.

~~– Warum bekommt die Ukraine keine Atomwaffen vom putinfreien Westen? Selenskij würde doch bestimmt vernünftig damit umgehen!~~

~~– Manche Leute sind so dumm, dass es sogar verschwendete Zeit wäre, versuchte man, deren gar nicht vorhandenen Argumente zu widerlegen. #deutschersatzbau~~

Wer hätte das gedacht! Gut, dass es Faktenchecker gibt! Die kriegen wirklich alles raus.

– Die Briten spielen mit dem Feuer. Doch halt! die Russen haben das schon gemerkt: „Laut BBC würden die ukrainischen Truppen nur drei dieser Kettenkampffahrzeuge erhalten. Wie britische Militärexperten bemerken, gibt es im Prinzip gar nicht sehr viele M270 im britischen Arsenal, die an Kiew geliefert werden könnten."

– Nein, ich bin auf jeden Fall *für* die Chatkontrolle. Das funktioniert wie bei der „Online-Durchsuchung": Wenn man fragt, wie das denn technisch umgesetzt werden soll, erntet man betretendes Schweigen. (Chat – was war das noch mal? IRC? Signal? Oder auf Suaheli in Second Life?) Vielleicht lernen dann einige Leute, wie man Kontrollen umgeht.

Erdbeer- und Rharbarbermarmelade – man gönnt sich ja sonst nichts.

Drive-by-Download oder: Die berittenen Griechen mal wieder

Tagesschau: „Das bekannteste Produkt von NSO ist „Pegasus“, ein Trojaner, mit dem unbemerkt iPhones und Android-Smartphones infiziert und mühelos Telefonate, SMS, E-Mails und

sogar verschlüsselte Chats überwacht werden können.“

Und jetzt alle im Chor: Und wie kommt das Pferd mit den Griechen auf die Geräte, ohne dass die Nutzer sich selten dämlich anstellen? Und noch mal der Refrain: Warum fragt die Journaille nicht nach? Zweiter Refrain: Haben Journalisten auch Linux?

Wir haben eine Anwort, sogar von Wikipedia: „…erhielt am 10. und 11. August 2016 jeweils eine SMS auf seinem iPhone 6 (iOS-Version 9.3.3), die auf neue Hinweise zu Menschenrechtsverletzungen aufmerksam machte und einen Link zu einer Webseite enthielt, die angeblich neue Geheimnisse enthülle. Der einzige Zweck dieser SMS war es, den Benutzer zum Anklicken des Links zu bewegen (Drive-by-Download).“

Wer klickt eigentlich auf Links, ohne die HTML dahinter zu prüfen? Ach – das machen alle? Warum?

Cyberdings oder: Unter Staatsgriechen et al

Mykonos Vase, 675 v.u.Z., Archäologisches Museum Mykonos, älteste bekannte Darstellung des Trojanischen Pferdes

Ich muss noch die Cybernachrichten der letzten Tage aufarbeiten. Ich habe das vor mir hergeschoben, weil ich wusste, das ich mich ärgern würde. So war es auch.

Die Zwangsfilter, die in Betriebssysteme eingebaut werden wollten, sind zugleich das Allerletzte und das Allerlustigste. Ich möchte gerne mal die Gesichter der Leute sehen, die sich so etwas ausdenken: Eine Mischung aus Claudia Roth, Saskia Esken und Philipp Amthor?

