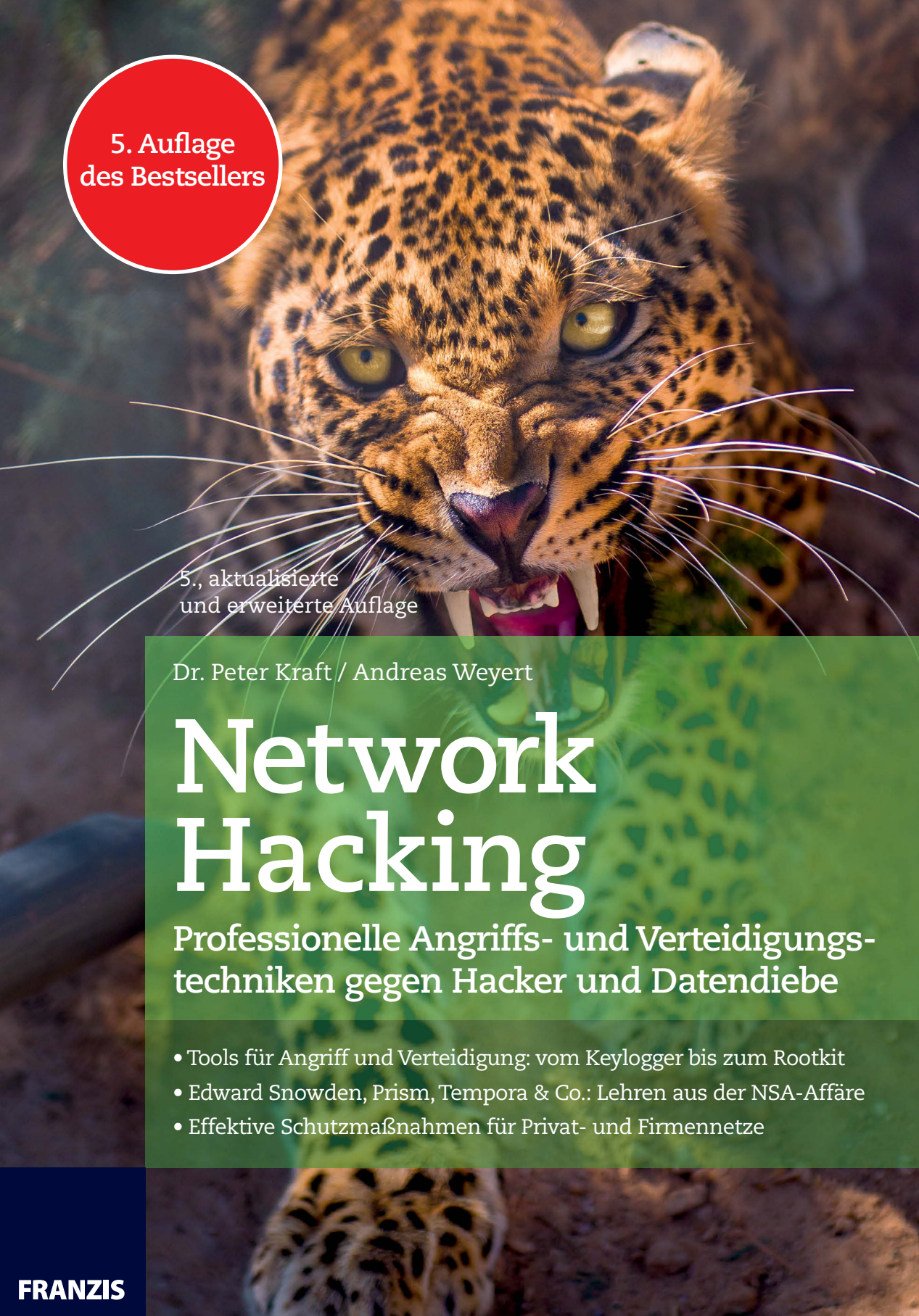


5. Auflage des Bestsellers

5., aktualisierte und erweiterte Auflage

Dr. Peter Kraft / Andreas Weyert

Network Hacking

Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe

- Tools für Angriff und Verteidigung: vom Keylogger bis zum Rootkit
- Edward Snowden, Prism, Tempora & Co.: Lehren aus der NSA-Affäre
- Effektive Schutzmaßnahmen für Privat- und Firmennetze

FRANZIS

Dr. Peter Kraft / Andreas Weyert

Network Hacking

Dr. Peter Kraft / Andreas Weyert

Network Hacking

Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe

- Tools für Angriff und Verteidigung: vom Keylogger bis zum Rootkit
- Edward Snowden, Prism, Tempora & Co.: Lehren aus der NSA-Affäre
- Effektive Schutzmaßnahmen für Privat- und Firmennetze

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de

ISBN 978-3-645-20531-3

Vorwort

Die 5. Neuauflage – initiiert, gefordert und gefördert von unserem Lektor Dr. Markus Stäuble vom Franzis Verlag, dem wir einmal mehr zu danken haben für Nachdrücklichkeit und Motivationskraft.

Was hat sich zwischenzeitlich geändert? Und auf welche Trends werden wir hier näher eingehen?

Zuerst einmal: Edward Snowden is still alive. Aus seinem Exil in Russland meldet er sich in mehr oder minder regelmäßigen Abständen mit Berichten zu aktuellen Bedrohungsszenarien. Er ist mittlerweile nominiert für den Friedensnobelpreis; »am 29. Oktober 2015 empfahl das *Europäische Parlament* den Mitgliedstaaten, alle Vorwürfe gegen Snowden fallen zu lassen und ihm als *Menschenrechtler* Schutz zu gewähren.«[1] Für die USA bzw. die US-Regierung gilt er nach wie vor als Krimineller, der, falls er gefasst würde, mit einer sehr langen Haftstrafe rechnen müsste. Im Herbst 2016 veröffentlichte Oliver Stone seinen neuen Film »Snowden« mit *Joseph Gordon-Levitt* in der Rolle des Edward Snowden. Was viele Sicherheitsexperten am meisten stört, ist aber nicht der Hype um Snowden, sondern die mehr als verhaltene Reaktion der Öffentlichkeit auf die unwiderlegbaren Beweise, auf breiter Front ausspioniert worden zu sein – ohne dedizierten Anlass.

In Deutschland steht die Vorratsdatenspeicherung wieder auf dem Tapet resp. im Gesetzblatt. Die TK-Anbieter werden zu Folgendem verpflichtet[2]:

- Standortdaten der Teilnehmer aller *Mobiltelefonate* bei Beginn des Telefonats für 4 Wochen zu speichern
- Standortdaten bei Beginn einer mobilen *Internet*nutzung für 4 Wochen zu speichern
- *Rufnummern*, Zeit und Dauer aller *Telefonate* für 10 Wochen zu speichern
- Rufnummern, Sende- und Empfangszeit aller *SMS-Nachrichten* für 10 Wochen zu speichern
- zugewiesene *IP-Adressen* aller Internetnutzer sowie die Zeit und Dauer der Internetnutzung für 10 Wochen zu speichern

2015 erschienen Meldungen, wonach die Bundesregierung plant, starke Verschlüsselung zu limitieren, z. B. durch eingebaute Hintertüren für Sicherheitsdienste. Eine Zusammenarbeit mit Frankreich ist angedacht[3]: »Paris und Berlin planen Aktionsplan gegen Verschlüsselung«. Das Bestreben, starke Verschlüsselung einzuschränken, wobei, anbei

---

1 *https://de.wikipedia.org/wiki/Edward_Snowden*

2 *https://de.wikipedia.org/wiki/Vorratsdatenspeicherung*

3 *http://www.golem.de/news/kampf-gegen-terrorismus-paris-und-berlin-planen-aktionsplan-gegen-verschluesselung-1608-122669.html*

bemerkt, Großbritannien schon ein Stückchen weiter ist – Stichwort »Schnüffel-Charta«. Der dritte Streich der deutschen Bundesregierung 2016 ist das geplante Verbot anonymer Prepaidkarten.[4]

Wenn man bedenkt, dass gerade deutsche Unternehmen (United Internet und Telekom) an vorderer Front geholfen haben, die Ende-zu-Ende-Verschlüsselung voranzubringen, muten die Bestrebungen, das Erreichte zurückzuschrauben, wie ein schlechter Scherz an. Ob man der Industrie damit einen Gefallen tut, darf tunlichst bezweifelt werden. Je stärker die Geschäftsprozesse digitalisiert werden (Industrie 4.0), desto wichtiger werden Sicherheitsaspekte, weil digitale Infrastrukturen auf Cyberkriminelle eine unwahrscheinliche Anziehungskraft ausüben. Werden hier pseudosichere Lösungen implementiert, wächst die Gefahr, von der »falschen Seite« ausspioniert und manipuliert zu werden, exponentiell. Einen denkenswerten Ansatz hat Roland Berger im Think Act Cyber-Security[5] formuliert.

Bild V.1: Bedrohungsszenarien Cyber Space

Manche Analysten nehmen an, dass 97% der Fortune-500-Unternehmen sich in der Vergangenheit mit Hackerangriffen und ihren Folgen auseinandersetzen mussten; die übrigen 3% wüssten nur noch nichts von ihrem Unglück[6]. Yahoo kann das wahrlich

4 *http://www.spiegel.de/netzwelt/netzpolitik/prepaid-sim-regierung-will-anonyme-handy-karten-verbieten-a-1087295.html*

5 Download hier: *https://www.rolandberger.com/publications/publication_pdf/roland_berger_tab_cyber_security_20150305.pdf*

6 THINK ACT CYBER-SECURITY S. 5

nicht sagen seit dem massiven Datenklau von mehr als einer Milliarde Yahoo-Konten[7] im August 2013 und Ende 2014 mit mindestens 500 Millionen betroffenen Anwendern[8]. Erste Klagen von Betroffenen sind seit Ende 2016 bei US-amerikanischen Gerichten anhängig. Dem Konzern wird insbesondere vorgeworfen, seine Daten unzulänglich geschützt zu haben. Verschlüsselungstechniken mit eingebauter Backdoor für die Dienste durchlöcherten diesen doch sehr notwendigen Schutz wie einen Schweizer Käse.

Neu hinzugekommen ist, dass die Europäische Kommission unzufrieden ist mit den Erläuterungen der US-Regierung zu der Enthüllung, Yahoo habe im Auftrag von US-Geheimdiensten alle E-Mails an Yahoo-Kunden zu scannen. Es bleibt also auch weiterhin spannend.

Natürlich sind auch kleinere, mittelständische Unternehmen und öffentliche Einrichtungen bedroht. Dieses Mal jedoch nicht durch staatliche (chinesische oder russische) Hacker wie – angeblich – bei Yahoo[9], sondern durch »gemeine« Cyberkrimelle, die ihr Produkt querbeet im Internet verteilen. Gemeint ist Ransomware, der beispielsweise Anfang des Jahres 2016 ein Krankenhaus in Neuss zum Opfer fiel. Angriffsvektoren sind in aller Regel infizierte Webseiten oder, wie im Neusser Fall, infizierte Dateianhänge. Einmal unfreiwillig gestartet, verschlüsselt der Erpresserschädling Office Dokumente, Bilder, Musik- Datenbankdateien. Es erscheint ein Sperrbildschirm, auf dem die Erpresser für die Entschlüsselung der Dateien ein Lösegeld (engl.=Ransom) fordern, zahlbar meistens in Bitcoins oder anonymen Zahlungsanweisungen. Zwischen 2014 und 2016 hat diese Art von Schädlingen den größten Zuwachs aller Schädlinge erzielt. Im Februar 2016 titelte Heise: »Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde«[10] Schuld an dieser relativ neuen Misere sind nicht nur schlecht gewartete Systeme, schwache Passworte, unglückliche Netzkonfigurationen und vor allem unvorsichtige, uninformierte Anwender sowohl im Privatbereich als auch bei Unternehmensmitarbeitern.

Es hat sich in den letzten beiden Jahren also durchaus einiges getan. Um die Erwartungshaltung unserer Leser gleich vorweg auf ein realistisches Niveau zu bewegen: NSA und GCHQ sind weiterhin mit ihren phantastisch wirkenden Überwachungsprogrammen aktiv und von ihren Regierungen unmaßgeblich eingebremst. Im Jahre 2014 kam heraus, dass der Dateneinbruch beim belgischen TK-Anbieter Belgacom auf Veranlassung von NSA und GCHQ erfolgte[11]. In Deutschland wurde im BKA-Gesetz zwar der Funktionsumfang des Staats- oder Bundestrojaners leicht kastriert: So sollen bei der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) »nur« Kommunikations-

---

7 *https://heise.de/-3570674*

8 *http://www.handelsblatt.com/unternehmen/it-medien/hacker-angriff-bei-yahoo-erste-klagen-nach-riesigem-datendiebstahl/14595290.html*

9 *https://heise.de/-3336946*

10 *http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html*

11 *https://netzpolitik.org/2014/regin-staatstrojaner-enttarnt-mit-denen-nsa-und-gchq-ziele-auch-in-europa-angriffen-haben*

daten (E-Mail, Chat und Videotelefonate) ausgespäht werden dürfen, nicht aber der komplette Festplatteninhalt des Verdächtigen.