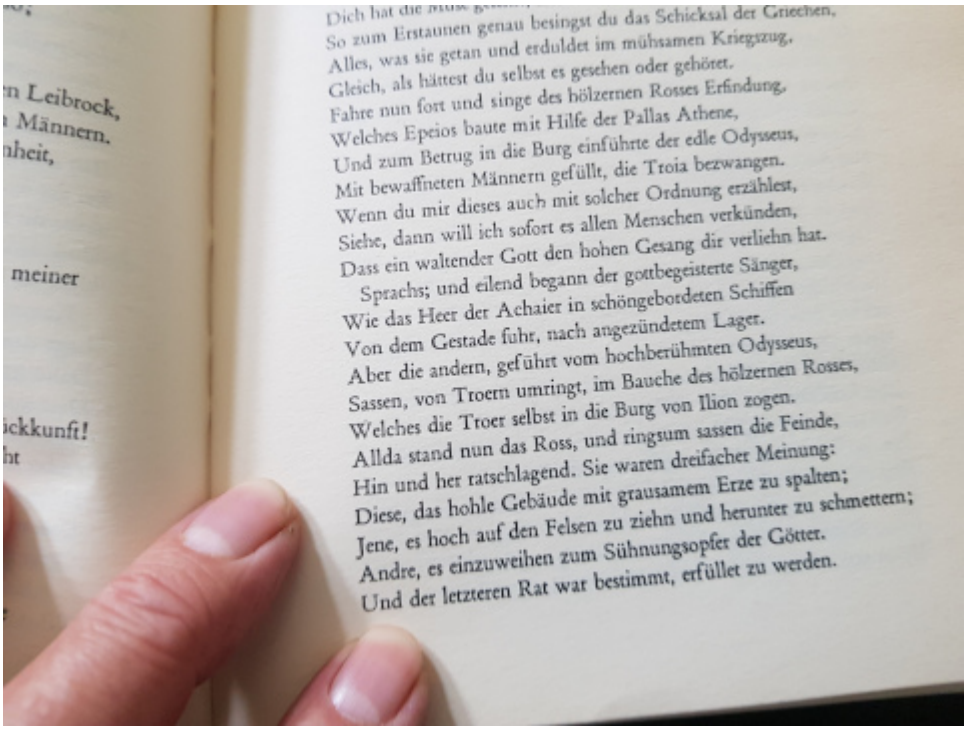
Dazu ein Kommentar bei Heise: *Ach, die drehen das so, dass freie Betriebssysteme ohne diesen Jugendschutzblödsinn plötzlich zu „terroristischem Werkzeug" umdeklariert werden. Der Bezug, Besitz und die Weitergabe werden dann pauschal als „Unterstützung einer Terrororganisation" eingetütet. +seufz+ … und Krieg ist Frieden.*

Dann haben wir noch die x-te Version vom Staatstrojaner. Manchmal möchte ich den Kollegen Krempl einfach nur ohrfeigen, wenn er zm 1000-sten Mal mit seinen schlampigen Begriffen Schlampiges daherschreibt. Und warum müssten Journalisten bürokratisches Neusprech wie „Quellen-TKÜ plus" übernehmen?

Das ist doch sowieso alles Unfug. Seit dem Erscheinen meines Buches hat mir immer noch niemand die Frage beantwortet, *wie* mir jemand ein Programm unterjubeln könnte, ohne dass ich mich vorher total bekloppt verhalten hätte? (FinSpy hatten wir hier schon.) Oder geht es gar nicht um meine Computer?

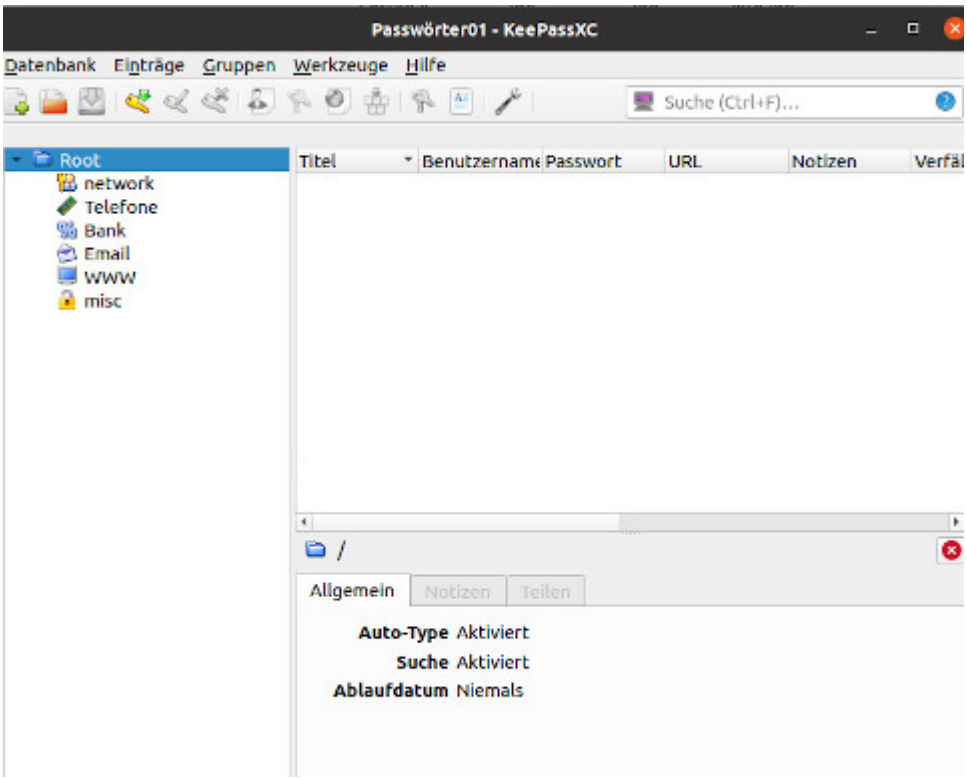
….sollte die Bundespolizei mithilfe des Bundestrojaners Messenger-Kommunikation etwa via WhatsApp, Signal oder Threema sowie Internet-Telefonate und Video-Calls… Gefasel und Bullshit-Bingo. Geht es nicht genauer? Mich regt noch mehr auf, dass die Journaille einfach nicht genauer nachfragt, sondern alles nachplappert. Netzsperren reloaded halt.