Zwar haben wir uns aus gegebenem Anlass dazu entschlossen, einen eigenen Beitrag zur Abwehr des globalen Spionagewahns zu leisten, der durch NSA, GCHQ und andere Dienste befeuert wird, allerdings liegt unser Schwerpunkt auch weiterhin auf den »Klassikern« der Cyberkriminalität inklusive der Ransomware, dem »Entführen« von Datenbanken[12] (wie erst vor Kurzem mit MongoDB und Elastic Search geschehen) oder beispielsweise durch Online-Skimming kompromittierte Online-Shops[13].

Entscheidend war für uns die Frage, ob Anwender trotz der Novitäten auf dem Markt unser Buch auch weiterhin als Leitfaden benutzen können, um Netzwerkangriffe zu erkennen und abzuwehren.

Wir sind der festen Überzeugung, dass das nach wie vor der Fall ist. Zwar gibt es wie jedes Jahr neue Techniken, Tools und Angriffsszenarien, aber die Methodologie der Abwehr von Netzwerkattacken ändert sich nicht grundlegend.

Die letzten zwei Jahre, die seit der vierten Neuauflage von »Network Hacking« vergangen sind, waren ohnehin geprägt von einer ungeheuren Dynamik. So wird es niemanden überraschen, dass die Bedrohung durch Cyber-Gefahren unvermindert anhält und sich auch die Angriffslast auf weiterhin hohem Niveau bewegt.

Neu hinzugekommen, quasi als qualitative Herausforderung, sind Angriffe auf das »Internet der Dinge« durch beispielsweise ZigBee-Würmer[14]. Angriffe auf Produktionssysteme, die auf Lebenszeiten von 20 Jahren angelegt sind, stellen ganz neue Anforderungen[15] an das Patch-Management. Im selben Maß, wie unsere Alltagsdinge (PKW, Kühlschrank, Heizung, Strom) vernetzbar werden, kommen neue Bedrohungsszenarien bzw. neue Chancen für Kriminelle. Wer möchte schon gern in seiner Lieblingskarosse sitzen, wenn andere parallel die Finger an Lenkung, Gas und Bremse haben? Das Phänomen könnte man dann mit »heteronomem Fahren« übersetzen[16].

Für die Hersteller sind solche News natürlich eine Katastrophe. Das Problem liegt nicht an mangelhaft implementieren Sicherheitsmechanismen gegen Manipulation von außen, sondern an der Vernetzung selbst. Netzwerke und ihre Komponenten, wie Computer, sind immer angreifbar. Auch im Gesundheitssektor. Am 6. 10. 2016 titelte die FAZ auf Seite 17: »Wenn IT-Einbrecher lebenswichtige Medizingeräte entern«. Konkret betrifft die neue Sicherheitslücke vernetzte Insulinpumpen, die auch durch kein

---

12 *https://twitter.com/certbund/status/819893537059827714*

13 *https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Skimming_09012017.html*

14 *https://heise.de/-3459004*

15 *https://heise.de/-3463589*

16 Ein grundsätzlicher Beitrag zum Thema: *http://www.manager-magazin.de/unternehmen/autoindustrie/gefahrenquelle-autoelektronik-wie-hacker-autos-manipulieren-koennten-a-974528.html*. Oder etwas konkreter: »Hacker schalten bei Jeep per Funk die Bremsen ab« *https://www.welt.de/wirtschaft/webwelt/article144329858/Hacker-schalten-bei-Jeep-per-Funk-die-Bremsen-ab.html*

Softwareupdate wieder fit gemachen werden können. Wenn, was zugegebenermaßen nicht so wahrscheinlich ist, die Durchflusssteuerung über Funk manipuliert würde, sind Todesfälle, z. B. wegen einer Insulinüberdosierung, nicht ausgeschlossen.

Es ist zu verzeichnen, dass Cyberkriminelle verstärkt die Wirtschaft ins Visier nehmen, wobei mittelständische Unternehmen in besonderem Maße von Wirtschaftsspionage, Konkurrenzausspähung und auch von Erpressung betroffen sind.

Als dominierendes Motiv für Internetangriffe gelten nach wie vor finanzielle Beweggründe. Der verstärkte Einsatz von Ransomware spricht eine deutliche Sprache. Darüber hinaus haben auch Sabotage und der Versuch politischer Einflussnahme durch Hacktivismus im Motivspektrum der Täter deutlich an Gewicht gewonnen. Der Einsatz von Angriffswerkzeugen, die mittlerweile auch von nicht-professionell agierenden Akteuren verwendet werden, wird durch sinkende Beschaffungskosten und die zunehmende Industrialisierung der Cyberkriminalität leichter möglich.

Abseits der Masse von Standardangriffen auf IT-Systeme von Privatnutzern und Unternehmen ist eine gesteigerte Zielorientierung, eine weitere Professionalisierung der Angreifer und damit eine gesteigerte Qualität der Angriffe zu beobachten.

So kam es über die letzten Jahre erneut und verstärkt zu mehrstufigen Angriffen, die sich dem eigentlichen Ziel nur schrittweise näherten. In einigen Fällen wurden sogar eigens neue Schadprogramme mit speziellen Funktionen konstruiert – etwa zur Tarnung oder um nach dem Angriff Spuren zu verwischen. Insbesondere bei langfristig ausgelegten und von professionellen Tätern ausgeführten Cyberangriffen stellt dies mittlerweile die Regel dar und ist vergleichbar mit dem Repertoire von Geheimdiensten.

Das Bundesamt für Sicherheit in der Informationstechnik[17] (BSI) veröffentliche 2015 seinen Report »Die Lage der IT-Sicherheit in Deutschland«[18].

Interessant daran sind die Trends für 2015 / 2016. Wir greifen hier die wichtigsten heraus:

- **Ausnutzen von Softwareschwachstellen**
  Es ist bekannt, dass Cyberkriminelle und staatliche Stellen für Zero-Day-Exploits gut bezahlen.

17 *https://www.bsi.bund.de*

18 *www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html*

- Angriffe auf mobile Netz- & Infrastrukturen

Gefährdung	2014	2015
Cloud Computing		→
Software-Schwachstellen	→	↑
Hardware-Schwachstellen		→
Nutzerverhalten und Herstellerverantwortung		↑
Kryptografie		→
Internet-Protokolle		↑
Mobilkommunikation		↑
Sicherheit von Apps		↑
Sicherheit von Industriellen Steuerungsanlagen		↑
Schadsoftware	↑	↑
Social Engineering	↑	→
Gezielte Angriffe - APT	→	↑
Spam	↑	↑
Botnetze	→	↑
Distributed Denial-of-Service (DDoS)-Angriffe	→	→
Drive-by-Exploits und Exploit-Kits	→	↑
Identitätsdiebstahl	↑	↑

Legende
Gefährdung 2015 (niedrig, durchschnittlich, hoch) ↓ → ↑

Bild V.2: BSI-Report 2015

- **Angriffe auf industrielle Steuerungsanlagen**
  Beispielsweise im Zuge des Cyber Wars; grundsätzlich eine klassische Kontraindikation von Industrie 4.0[19].

- **APT-Angriffe**
  Die Advanced Persistent Threads (APT) sind gezielte Versuche, kritische IT-Strukturen gezielt und permanent zu kompromittieren.

---

[19] *https://www.vdi-wissensforum.de/weiterbildung-it-security/industrial-it-security/* oder auch hier: *http://www.heise.de/newsticker/meldung/31C3-Wie-man-ein-Chemiewerk-hackt-2507259.html*

- **Bot-Netze**
  Sie dienen unterschiedlichen Zwecken, angefangen mit der Funktion von Spam-Schleudern, Klick-Betrug bis hin zu konzentrierten Angriffen auf Webseiten (DDOS-Attacken). Quantitativ war 2016 ein leichter Rückgang zu beobachten, qualitativ haben die Bot-Netzbetreiber aufgerüstet und ihre Schlagkraft um das Vierfache gesteigert[20].
- **Drive-by-Exploits und Exploit-Kits**
  Sicherheitslücken auf den Opfer-PCs werden systematisch und gezielt ausgenutzt und entsprechende Schadsoftware häufig mittels entsprechender Browser-Plugins ausgeführt.

Damit sie mit diesen vielfältigen Bedrohungsszenarien besser umgehen können, zeigen wir – wie gewohnt – interessierten Laien wie auch IT-Praktikern, wie »böse Buben« in fremde Rechner und Netze eindringen – nicht um sie selbst zu »bösen Buben« zu machen, sondern um sie für zusätzliche Sicherheitsmaßnahmen zu sensibilisieren. Versierten Cyberkriminellen sagen wir mit diesem Buch nichts Neues, und die oft geschmähten Skriptkiddies mögen vielleicht an wenigen Stellen profitieren, finden im Internet aber erheblich brisantere Informationen als hier. Richtig profitieren werden aber alle, die motiviert sind, sich mehr und vor allem gezielter für die Sicherheit ihrer Rechner und Netze zu engagieren.

Der obligatorische Hinweis am Rande: Wir verwenden der Einfachheit halber den Begriff »Hacker« als Synonym für einen Computerkriminellen. Wir sind uns der Tatsache bewusst, dass der Begriff »Hacker« grundsätzlich wertneutral ist und dass es verschiedene Formen der Interpretation gibt (so beispielsweise bei Steven Levy[21] und Bruce Schneier[22]). Keineswegs möchten wir denjenigen zu nahe treten, die sich selbst als »Hacker« bezeichnen und beispielsweise als Kernel-Hacker in der Linux-Community mitwirken.

An der bewährten Struktur unseres Buchs halten wir fest. Das Tools-Kapitel wurde behutsam und teilweise auch nur exemplarisch »renoviert«. Wir hoffen, dass wir damit, wenigstens für die kommenden zwei Jahre, wieder auf der Höhe der Zeit sind.

Teil I – Hacking-Tools

Wir haben für dieses Buch die gewohnte dreiteilige Gliederung beibehalten. Im ersten Teil stellen wir gängige Hacking-Werkzeuge vor, wobei wir bewusst darauf verzichtet haben, zwischen Malware-Tools und klassischer bzw. kommerzieller Security-Software zu unterscheiden. Die vorgestellten Tools ermöglichen meistens beides: sowohl

---

20 *https://de.securelist.com/analysis/quartalsreport-malware/71340/kaspersky-ddos-intelligence-report-for-q1-2016*

21 *www.stevenlevy.com/index.php/other-books/hackers*

22 *www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html*

Angriffsvorbereitung und -durchführung als auch Erkennung bzw. Abwehr von Schwachstellen und Sicherheitslücken. Die »Tools-Sektion« hat darüber hinaus durch die gewählte Systematik den Charakter eines Nachschlagewerks. Durch die Beschreibung des Anwendungszwecks und die Ergänzung mit Bezugshinweisen, Kosten und Installationshinweisen kann jeder abschätzen, wie nützlich und brauchbar das eine oder andere Werkzeug für seine Zwecke sein mag. Vollständigkeit haben wir bewusst nicht angestrebt. Dennoch glauben wir, damit einen guten Querschnitt über die gängigsten Tools der Cyberkriminellen und die ihrer Gegenspieler bieten zu können.

Teil II – Angriff und Abwehr

Der zweite Teil unseres Buchs ist der kreativste. Hier beschreiben wir im Detail, wie typische Angriffsszenarien aussehen können. Angriffsobjekte sind Rechner mit einer Netzwerkanbindung, im einfachsten Fall ein kleineres Heimnetzwerk. Wir zeigen natürlich auch, wie Firmennetzwerke und Internetpräsenzen mit den eingangs vorgestellten Tools penetriert werden können. Die Szenarien sind so gewählt, dass sie auch von Nichtprofis praktisch nachvollzogen werden können. Allerdings sollte man als Leser ein Grundverständnis für die Netzwerk-Basics mitbringen. Wem beispielsweise die Unterschiede zwischen TCP/IP, UDP oder SSH, HTTP, FTP etc. nicht recht geläufig sind, der wird hier eine grundlegende Erläuterung vermissen und sollte sich an anderer Stelle noch ein wenig einlesen.