By the way: Ich hoffe nur, dass es keine Serienmörder oder andere Kriminelle gibt, die so wie ich heißen. Sonst müsste ich Google verklagen. Und ASCII ist jünger als ich. Ich weiß nicht, ob das gut oder schlecht ist.



Odyssee von Homer, übersetzt von Johann Heinrich Voss – obwohl das Pferd in den Gesängen der Osyssee gar nicht vorkommt, sondern in den Iliu persis.

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.

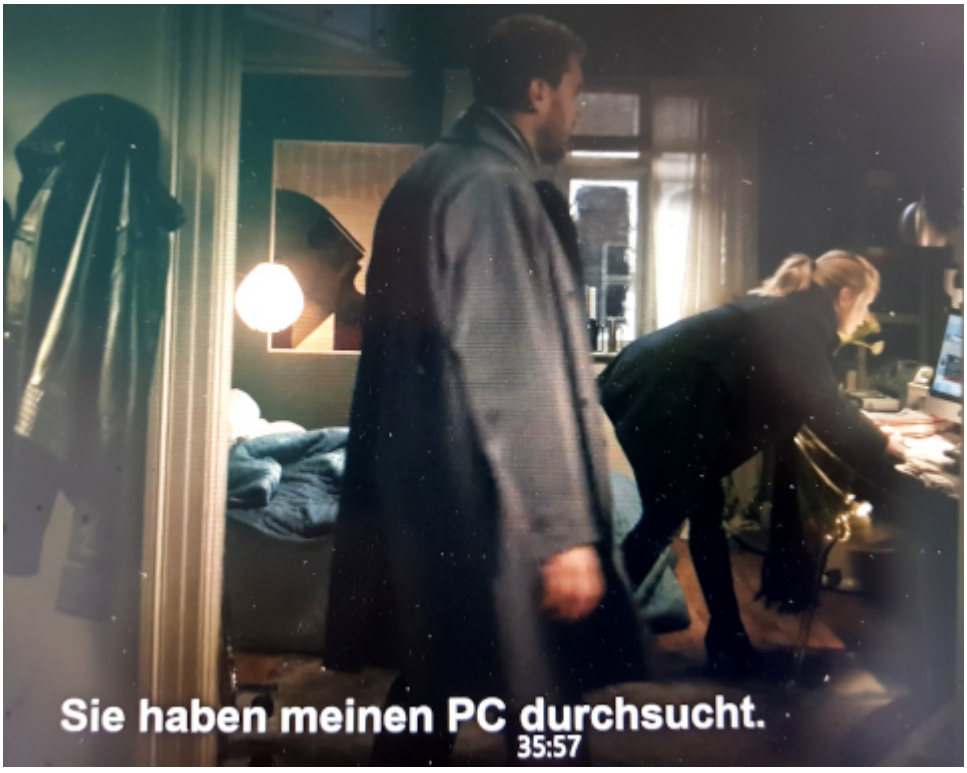
TKÜ, ick hör dir nicht trapsen

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



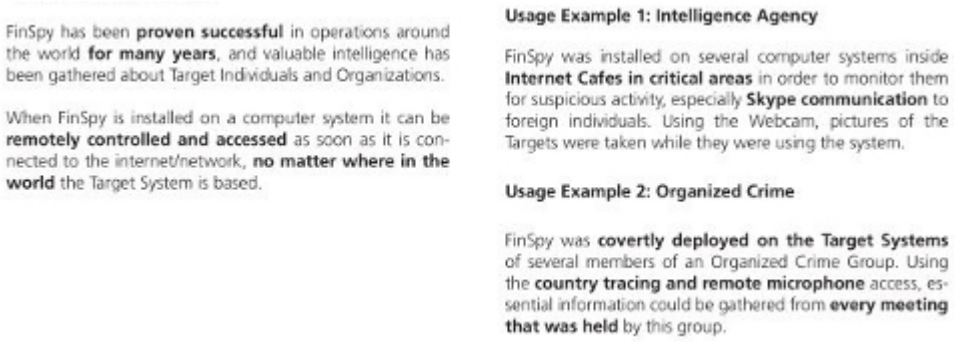
Screenshot aus Borgen, Staffel 1

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.