Hier beschäftigen wir uns auch nicht damit, wie man Exploits, Trojaner oder Rootkits entwickelt – wir zeigen, wie sie funktionieren und wie man sie in bestimmten Situationen anwendet. An dieser Stelle auch die obligatorische Warnung: **Sie als Leser sind auf jeden Fall für die Folgen Ihres Tuns selbst verantwortlich.** Wer ein Netzwerk erkundet, das nicht sein eigenes ist, bewegt sich in einer rechtlichen Grauzone. Wer sich durch einen Passwortcrack ein Log-in auf einem fremden Rechner erschleicht, eine bestehende Schwäche ausnutzt, um dort eine Remote-Shell zu etablieren, oder anderen Usern einen getarnten Keylogger schickt, ist definitiv auf der anderen Seite und kollidiert mit dem Strafgesetzbuch. Alle Angriffsszenarien enden übrigens mit einem Abschnitt, der sich der Abwehr genau dieser zuvor beschriebenen spezifischen Angriffstechnik widmet. Dies soll noch einmal klar belegen, dass wir kein Hackertraining anbieten, sondern für Hackangriffe und ihre Abwehr sensibilisieren wollen.

Teil III – Vorsorge

Im dritten Teil geht es um das grundsätzliche Thema der Prävention und Prophylaxe. Proaktives Sicherheitsmanagement ist ein Thema sowohl für den Betreiber privater Netze als auch für den Verantwortlichen kleinerer und mittlerer Firmennetze.

Inhaltsverzeichnis

1 Snowden, NSA & Co.

Man mag sich streiten, ob der Terroranschlag vom 11. September tatsächlich eine Zäsur in der US-amerikanischen Außen- und Innenpolitik markiert oder nicht. Was man aber ohne Zweifel nachzeichnen kann, sind gravierende Einschränkungen der Bürgerrechte im Versuch, asymmetrisch Bedrohungsszenarien (Terroranschläge, Selbstmordattentäter sowie deren Finanziers) einzudämmen. Hinzu kommen die Kollateralschäden im von George W. Bush ausgerufenen »Krieg gegen den Terror«, die vermutlich ein Vielfaches der bei dem Terroranschlag vom 11. September getöteten knapp 3.000 Opfer ausmachten.

Am 26. Oktober 2001 wurden im Rahmen des Patriot Act weitreichende Einschränkungen der Bürgerrechte juristisch verankert: Verdächtigte Personen dürfen auch ohne richterliche Anordnung überwacht, ausgespäht, abgehört und auf Monate hinaus ohne Anklage festgehalten werden. Neben dem Ministerium für Heimatsicherheit (ein Euphemismus Orwell'schen Ausmaßes) mit 170.000 Beschäftigten wurden 263 Sicherheitsbehörden neu gegründet bzw. reorganisiert.[23] Zeitgleich wuchsen auch die Budgets für die zahlreichen Inlands- und Auslandsdienste kräftig. Laut Whistleblower Edward Snowden[24] geht das meiste Geld an die CIA (14,7 Mrd. US-Dollar), gefolgt von der NSA (10,8 Mrd. US-Dollar) und dem Militärnachrichtendienst National Reconnaissance Office (NRO) mit 10,3 Mrd. US-Dollar Budget.

Wofür das Geld verwendet wurde, das ist, wenigstens was die NSA betrifft, dank Snowden jetzt in gewissen Bereichen transparent geworden. Die Big Player des globalen Abhörwahns heißen *Prism*, *Tempora* und *XKeyScore*. Sofern die Zielperson mit mehr als 51 % Wahrscheinlichkeit Ausländer ist, kann sie via Prism umfassend ausspioniert werden, wie Snowden im Detail berichtete: Danach könne deren Kommunikation »direkt von den Servern« der US-Anbieter Microsoft, Google, Yahoo!, Facebook, Paltalk, YouTube, Skype, AOL und Apple mitgeschnitten werden. Zugreifen könne der einzelne Analyst auf E-Mails, Chats (auch Video- und Audioübertragungen), Videos, Fotos, gespeicherte Daten, VoIP-Kommunikation, Datenübertragungen und Videokonferenzen. Außerdem erhalte er Daten über die Accounts in sozialen Netzwerken und könne benachrichtigt werden, wenn sich die Zielperson einlogge.[25] Vereinfacht ausgedrückt: Der gläserne Bürger ist das Endresultat des amerikanischen (und englischen) Datensammelns – unabhängig davon, wo sich sein Lebensmittelpunkt befindet. Da hier nicht nur politische,

---

23 Quelle: »Terroranschläge am 11. September 2001« – Wikipedia

24 *www.heise.de/newsticker/meldung/NSA-Affaere-Schwarzes-Budget-der-US-Geheimdienste-enthuellt-1945661.html*

25 *www.heise.de/newsticker/meldung/NSA-Ueberwachungsskandal-PRISM-Tempora-und-Co-was-bisher-geschah-1909702.html*

sondern auch wirtschaftliche Interessen mit dem Ausspähwahn eine unheilige Koalition eingehen, sind die Kollateralschäden für die Gesellschaft als Ganzes nicht unbeträchtlich:

- Die moralische Überlegenheit des Westens (so sie überhaupt jemals in Reinkultur vorhanden war) gegenüber totalitären Regimes wird löchrig. Chinesische, russische und amerikanische Dienste haben mehr gemeinsam, als es bislang schien, nämlich den Generalverdacht gegenüber jedem.
- Sicherheit wird als »Supergrundrecht« (Hans-Peter Friedrich, Bundesinnenminister a. D.) postuliert[26], um dreist alle relevanten Daten eines jeden »abschöpfen« zu können. Die Unschuldsvermutung weicht dem permanenten Verdacht.
- Big Data als Big Business: Global abfischbare Daten – unabhängig von Freund-Feind-Überlegungen – werden verstaatlicht und nach Wohlwollen und politischen Opportunitätsgesichtspunkten neu verteilt.
- Das klassische Missbrauchspotenzial wächst. Vielleicht ist die Lücke, die Snowden erlaubt hat, Teile der staatlich organisierten Paranoia dingfest zu machen, nur die Spitze des Eisbergs. Wenn die NSA es nicht einmal geschafft hat, ihr Tafelsilber vor unberechtigtem Zugriff zu schützen, wer glaubt dann noch ernsthaft, dass die gesammelten Daten von Max Müller und Lieschen Lotter missbrauchssicher auf den Serverfarmen der NSA bzw. ausgelagerter Partnerunternehmen liegen?

Peu à peu sickern mehr und mehr Informationen durch. So ist die NSA in der Lage, so gut wie alle Handys weltweit abzuhören – nicht nur das von Angela Merkel. Seit die rund 30 Jahre alte Verschlüsselung des Mobilfunkstandards GSM geknackt wurde, können alle Handys prinzipiell ohne großen Aufwand abgehört werden. Aus diesem Grund kündigte die Telekom an, ihr ursprüngliches Verschlüsselungssystem A5/1 rasch auf die als sicherer eingeschätzte Variante A5/3 umzustellen. »Im November 2013 wurde bekannt, dass die NSA weltweit 50.000 Computernetzwerke mit Schadsoftware infiltriert hat und sich das Ziel gesetzt hat, bis Ende 2013 Zugriff auf 85.000 Systeme zu haben.«[27] Selbst Amateure können unsere mobile Kommunikation belauschen. »Mit Technik von gerade einmal rund 1.500 Euro und OpenBTS, einer Open-Source-Software, kann man fremde Handys abhören.«[28]

Zwischenzeitlich[29] sind weitere Details bekannt geworden. Von 2001 bis 2015 wurden von der NSA die Verbindungsdaten (Telefon, E-Mail) aller US-Bürger ausgespäht. Weltbank, Opec, IWF, etliche europäische Botschaften, Amnesty International sowie Human Rights Watch waren ebenfalls betroffen. Flankenschutz für weitere Ziele erhielt die NSA vom BND – Stichwort Selektorenliste.

---

26 *http://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html*

27 *http://de.wikipedia.org/wiki/%C3%9Cberwachungs-_und_Spionageaff%C3%A4re_2013*

28 *www.mobiflip.de/abhoertechnik-fuer-handys-jetzt-beim-discounter/1347658450000*

29 *http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal*

»Selektorenliste« klingt erst einmal recht harmlos. Ist es aber nicht. Selektoren sind Merkmale wie E-Mailadressen, Mobilfunknummern, Schlüsselwörter, MAC- und IP-Adressen etc., mit denen das Netz nach relevanten Informationen – aus Sicht der Geheimdienste – durchsucht werden soll. Die besagte »Selektorenliste« hat der BND jahrelang für die NSA »abgearbeitet«. Für öffentliche Unruhe in Deutschland sorgte der Verdacht, dass auf der Selektorenliste auch Ziele in Deutschland und Europa aufgeführt waren. Gegen diese »Geheimniskrämerei« hatte die G10-Kommission des Bundestags in Karlsruhe geklagt. Die Klage wurde am 14.10.2016 vom Bundesverfassungsgericht aus formalen Gründen abgewiesen[30].

Die NSA hat natürlich auch seine östlichen Verbündeten gehackt, z. B. die israelischen Drohnen, um frühzeitig über mögliche Präventivschläge gegen den Iran informiert zu sein[31].

Mit der Aufarbeitung der Spähaffäre tat und tut sich Deutschland schwer. Zwar wurde am 20. März 2014 vom Bundestag ein Untersuchungsausschuss eingesetzt, aber die Ergebnisse bleiben mager. So recherchierte der Verfassungsschutz gut zwei Jahre lang, ob die NSA in Deutschland direkt spionierte – mit dem Ergebnis, dass er zu keiner abschließenden Beurteilung kommen konnte oder wollte. »Es haben sich keine Beweise im eigentlichen Sinne ergeben«, sagte Frank Wingerath, Referatsgruppenleiter beim Verfassungsschutz im Bundestag[32]. Wer's glaubt, möge selig werden.

Guten Gewissens hat der Verfassungsschutz auch Handydaten deutscher Bürger an die NSA weitergereicht im naiven Glauben, dass diese Daten nicht zur Geolocation verwendet werden können. »Geolocation« klingt harmlos, kann jedoch den sicheren Tod bedeuten, den z. B. zwei deutsche Staatsbürger am 4.10.2010 in Pakistan erlitten. Es gilt als zweifelsfrei erwiesen, dass eine Hellfire-Rakete mittels IMSI-Catcher (genannt »Gilgamesch«) ein Mobiltelefon mitsamt IMEI und IMSI orten und es samt Benutzer zerstören kann[33].

Vom »Erfüllungsgehilfen zum Selbstüberwacher« wird die Bundesregierung mit ihrem Antiterror-Paket[34]. Darin wird nicht nur die Zusammenarbeit mit fremden Diensten »verbessert«, sondern auch die lückenlose Überwachung auf deutschem Boden vorbereitet. Da passt es ins Bild, wenn der Verfassungsschutz das mächtigste Werkzeug der Massenüberwachsungsprogramme seit Orwell – Xkeyscore – seit über drei Jahren testet, obwohl der Inlandsgeheimdienst laut Gesetz nur Einzelpersonen überwachen darf[35].

Natürlich regt sich auch Widerstand gegen die Sammelwut unserer Dienste. Der größte Internetknoten der Welt, De-CIX in Frankfurt, war seit 2008 im Fadenkreuz des BND

---

30 *http://www.heise.de/newsticker/meldung/G10-Kommission-scheitert-mit-Klage-im-Selektoren-Streit-3350362.html*

31 *https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/*

32 *http://www.zeit.de/politik/deutschland/2016-05/verfassungsschutz-snowden-merkelphone-nsa-nsaua*

33 *http://www.zeit.de/digital/mobil/2016-09/hellfire-drohnen-verfassungsschutz-nsa*

34 Als Download hier: *https://netzpolitik.org//wp-upload/2016/06/2016-05-30_BMI-Anti-Terror-Gesetz-Entwurf.pdf*

35 *http://www.zeit.de/digital/datenschutz/2016-02/verfassungsschutz-bfv-nsa-xkeyscore*

und indirekt auch der NSA. »Im Jahr 2014 wurde bekannt, dass der BND am De-CIX in Frankfurt Daten absaugte, durchsuchte und die Ergebnisse der Suche mit dem amerikanischen Geheimdienst NSA teilte. Eikonal lautete der interne Tarnname des Projekts, das international für Aufregung sorgte«[36]. Die Betreiber des Netzknotens haben 2016 Klage gegen dieses behördlicherseits verordnete Ausspähen angestrengt. »Sollten die Betreiber des De-CIX gewinnen, müssten Überwachungsnormen wie das sogenannte *G10-Gesetz* oder das *Gesetz über den Bundesnachrichtendienst* wohl völlig neu verhandelt werden«[37].

Dass man das Ausspionieren und die massenhafte Verletzung der Privatsphäre noch steigern kann, zeigt das Vorgehen der Polizei in den USA. Wie am 19.10.2016 bekannt wurde, haben Ordnungskräfte dort 117 Millionen Führerscheine gescannt mit dem Ziel, die Gesichtserkennung im öffentlichen Raum zu intensivieren[38].

Berücksichtigt man jetzt die Tatsache, dass nicht nur Nachrichtendienste und Cyberkriminelle die allgemeine Kommunikation abhören, sondern auch kommerzielle Anbieter (z. B. Google, Facebook & Amazon) fleißig unsere Daten sammeln und uns gläsern machen wollen, stellt sich die Frage, inwieweit man dem entkommen kann.