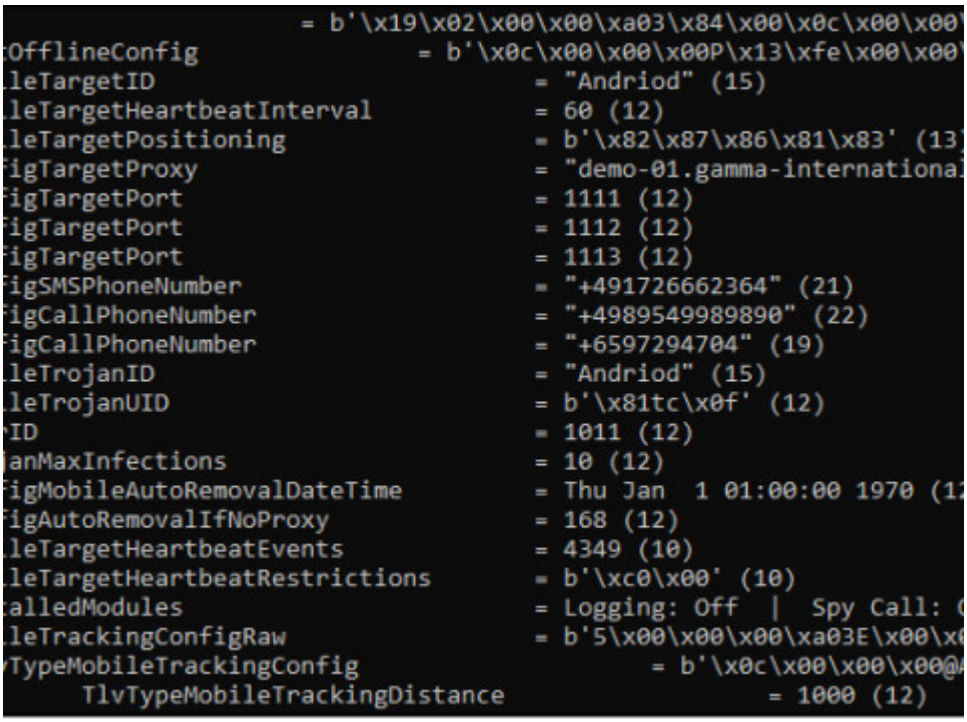
Hier ein Beispiel, die Fotos oben sind das Ergebnis: Das linke Bild ist das Original, im rechten Foto ist ein längeres Zitat aus dem Koran verborgen. Ich habe vorher nachgesehen, in welchen Passagen es um den Jihad geht.

```
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**."

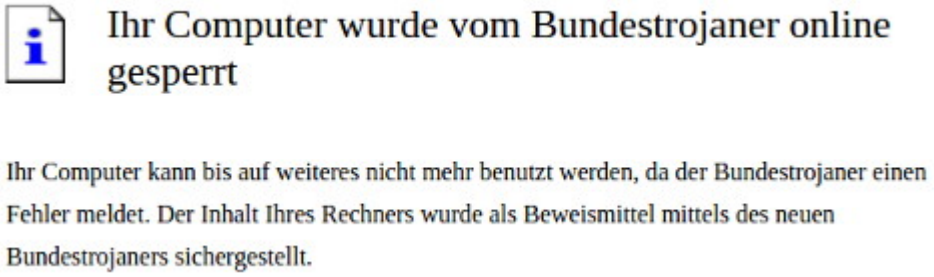
Genau das – und nur das! – habe ich immer behauptet, während fast alle Medienberichte entweder das Problem, wie die Spionage-Software zu installieren sei, vornehm ignorierten oder zu Magie – der Hacker hackt und ist irgendwann drin – greifen mussten.

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?