1.1 Kryptohandys und andere Tarnkappen

Oft höre ich von Bekannten die Frage: Kann man mit seinem Smartphone anonym und »spionagefrei« unterwegs sein? Grundsätzlich muss diese Frage verneint werden. Eine (abhör)sichere Kommunikation ist nur mit echten Kryptohandys möglich. Und diese waren in der Vergangenheit nicht nur teuer (ca. 1.700 bis 2.500 Euro), sondern auch ausgesprochen unkomfortabel – außerdem setzen sie beim Gegenüber ein passendes Gegenstück voraus. Selbst dann fallen zwingend Verbindungsdaten an, die oftmals mehr Aussagekraft haben als das gesprochene Wort an sich.

In den letzten beiden Jahren hat sich aber einiges getan. Leider schon nicht mehr lieferbar ist der knapp 300 € teure Sprachcodierer[39] oder Handy-Scrambler, ein externes Zusatzgerät, das die Telefonate verschlüsselt. Für die Verschlüsselung ist ein MDP2-ASIC-Chip zuständig, der Sprache in Rauschen umwandelt, das auf der anderen Seite (dort ist ebenfalls ein Scrambler nötig) in Sprache zurückverwandelt wird. Scrambler an sich ist ein alter Hut: seine Technologie basiert auf linear rückgekoppelten Schieberegistern, ein Verfahren, das heute höchstens einen Amateurdetektiv vom Lauschen abhält.

---

36 *http://www.zeit.de/digital/datenschutz/2016-09/ueberwachung-bnd-nsa-decix-klage?sort=desc#comments*

37 ebenda

38 *http://thehackernews.com/2016/10/police-face-recognition.html*

39 *http://www.shop-alarm.de/Abhoersicheres_Handy.html*

Nützlicher und auch sicherer ist das 2014 erschienene und heute in Version 2 vorliegende Blackphone, eine Gemeinschaftsarbeit von Silent Circle und (nur für die Version 1) Geeksphone. Die eingesetzte Hardware entspricht erst mit Version 2 einem Oberklassehandy und kostet so viel wie ein Apple 6S. Bei Version 1 wurden etliche gravierende Sicherheitslücken, z. B. im Modul Secure-Text, entdeckt, sodass ein Angreifer nicht nur vertrauliche Texte ausspähen, sondern auch gleich das gesamte Handy übernehmen konnte[40].

Bei der zweiten Generation (jetzt ohne Geeksphone) sind die Lücken geschlossen. Man kann mit AES-128 verschlüsselte Texte verschicken, über einen VPN anonym surfen sowie verschlüsselt telefonieren. Neben einer speziell angepassten Hardware wird ein unter Sicherheitsaspekten angepasstes Android-Betriebssystem (PrivatOS) verwendet. Dieses gestattet es, jeder App spezielle Rechte zuzuweisen bzw. zu entziehen, was man ansonsten nur mit einem gerouteten Smartphone machen kann.

Wie soll man nun das Blackphone 2 unter Sicherheitsaspekten beurteilen? Der Algorithmus AES-128 darf wohl noch als sicher gelten – auch wenn z. B. in den USA die Anwendung von AES-192 und AES-256 für die Verschlüsselung von hochvertraulichen Dokumenten gefordert wird[41]. Die größeren Gefahren resultieren zumeist aus der Implementierung dieses Algorithmus. Wie es scheint, sind die größten Schwachstellen wohl behoben. Außerdem versichert der Hersteller, jede bekannt gewordene Sicherheitslücke innerhalb von 72 Stunden zu fixen.

Preislich günstiger (und mit geringen Sicherheitsabschlägen) kann man seiner Privatsphäre mit diversen Sicherheits-Apps wie *RedPhone oder Signal* auf die Sprünge helfen. Sie verschlüsseln Telefonate von Android-Handy zu Android-Handy via Voice-Over-IP. Vom selben Anbieter kommen auch professionelle Tools wie *WhisperCore* und *WhisperFirewall*, die das System verschlüsseln und gegen den Zugriff Unbefugter absichern (*https://whispersystems.org*). Selbst verschlüsseltes Chatten ist möglich, z. B. mit *Pidgin* (*http://www.pidgin.im*) durch die Einbindung von OTR. *Silent Circle* von Phil Zimmermann (*https://silentcircle.com/?lang=de*) ist ein ähnliches Produkt.

Seit 2016 bietet der beliebteste Messanger WhatsApp die schon seit langem geforderte Ende-zu-Ende-Verschlüsselung an. Nachrichten, Anhänge und Gruppenchats werden so verschlüsselt, dass die kommunizierenden Personen Klartext reden können, die Betreiber der App aber davon nichts mitbekommen – vorausgesetzt, sie ändern nicht unter der Hand die Funktionsweise der App. Da der Quelltext nicht offen gelegt wurde, muss man den Betreibern glauben, dass sie es mit unserer Privatsphäre ernst meinen. 2016 hat Heise die neue App getestet und als echten Gewinn in Sachen Privatsphäre bewertet[42] – sofern »Mr. WhatsApp« keine Hintertüren eingebaut haben sollte.

---

40 *http://www.heise.de/newsticker/meldung/Gravierende-Sicherheitsluecke-im-Blackphone-geschlossen-2530612.html*

41 Was ggf. aber auch wieder kontraproduktiv sein könnte: vgl. *https://de.wikipedia.org/wiki/Advanced_Encryption_Standard#Weitere_Angriffe*

42 *https://www.heise.de/security/artikel/Test-Hinter-den-Kulissen-der-WhatsApp-Verschluesselung-3165567.html*

Mit einem Missverständnis muss man allerdings aufräumen: Zwar ist der kommunizierte Inhalt sicher (verschlüsselt), nicht aber, was viele so noch nicht gesehen haben, die Metadaten – also z. B. wer mit wem wie lange getextet hat. Daran sind die Geheimdienste natürlich sehr interessiert und hier werden sie auch bei WhatsApp und iMessage (Apple) prinzipiell gut bedient. Unter Sicherheitsaspekten ist der Signal Messenger daher wesentlich besser geeignet, da er nur ein Minimum von Metadaten speichert[43].

Ansonsten gilt natürlich, dass registrierte Smartphones im Hinblick auf Verbindungs- und Lokalisierungsdaten generell unsicher sind obwohl man z. B. mit WhisperMonitor[44] das Smartphone am »Ausposaunen« seiner GPS-Daten hindern kann. Via digitaler Schleppnetzfahndung geraten auch unbescholtene Bürger ins Visier der Fahnder, wenn sie sich in der Nähe von Verdachtspersonen aufhalten. Die Dresdener Polizei »hatte kurzerhand alle Handybesitzer zu Verdächtigen erklärt, die während einer Demonstration gegen einen Naziaufmarsch innerhalb einer bestimmten Mobilfunkzelle in der Dresdener Innenstadt telefoniert hatten«[45].

Der Hintergrund für die verwendete Technik ist simpel genug: Mittels der Provider-/Rechnungsdaten lassen sich Funkzellendaten feststellen, über die dann auch eine Zielwahlsuche möglich ist. Die einzige Chance, die man hat – sofern das Handy nicht verwanzt ist –, besteht darin, ein nicht rückverfolgbares Prepaidhandy zu benutzen. Man besorgt sich anonym ein Zweithandy und eine Prepaidkarte. Alternativ kann man auch auf eBay oder bei einem der Kleinanzeigenanbieter für wenig Geld eine gebrauchte bzw. vorregistrierte Prepaidkarte anonym, bei Abholung, kaufen. Was man jedoch keinesfalls tun sollte, ist, sein »normales« Handy parallel zum (noch) anonymen Prepaidhandy eingeschaltet zu lassen. Eine Analyse der Funkzellendaten würde die Identität des Besitzers der Prepaidkarte leicht aufdecken. Es versteht sich auch von selbst, dass man kein schon registriertes Smartphone (IMEI) mit einer anonymen Prepaidkarte bestücken noch die Aufladung der Simkarte unbar erledigen sollte. Wie wir eingangs schon erläutert haben, wird es in Deutschland immer schwieriger, eine anonyme Prepaidkarte zu kaufen. Der Gesetzgeber räumt den Verkäufern von Prepaidkarten eine Übergangsfrist von einem Jahr ein (bis Mitte 2017), um sicherzustellen, dass Prepaidkarten nur an Käufer mit gültigem Personalausweis (der vorgelegt werden muss) verkauft werden. Die Provider waren schon davor gehalten, sich die Ausweise vorlegen zu lassen. Wer also auf eine anonyme und neue Prepaidkarte wert legt, möge sich z. B. mal bei den Discountern, z. B. Rossmann kundig machen, ob man die dort gekaufte Prepaidkarte auch übers Netz freischalten kann.

Noch einmal zur Erinnerung: Vom Prinzip her arbeitet jedes Smartphone permanent als »Wanze«. Tausende von Apps sammeln die Daten ihrer Kunden und verschicken Bewegungs- und Browserprofile, Telefonstatus sowie Adressdaten zu professionellen

---

43 *http://thehackernews.com/2016/10/signal-messenger-fbi-subpoena.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1337.nm0ao08cjo.s7m*

44 *https://www.heise.de/download/product/redphone-ehemals-whispercore-80293*

45 *www.welt.de/wirtschaft/webwelt/article13593670/Wie-der-Staatsanwalt-an-Handydaten-kommt.html*

Datensammlern. Die Möglichkeiten, dem zu entgehen, sind gering, denn sie konterkarieren den Nutzen, den man sich mit dem Erwerb eines Smartphones erhofft. Natürlich kann man das Mobilteil ausschalten und den Akku herausnehmen (sofern er sich überhaupt herausnehmen lässt). Die harmlosere Variante: Man schaltet das Smartphone in den Flugmodus. Jetzt wird jede Lokalisierung unterbunden; das Handy kann sich nicht mehr in einer Funkzelle einbuchen, und auch das Home-Phoning ist nicht mehr möglich. Aber wozu braucht man dann noch ein Smartphone?

Wer also seine digitalen Gewohnheiten nicht völlig verändern will, wird zu Kompromissen genötigt sein, z. B. durch den gezielten Einsatz eines (anonymen, auch anonym bezahlten) Prepaidhandys und den umsichtigen Gebrauch eines normalen Smartphones, das allerdings durch etliche Sicherheits-Apps[46] aufgepeppt werden sollte. Dazu gehören auch Überwachungstools (guter Überblick auf *www.netzwelt.de/news/89033_2-handy-kontrolle-so-ueberwachen-datentraffic.html#Daten-Apps*), mit denen man kontrollieren kann, was im eigenen Handy datenmäßig im Hintergrund passiert.

Empfehlen können wir für Android-Handys ebenfalls die kostenlose Appguard (*www.srt-appguard.com/de*), mit deren Hilfe Anwender andere installierte Apps daran hindern können, Standort- und Adressdaten ins Netz zu funken bzw. die eingebaute Kamera zu benutzen, um Bilder zu versenden. Die App deinstalliert die zu überwachenden Programme, installiert sie neu und beschränkt dann gezielt ihre Berechtigungen. Einschränkend gilt aber, dass nicht deinstallierbare System-Apps auch nicht gefiltert werden (und also durchaus hinter dem Rücken der Anwender kritische Daten ins Netz senden können.

Eine andere Angriffs- und Ausspähtechnik bietet ein IMSI-Catcher. Kurz gesagt, erlaubt er Strafverfolgern wie Nachrichtendiensten das Mithören / Mitschneiden der gesamten Mobilfunkkommunikation im Erfassungsbereich des IMSI-Catchers. Er arbeitet quasi als Vermittler (man in the middle) zwischen Basisstation und Mobiltelefon. Dabei buchen sich alle Mobiltelefone, nicht nur das des Verdächtigen, im Umkreis des IMSI-Catchers ein und können damit abgehört werden. Im schlimmsten Fall blockiert der IMSI-Catcher den gesamten Mobilfunkverkehr der betroffenen Handys und Smartphones, sodass auch keine Notrufe mehr möglich sind[47]. Es gibt unterschiedliche Hersteller und unterschiedliche Angriffstechniken, selbst IMSI-Catcher-Catcher sind in Entwicklung[48]. In dieselbe Richtung zielt die Entwicklung einschlägiger Apps für Android-Handys, z. B. der Android-IMSI-Catcher-Detector[49] oder der im Google Play Store erhältliche Cell Spy Catcher.

---

46 Einen guten Überblick gibt's hier: *https://guardianproject.info/apps*

47 Vgl. *https://de.wikipedia.org/wiki/IMSI-Catcher*

48 Ein guter Überblick findet sich hier: *http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html*

49 *https://f-droid.org/repository/browse/?fdfilter=IMSI&fdid=com.SecUpwN.AIMSICD*

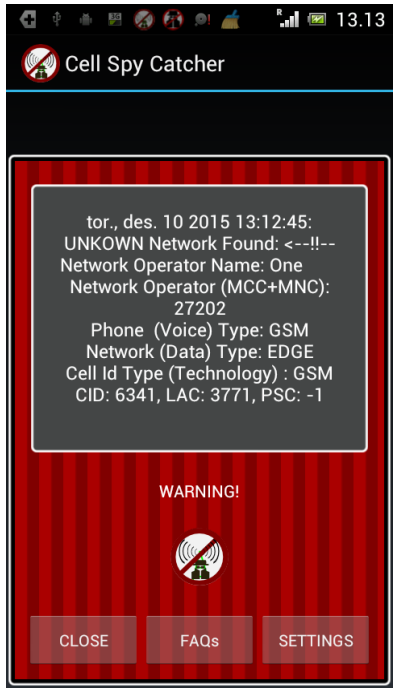


Bild 1.1: Cell Spy Catcher

Mehr Möglichkeiten bietet SnoopSnitch, ebenfalls im Play Store erhältlich, aber angewiesen auf ein gerootetes Handy mit Qualcomm-Chipsatz. Hier hat man die Möglichkeit, stille SMS zu detektieren oder einen SS7-Angriff abzuwehren.[50]

1.2 Anonym im Internet?

Es gibt vermutlich keinen Internetnutzer, der nicht die Dienste von Google genutzt hätte. Die wenigsten User wissen natürlich, was hier im Hintergrund passiert, während Google die gesuchten Informationen (plus Werbung) bereitstellt. Auf Heise.de (*www.heise.de/ct/artikel/Der-Datenkrake-290454.html*) findet sich dazu eine prophetisch klingende Stellungnahme: »Spinnt man den Gedanken eines Google weiter, das möglichst viele Daten sammelt, und nimmt man an, der Suchmaschinenriese würde nicht nur seine Nutzer, sondern alle Surfer ausspionieren wollen, so ergäbe sich eine fast Orwell'sche Vision der totalen Überwachung. Das Erschreckende daran ist, dass auch hierfür viele technische Voraussetzungen bereits existieren.« Wie also kann man es vermeiden, zu viele Spuren im Internet zu unterlassen? Im Privacy-Handbuch (kostenlos unter *wirbleibenalle.org/wp-content/uploads/privacy-handbuch.pdf*, Seite 54 ff.) findet sich dazu ein fiktives Beispiel, wie man durch Verkettung von auf unterschiedlichen Seiten verstreuten Datenpaketen einen »normalen« User identifizieren und outen kann.

---

50 *https://play.google.com/store/apps/details?id=de.srlabs.snoopsnitch*

Über eine andere, sehr reale Falle berichteten zum Ende des Jahres 2013 Presse, TV und Rundfunk: Die bis zum letzten Jahr kaum in Erscheinung getretene Kanzlei »Urmann und Collegen« verschickte gegen Ende des Jahres massenhaft, d. h. zehntausende, Abmahnungen an nichts ahnende Redtube-Benutzer. Redtube ist ein Erotik-streaminganbieter für so illustre Filmchen wie »Miriam's Adventures«, »Dream Trip«, »Hot Stories« oder »Amanda's Secrets«. Wer sich hier gütlich tat, soll jetzt 250 Euro Abmahngebühren zahlen. Abgesehen von der Tatsache, dass der Unterschied zwischen Kopieren und Streamen nicht so genau genommen wurde, bleibt die spannende Frage, woher die IP-Adressen der beschuldigten User kommen! Nur aufgrund dieser IP-Adressen konnten per Umweg über das Landgericht die realen Daten der Porno-konsumenten ermittelt werden. Und diese wurden natürlich auf den Anbieterseiten des Streamportals geloggt, gegebenenfalls wurden diese Daten auch durch Dritte ausgespäht, oder – der wahrscheinlichste Fall – die Userdaten wurden von Trafficholder.com geloggt, der sie dann automatisch an Redtube weiterroutete. Trafficholder.com ist ein Adult-Traffic-Broker, der sich dafür bezahlen lässt, Seitenaufrufe von seinem Redirect-Dienst zu einer vom User nicht ursprünglich gewünschten Seite weiterzuleiten.

Grundsätzlich bleibt an der Stelle festzuhalten, dass 100 % anonymes Surfen eher nicht möglich ist bzw. so viele Hürden zu überwinden sind, dass die meisten vorher aufgeben. Wer nur bestimmte Seiten im Netz anonym besuchen oder Daten bei OCHs (One-Click-Hostern) laden will, der kann dies z. B. über einen Webproxy bewerkstelligen. Die Technik ist relativ simpel. Die Funktionsweise lässt sich recht einfach auf *http://www.hidemyass.com/proxy* oder *http://www.schnellster-webproxy.net* testen. Hierfür gibt man seine gewünschte Zieladresse an und surft von dort aus dann anonym weiter. Sicherheitshalber sollte man die korrekte Funktionsweise des Webproxys durch einen Vorher-nachher-Vergleich überprüfen. Für diese Überprüfung eignen sich dann Internetseiten wie *http://www.anonym-surfen-test.de*.

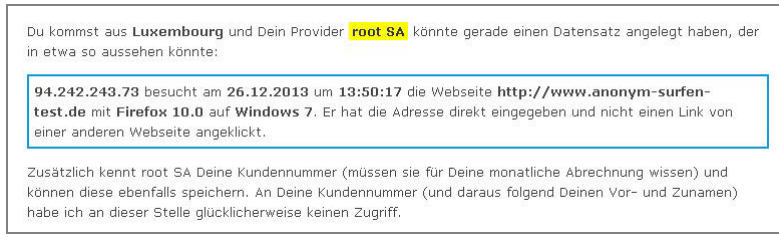


Bild 1.2: IP-Test 1

Im ersten Fall wird uns die IP 94.242.243.73 und der Provider root SA (Luxembourg) unterstellt, im zweiten Fall (über einen anonymisierenden Webproxy) waren wir mit der IP 93.174.93.145 und dem Provider Ecatel.net (Niederlande) unterwegs.

Bild 1.3: IP-Test 2

Noch etwas eleganter funktioniert dieses Prozedere, wenn man einen Proxyswitcher benutzt, beispielsweise Proxy-Listen.de auf *www.proxy-listen.de*. Sofern man nicht gerade mit hochkriminellem Elan oder gesteigertem Sicherheitsbewusstsein unterwegs ist, mögen diese Werkzeuge ein einigermaßen sicheres Gefühl beim Surfen geben. Was aber häufig außen vor bleibt, sind die Fragen nach dem Sitz des Providers (von dem man seine Sicherheit abhängig macht) und den Serverlogs. Hat der Provider seinen Sitz in der EU, vielleicht sogar in Deutschland selbst, wird er mit Ermittlern oder Nachrichtendiensten leichter zusammenarbeiten, als wenn der Provider beispielsweise in der Mongolei residiert. Eine andere Frage sind die Serverlogs. Genauer gefragt: Werden Serverlogs geschrieben (mit unserer echten IP-Adresse), und, wenn ja, sind die Serverplatten verschlüsselt?

Wer sich nicht von einem Anbieter abhängig machen möchte, kann auf Anonymisierungsdienste wie Tor Onion Router zurückgreifen. In Kombination mit einem modizierten Firefox-Browser in Form des »Tor-Browsers« verfügt man dann über einen sehr guten Basisschutz fürs anonyme Surfen (kostenlos als Installationspaket zum Herunterladen unter *https://www.torproject.org/projects/torbrowser.html.en*).

Wer Tor nutzt, surft über ein weltweit verteiltes Netz von 2.400 aktiven Knoten. Für die eigene Route werden davon drei Knoten genutzt, die in Abständen von etwa zehn Minuten gewechselt werden. Theoretisch soll ein Mitlesen unbefugter Dritter selbst dann noch nicht möglich sein, wenn zwei von drei Knoten kompromittiert wurden, da die Pakete innerhalb des Tor-Netzwerks immer verschlüsselt weitergereicht werden. Einzige Ausnahme von dieser Regel: Der erste und der letzte Knoten dürfen nicht in der Hand des Angreifers liegen. Zusätzliche Sicherheit vor der Identifikation im Netz bietet eine angepasste Browserkonfiguration, die Cookies, das Auslesen des HTTP-Headers etc. unterbindet. Leichtfertig verhalten sollte man sich selbst dann allerdings nicht, zumal es Januar 2017 Forschern gelungen ist, Verfahren des Browser-Fingerprintings deutlich zu verbessern: Mit diversen Tricks konnten Forscher von der Lehigh University[51] in Pennsylvania/USA Browser mit einer Zuverlässigkeit von 99,24 Prozent identifizieren – ohne dabei auf IP-Adressen, Cookies oder ähnliche Techniken zurückgreifen zu müssen. Als wirkungsvollen Schutz gegen Browser-Fingerprinting[52] empfehlen die Forscher den soeben erwähnten Tor-Browser, der insbesondere kein Canvas und damit kein WebGL ermöglicht, oder einen Browser, der in einer VM läuft.

---

51 *https://drive.google.com/file/d/0B4s900Byvv1ibW5uc1NiU2g3R3c/view*

52 *https://github.com/Song-Li/cross_browser*

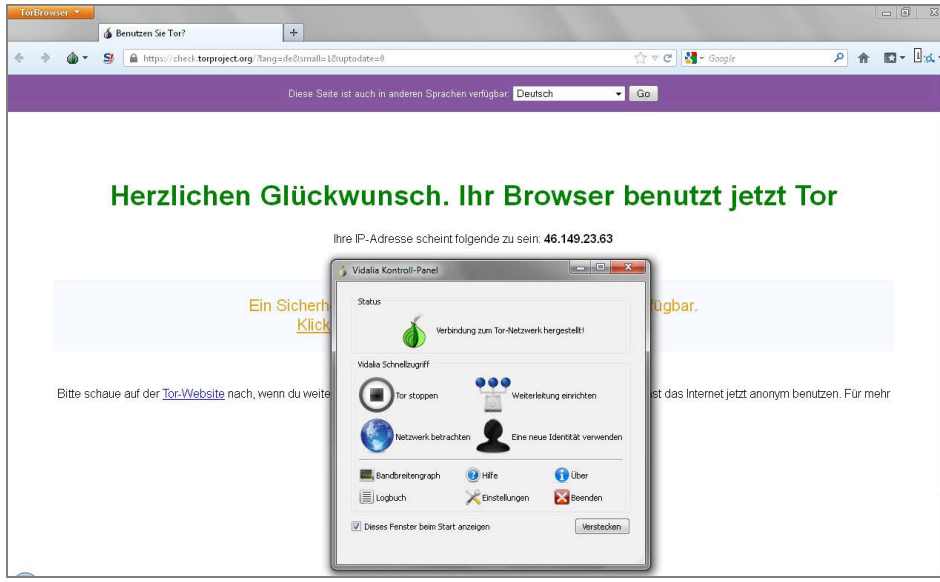


Bild 1.4: Eröffnungsbildschirm Tor

Was man aber im Auge behalten muss, sind zwei mögliche Nachteile, die sich durch den Gebrauch des Tor-Netzwerks ergeben:

- Kritisch zu betrachten sind die Bad Exit Nodes, das sind die Austrittspunkte, an denen die Informationen – sofern sie nicht SSL- oder TLS-verschlüsselt sind, im Klartext vorliegen. Erlangt ein Angreifer die Kontrolle über einen Ausgangsknoten, kann er HTTPS- durch HTTP-Links ersetzen, SSL-Zertifikate fälschen oder JavaScript in abgerufene Webseiten einschmuggeln. Betreibt jetzt ein Angreifer (z. B. die NSA) ein mittleres Tor-Relay in Eigenregie, kann in sechs Monaten die Anonymität von 80 % der verfolgten Benutzer gebrochen werden, so eine im Jahr 2013 veröffentlichten Studie von Wissenschaftlern des U.S. Naval Research Laboratory und der Georgetown University (siehe *http://de.wikipedia.org/wiki/Tor_%28Netzwerk%29*). Werden mehr Überwachungsressourcen eingesetzt, erhöht sich die Zahl der deanonymisierten User auf 95 %. Den Nutzern dieses Diensts sollte klar sein, dass sie durch dessen Gebrauch verstärkt ins Visier der Fahnder und Datenschnüffler geraten.
- Von Nachteil ist der Geschwindigkeitsverlust. Allein schon der Aufruf des Browsers über das Vidalia-Kontrollpanel braucht gut 15 Sekunden, bis er startklar ist. Eigene Tests ergaben, dass Seitenaufrufe zum Teil bis zu 50 % länger dauern, wenn sie über das Tor-Netzwerk geroutet werden. Noch schlimmer wird es, wenn umfangreiche Downloads über Tor abgewickelt werden sollen.

Eine Alternative zu Tor bietet JonDonym (*https://www.anonym-surfen.de/*). Das Anonymisierungsnetzwerk besteht aus einer Reihe fester, d. h. fest zugeordneter Mixerkaskaden, die von öffentlichen Einrichtungen, Firmen und Einzelpersonen betrieben

werden. Nach dem Einloggen in das Netzwerk werden die Daten der einzelnen Nutzer mehrfach verschlüsselt, weitergeleitet und gemixt. Es gibt hier zwei Modelle: kostenfreie, nur für das Surfen geeignete Mixerkaskaden und die Premiumkaskaden, die man für einige Tage kostenfrei testen kann.

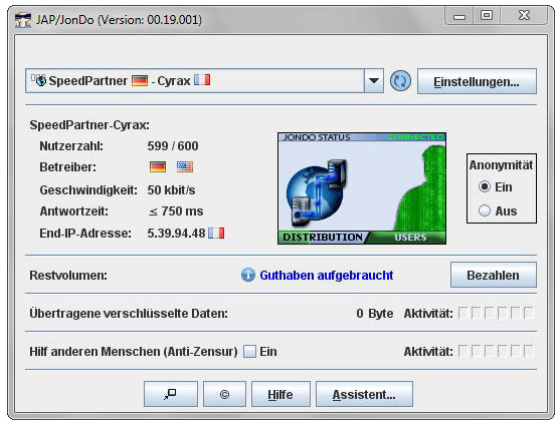


Bild 1.5: JonDo-Konsole

Der JonDo-Client gestattet die Auswahl entsprechender Mixerkaskaden.

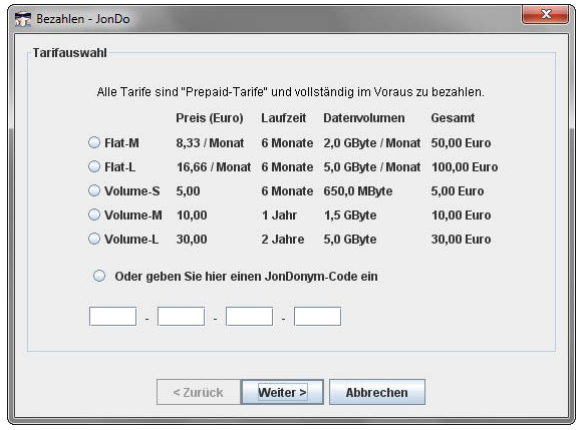


Bild 1.6: JonDo-Kostenübersicht

Wenn das kostenfreie Datenvolumen aufgebraucht ist, kann der entsprechende Premiumdienst gebucht werden. Da anonymes Surfen mehr ist als nur die Verschleierung der IP-Adresse, kommt JonDonym mit einem eigenständigen Firefox-Profil daher: JonDofox (auch fürs Tor-Netzwerk nutzbar), das Firefox so konfiguriert, dass keine verräterischen Spuren auf die eigentliche IP-Adresse zurückverweisen. Da die Premiumkaskaden im Ausland verteilt arbeiten, wird übergreifendes Schnüffeln bzw. Überwachen stark erschwert, denn man braucht Zugriff auf alle beteiligten Mixerkaskaden, um einen Anwender zu enttarnen und seinen Datenverkehr mitzuschneiden. Bislang sind im Gegensatz zum Tor-Netzwerk keine Schnüffelkaskaden bekannt

geworden. Aus diesem Grund verfügt JonDo wohl über den höheren Sicherheitsstandard als das Tor-Netzwerk. Auch lässt sich über die Premiumkaskaden ein besserer Datendurchsatz erzielen als über das kostenlos zu nutzende Tor-Netzwerk. Aber selbst bei Premiumkaskaden ist der Java-Client in JonDonym ziemlich träge. VoIP-Anwendungen sind nicht sinnvoll damit zu betreiben.

Eine weitere Alternative zu Tor ist der noch im Anfangsstadium steckende Dienst I2P.

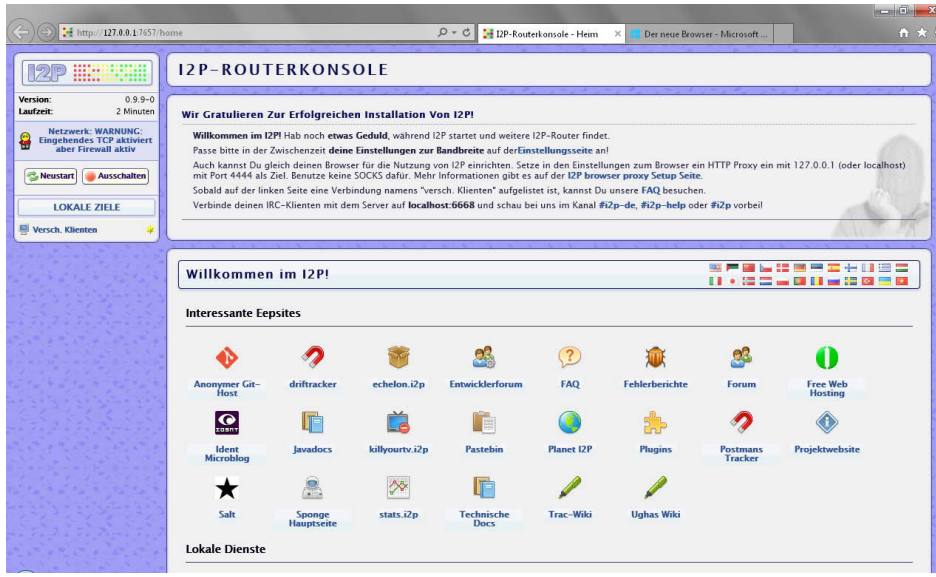


Bild 1.7: I2P – Routerkonsole mit umfassenden Konfigurationsmöglichkeiten

I2P (Invisible Internet Project) gehört zu den anonymen P2P-Netzwerken, in denen der Datenverkehr mehrfach verschlüsselt über wechselnde Stationen des Netzes geleitet wird. Im Gegensatz zu JonDo ist auch der eigene Rechner in die Weiterleitung von Daten anderer Teilnehmer eingebunden. Aufgrund dieser Topologie ist ein Spähangriff durch Dritte nur schwer realisierbar. Die von uns vor mehr als zwei Jahren – mit mäßigem Erfolg – getestete Software liegt nun in der neuen Version 0.9.27 vor.[53] Leider können wir unser Urteil aus der letzten Auflage nicht revidieren. Das Konzept klingt spannend, in der Praxis dürfte es die meisten Anwender stark überfordern. Der Funktionstest hat uns ebenfalls nicht überzeugt. Die Entwicklung tritt anscheinend auf der Stelle, was sich auch an der parallel angebotenen portablen Version von I2P zeigt: Sie verharrt auf dem Stand von 2012[54].

Neu und auf der Basis des TOR-Netzwerkes ist Tails[55]. Es steht für »theamnesicincognit olivesystem« und ist ein Live-Betriebssystem, das von USB-Stick oder DVD gestartet

53 *https://geti2p.net/de/download*

54 *http://portable-i2p.blogspot.de/*

55 *https://tails.boum.org/index.de.html*

wird, um anonym ins Internet gehen, E-Mail und Messanger nutzen zu können, ohne irgendwelche Spuren zu hinterlassen.

Wir haben es getestet und können es mit gewissen Einschränkungen weiterempfehlen.

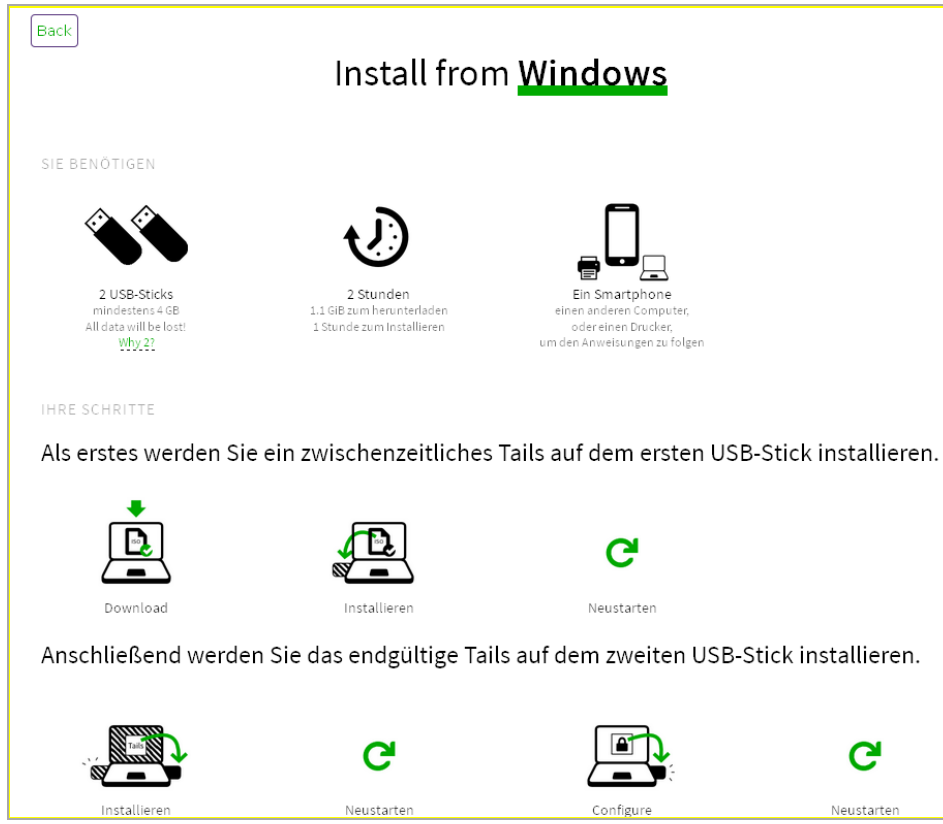


Bild 1.8: Tails – anonym ins Internet ohne Spuren zu hinterlassen

Die Einschränkungen bestehen einmal im Installationsprocedere: Zuerst muss man die ISO-Datei mittels eines zu installierenden Firefox-Add-ons herunterladen und verifizieren. Dann ist ein spezieller USB-Installer herunterzuladen und in Betrieb zu nehmen. Damit wird Tails temporär auf einem ersten USB-Stick installiert. Danach wird der PC mit diesem USB-Stick gestartet, was laut Entwickler mitunter etwas diffizil sein kann. Auf einer Linux-Oberfläche ist dann ein zweiter USB-Stick für die endgültige Tails-Installation auszuwählen. Danach wird der erste auf den zweiten Stick geclont, damit weitere Sicherheitsoptionen aktiviert werden können. Von diesem zweiten Stick wird der Rechner neu gebootet. Der abschließende Test zeigte, nach Stunden Arbeit, ein gemischtes Resultat:

Der erste Stick ließ sich problemlos booten, beim zweiten Stick verweigerten sich unsere Rechner, d. h. der zweite Stick fuhr das System nicht hoch, weder mit einem normalen

noch mit einem UEFI-Bios. Für Otto Normalanwender ist das keine befriedigende Lösung – auch wenn die Entwickler eine recht ausführliche Dokumentation zur Verfügung stellen, die Schritt für Schritt durch die Installation führt. Ein weiterer Schönheitsfehler: Der zweite, geclonte Bootstick kann unter Windows nicht mehr verwendet, also auch nicht formatiert oder repartioniert werden. Die einzige Möglichkeit, ihn zu reanimieren, ist die Resetfunktion des USB-Image-Tools[56]. Einfacher in Betrieb zu nehmen ist auf jeden Fall die oben schon beschriebene portable Version des Tor Browsers (auf Basis von Firefox). Wer noch paranoider ist und noch weniger Spuren hinterlassen möchte, lässt den Tor Browser außerdem in einer Sandbox (z. B. Sandboxie) laufen, ggf. (zusätzlich) auch auf einem separaten USB-Stick.

Als dritte Gruppe von Internetanonymisierungsdiensten fungieren kommerzielle Anbieter (wobei es hier abgespeckte bzw. Testangebote gibt) via VPN (Virtual Private Network). Eine gute Übersicht findet man auf der Seite der Verbraucherschutzstelle Niedersachsen (*verbraucherschutzstelle.de/anonym_surfen.htm*). Die Liste erhebt nicht den Anspruch auf Vollständigkeit, aber man sieht bereits, dass Anonymisierung durchaus ein taugliches Geschäftsmodell zu sein scheint. Sobald ein Anwender eine VPN-Verbindung aufgebaut hat, geht die Anfrage an die neue Zieladresse verschlüsselt über den Server des Anbieters, der in irgendeinem Land mit z. B. einem höheren Datenschutzlevel stehen kann. Viele Menschen aus autoritär regierten Ländern nutzen diese Möglichkeit, weitgehend anonym Informationen auszutauschen. Auch Anwender, die sich in unsicheren Netzen (Internetcafés, offene Hotspots) bewegen und nicht wollen, dass ihr Surfverhalten ausspioniert bzw. ihre Daten mitgelesen werden, nutzen VPN-Verbindungen – sollten aber im Hinterkopf haben, dass der VPN-Anbieter die Möglichkeit hat, die gesamte Kommunikation aufzuzeichnen. Diejenigen, die Angebote (z. B. auf YouTube) nutzen möchten, die für User aus Deutschland gesperrt sind, sind mit solchen Dienstleistern ebenfalls gut bedient.

Eine der günstigsten Möglichkeiten, sich weitgehend versteckt im Internet zu bewegen, bietet Swiss VPN (*www.swissvpn.net/?lang=de*) – einer von uns hat sie über ein Jahr positiv getestet. Der Dienst ist für die gebotene Leistung relativ preisgünstig (12 Monate für 96 Schweizer Franken ohne Volumenbegrenzung), die Installation einfach, und die praktischen Einschränkungen sind gering. Die Einrichtung wird über die Netzwerkfreigaben in Windows vorgenommen und ist in wenigen Minuten auch von Newbies abgehakt (siehe *www.swissvpn.net/sw7_de.html*).

---

56 *http://www.alexpage.de/usb-image-tool/*

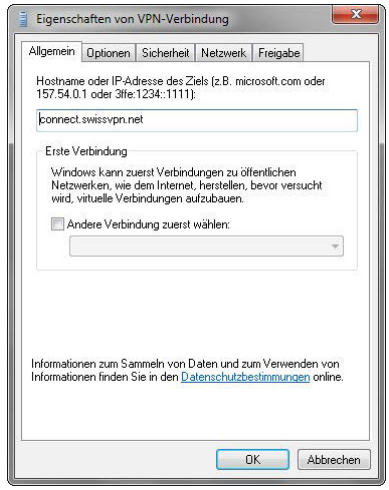


Bild 1.9: Einfach einzurichten: Swiss VPN

Es sind allerdings auch einige kleinere Nachteile mit Swiss VPN verbunden. Standardmäßig (Testbetrieb für SSL VPN und L2TP/IPsec seit Kurzem möglich) nutzt dieser Anbieter das PPTP-Protokoll, das als kompromittiert gilt. Im Artikel »Der Todesstoß für PPTP«[57] beschreibt Jürgen Schmidt präzise, wie mithilfe des Cloud-Diensts Cloudcracker und 200 US-Dollar die PPTP-Verbindung deanonymisiert werden kann. Die anderen angebotenen Protokolle gelten als sicher. Leider ist es nicht möglich, die angebotenen Dienstleistungen anonym via Paysafe oder Ähnliches zu begleichen. Der Anbieter ist dem strengen Schweizer Datenschutz verpflichtet: »While SwissVPN keeps logs of their users for six months, the logs only note VPN connection IPs, the amount of data transferred, and the total duration of the connection. SwissVPN *does not log any accessed website addresses* or information about downloads made through their VPNs.« (*http://vpn-services.bestreviews.net/swissvpn-reviews/*)

Wer hier noch höhere Anforderungen an seine Anonymität hat, greift zu einem Anbieter wie Perfect Privacy (*https://www.perfect-privacy.com/*), dem auch die Verbraucherschutzstelle Niedersachsen Bestnoten ausstellte. Es werden keine Logs gespeichert, die Datenträger sind verschlüsselt, und für die Dienstleistung kann anonym bezahlt werden. Schon die Internetseite der Betreiber (Zusammenschluss unabhängiger Privatpersonen) zeigt, wie professionell er aufgestellt ist. Der Anwender kann wählen, ob er seinen gesamten Internettraffic verschlüsseln will (via OpenVPN) oder einzelne Anwendungen via SSH2 und Perfect Privacy Tunnel Manager inkl. Portforwarding und Squid/SOCKS5-Proxys. Die Einrichtung gestaltet sich so oder so relativ einfach. Mit dem Aufruf der Perfect-Privacy-Seite kann man schnell feststellen, ob die Installation geglückt ist.

---

57 *http://www.heise.de/security/artikel/Der-Todesstoss-fuer-PPTP-1701365.html*

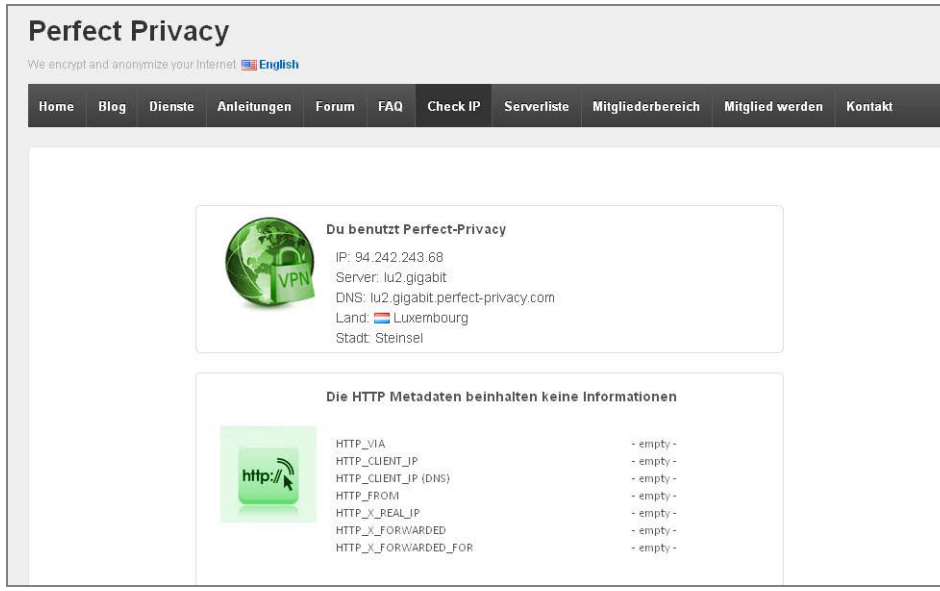


Bild 1.10: Perfekte Verschlüsselung und Tunneling

Im Vergleich mit anderen VPN-Anbietern glänzt Perfect Privacy vor allem mit hohem Datendurchsatz (ohne Beschränkung) und einem guten Support (unter Einsatz des Teamviewers).

Eingangs schrieben wir, dass Anonymität selten zu 100 % garantiert werden kann – egal durch welchen Anbieter. Hinter diesem Statement steht die Erfahrung, dass es nicht reicht, einen Anbieter bzw. einen Service zu wählen und sich dann beruhigt im Bürostuhl zurückzulehnen. Es gilt, eine komplette Kette von potenziellen Einschränkungen im Auge zu behalten.

Vollständige Anonymität ist nur sinnvoll, wenn die Inanspruchnahme des Diensts selbst anonym gestaltet werden kann, d. h. weder E-Mail-Adresse noch sonstige Kontaktdaten seitens eines Anbieters verlangt werden und auch die Bezahlung selbst anonym vonstattengehen kann. Darüber hinaus sollte alle Faktoren, die deanonymisierend wirken, ausgeschlossen werden.

Häufig wird trotz Umstellung auf einen VPN-Service der DNS-Server des ursprünglichen Internetproviders angezeigt. In einem solchen Fall ist eine Anonymisierung des Internetverkehrs illusorisch, da anhand des DNS-Servers die Identität des Anwenders aufgedeckt ist.

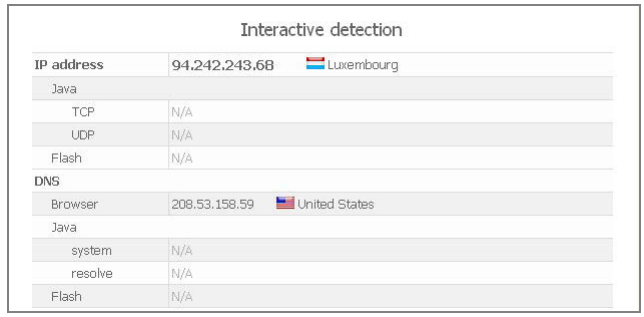


Bild 1.11: Wirklich anonym?

Betrachten wir den oberen Screenshot. Er wurde auf der Seite von *whoer.net/extended* erstellt. Beispielsweise deutet die IP-Adresse auf einen Luxemburger Standort hin, während der DNS-Server auf die Vereinigten Staaten verweist. Stünde hier jetzt die Adresse des originären Internetproviders, z. B. der Telekom, wäre die Tarnung hinfällig. Noch genauere Informationen ermöglicht der DNS-Leaktest auf *https://www.dnsleaktest.com*.

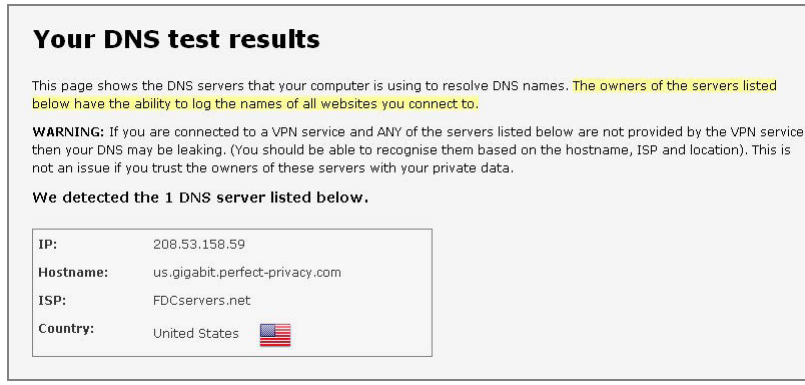


Bild 1.12: Geleakt oder nicht geleakt?

Hier finden sich mehr Details als auf Whoer.net, z. B. den Namen des ISP und das zugehörige Land. Wenn hier also der Name des tatsächlichen Internet-Service-Providers stünde, müsste in den Netzwerkeigenschaften ein anderer DNS-Server eingetragen werden – und zwar für jede Netzwerkverbindung. In diesem Fall öffnet man das Netzwerk- und Freigabecenter (unter Windows 7) und wählt dort den Menüpunkt *Adaptereinstellungen ändern*. Für jede dort gelistete Netzwerkverbindung trägt man jetzt unter *Eigenschaften* einen anderen DNS-Server ein.

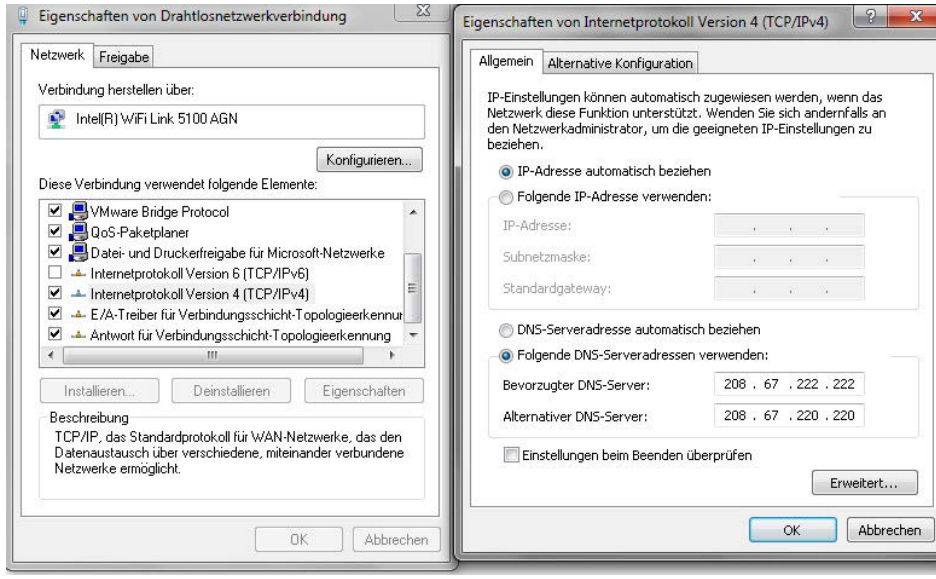


Bild 1.13: DNS-Server anonymisieren

Die korrekte Verfahrensweise wird ausführlich unter *https://community.hide.me/threads/dns-leak-erkennen-und-verhindern.20/* beschrieben. Eine Liste frei verfügbarer DNS-Server findet man hier: *www.fixmbr.de/opendns-und-andere-freie-dns-server/*. Und da man gerade dabei ist zu ändern, sollte man auch gleich das Internetprotokoll 6 (TCP/IPv6) deaktivieren. IPv6 wurde, vereinfacht gesagt, entwickelt, um eine größere Anzahl von Internetadressen zur Verfügung stellen zu können (128 Bit Länge von IPv6 zu 32 Bit Länge von IPv4), da im Rahmen von IPv4 diese so gut wie vergeben sind. Von Datenschützern wird kritisch beäugt, dass in der IPv6-Adresse der Interface Identifier die global einmalige MAC-Adresse enthält, die es wiederum gestattet, den Anwender via Hardware-ID eindeutig zu identifizieren. Abhilfe schafft nur eine dynamische Zuweisung der IPv6-Präfixe, die in Windows bei der Installation standardmäßig aktiviert ist. Wer hier unsicher ist, kann sich die aktuelle Einstellung mit nachfolgendem Befehl anzeigen lassen:

```
netsh interface ipv6 show global
```

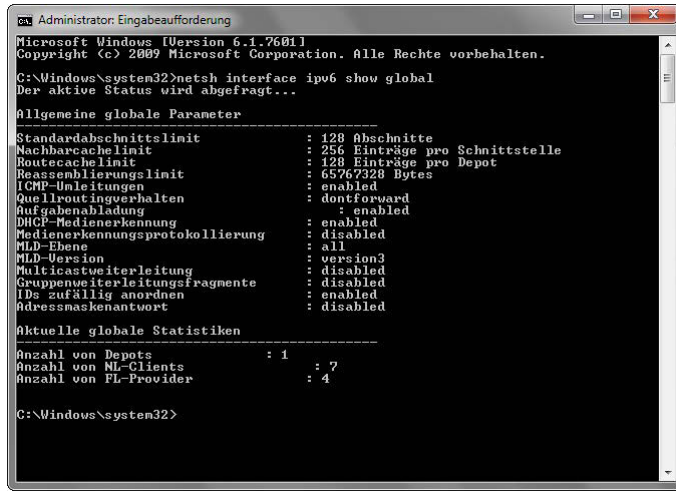


Bild 1.14: Achten Sie auf den Eintrag "IDs zufällig anordnen=enabled"

Auch die Aktivierung von Cookies (inklusive Supercookies und EverCookies), Java und JavaScript im Browser wirkt sich verhindernd auf die Anonymisierung aus. In jedem Browser gibt es die Möglichkeit, Cookies zu reglementieren bzw. sie ganz oder fallweise zu verweigern.

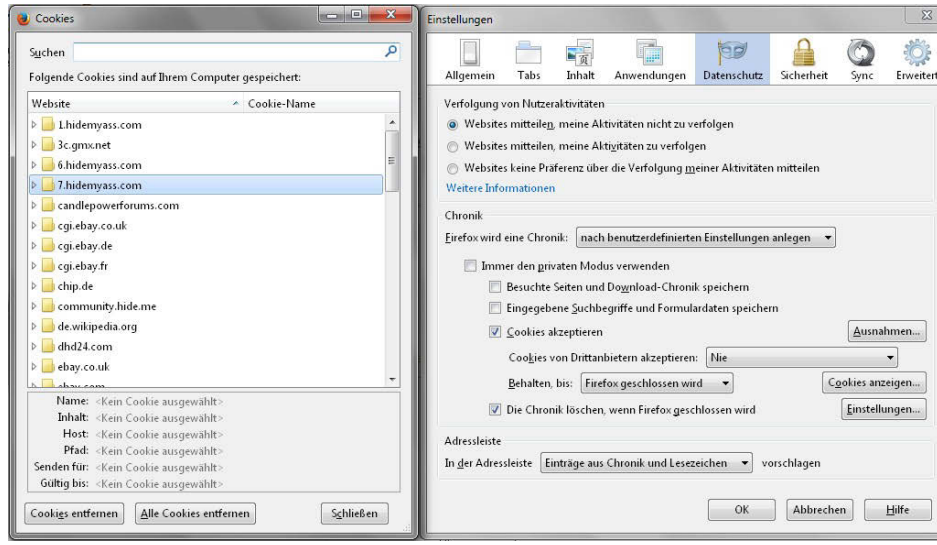


Bild 1.15: Cookies reglementieren mit Firefox

Besonders kritisch im Hinblick auf anonymes Surfen sind die EverCookies, die von der Werbewirtschaft speziell für diejenigen entwickelt wurden, die normale Tracking-Cookies blockieren. EverCookies zeichnen sich dadurch aus, dass sie aus mehreren Komponenten bestehen, die sich nach einer Cookie-Löschaktion wieder selbst

restaurieren. Vollständige Sicherheit vor EverCookies verspricht der Einsatz von Adblockern, z. B. des Firefox-Add-ons *Adblock Plus* in Kombination mit Privacy-Listen. Da viele EverCookie-Technologien mit JavaScript arbeiten, hilft es auch, JavaScript standardmäßig zu deaktivieren, z. B. mit dem Firefox-Add-on *Noscript*.

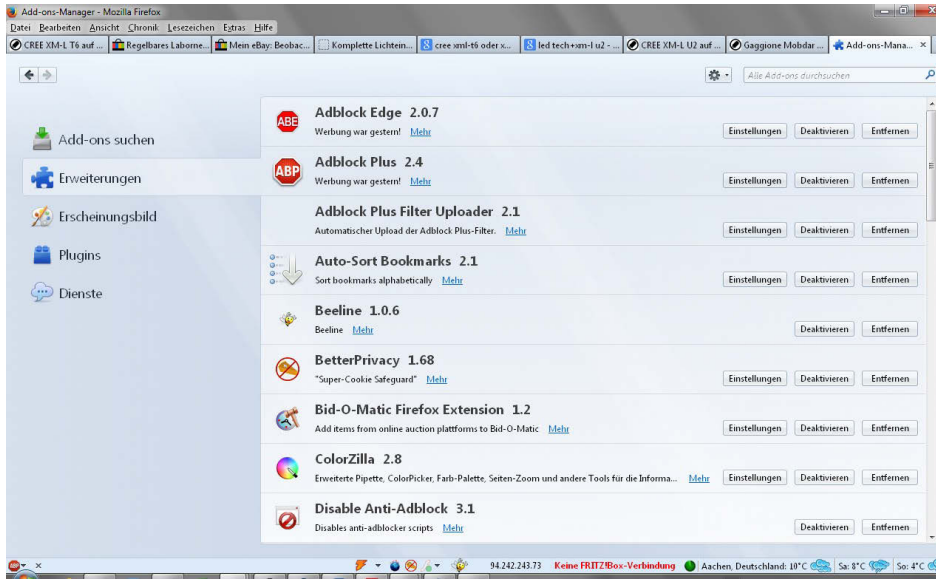


Bild 1.16: Firefox-Add-ons zur Stabilisierung der Privatsphäre

Etliche Werbeanbieter haben sich geradezu darauf spezialisiert, Surfer jederzeit und überall eindeutig identifizieren zu können (*www.bluecava.com/*). Ihr Versprechen: »At BlueCava, marketing means reaching and measuring consumers where they work and play.«

Auch Google nutzt JavaScript und ist als fleißiger Datensammler berüchtigt. Für die meisten dieser Deanonymisierungsbemühungen genügt, wie oben erwähnt, der kombinierte Einsatz von NoScript und Adblock Plus. Eine weitere Lücke, die für eine erfolgreiche Deanonymisierung genutzt werden kann, existiert in der Surfer History (siehe Privacy-Handbuch, Kapitel 4.7, »History Sniffing«, Seite 80). Hier hilft nur, die Historisierungsfunktion im Browser komplett zu deaktivieren.

Leider wird an der Stelle überaus deutlich, wie schwierig die vollständige Anonymisierung im Internet zu bewerkstelligen ist – und auch wie unkomfortabel: Mit den beschriebenen und aktivierten Antispionagetools werden manche Seiten schlicht unbenutzbar. Gegen ein Anti-Adblockerscript kann man noch hochrüsten, z. B. mit dem Add-on Disable Anti-Adblock 3.1, aber wenn JavaScripts für das korrekte Anzeigen einer Seite erforderlich sind, muss man seine Rüstung einen Schlitz weit öffnen – eventuell mit Folgen für die angestrebte Anonymisierung. Zudem soll nicht vergessen werden, zu erwähnen, dass bereits der Browser eine Vielzahl an Merkmalen bietet, den

Nutzer wiederzuerkennen – beispielsweise die installierten Fonts, die Auflösung, die Flash-Cookies, das PREF-Cookie von Google und Ähnliches.

In den letzten beiden Jahren hat eine Technologie von sich reden gemacht, die die Anonymisierung trotz Tor und VPN tendenziell aufhebt: das Canvas Fingerprinting. »Canvas« heißt Leinwand. Beim Seitenbesuch wird mittels Javascript dem Browser ein versteckter Text übergeben. Anhand der Verarbeitung ergibt sich ein (relativ) eindeutiger Fingerprint. Auf der Seite *https://panopticlick.eff.org* kann man z. B. testen lassen, ob der Browser über eine Reihe von einmaligen Merkmalen verfügt, die es erlauben, seinen Anwender auch dann zu identifizieren, wenn er mit Tor o.ä. unterwegs ist.

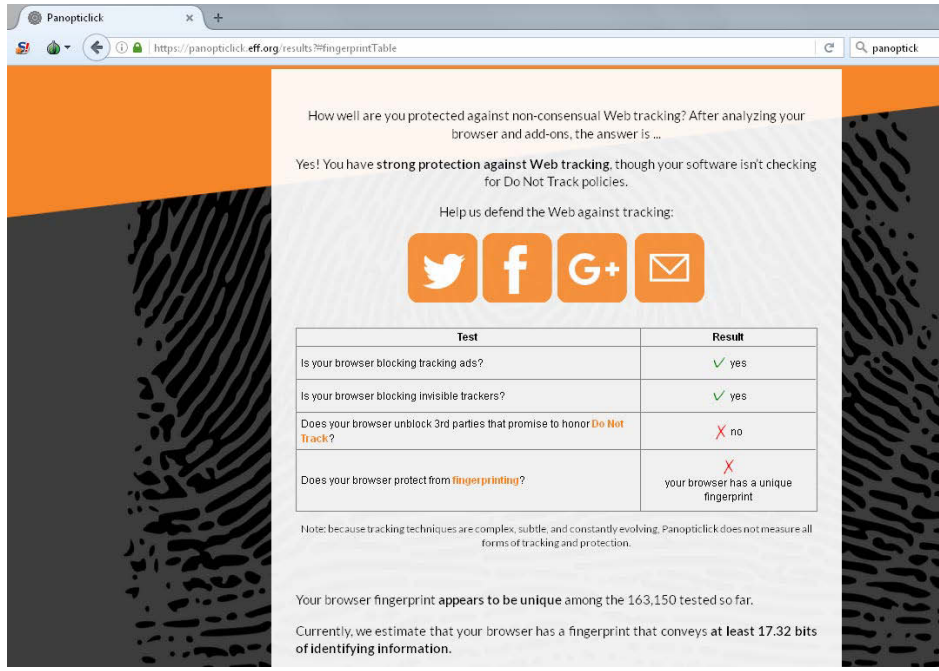


Bild 1.17: Fingerprinting: einmalig trotz Tor

In unserem Fall werden 17.32 Bits ausgelesen, die bewirken, dass nur einer von 163.150 User denselben Fingerprint hat wie wir. Zwar weist nichts auf unseren Namen, Wohnort etc. hin, aber man kann durchaus erkennen, dass wir auf bestimmten Seiten (wiederholt) unterwegs waren. Mit deaktiviertem Javascript kann man das Fingerprinting 100%ig unterbinden, leider auch die Anzeige mancher Internetseiten. Abhilfe verspricht ein Firefox Addon, der Canvasblocker: *https://addons.mozilla.org/de/firefox/addon/canvasblocker/*. Leider hat er bei uns nicht funktioniert, genausowenig wie Privacy Badger, Disconnect oder Adblock Plus in Kombination mit EasyList.

Zu guter Letzt noch ein Surftipp für alle, die Google in der Vergangenheit nutzten, eine praktikable Alternative aber noch nicht kannten. Die Rede ist von Startpage, laut

Eigenaussage die sicherste Suchengine internetweit. Die 2008 mit dem Europäischen Datenschutz-Gütesiegel ausgezeichnete Suchmaschine (siehe *https://startpage.com/deu/protect-privacy.html*) verspricht, weder ID-Cookies anzulegen noch die IP-Adressen ihrer Nutzer zu speichern.

1.2.1 Anonymer bzw. verschlüsselter Mailverkehr

Es hat sich mittlerweile herumgesprochen, dass E-Mails weder Anonymität noch Datenschutz versprechen. Im Grunde gleichen sie Postkarten, die jeder auf dem Transportweg einsehen und lesen kann. Eine erste Sicherheitsstufe kann erreicht werden durch das Einrichten eines anonymen E-Mail-Accounts. Eine anonyme E-Mail-Adresse kann sehr brauchbar sein, wenn man sich von unverlangt zugesandten E-Mails/Spam schützen möchte – z. B. bei der Anmeldung auf einer Website, deren Angebote man nutzen möchte, ohne seine wahre Identität preiszugeben. Man kann dafür eine spezielle Wegwerf-E-Mail-Adresse einrichten (z. B. *http://www.trash-mail.com/*), oder man meldet sich bei einem (kostenpflichtigen) E-Mail-Provider an:

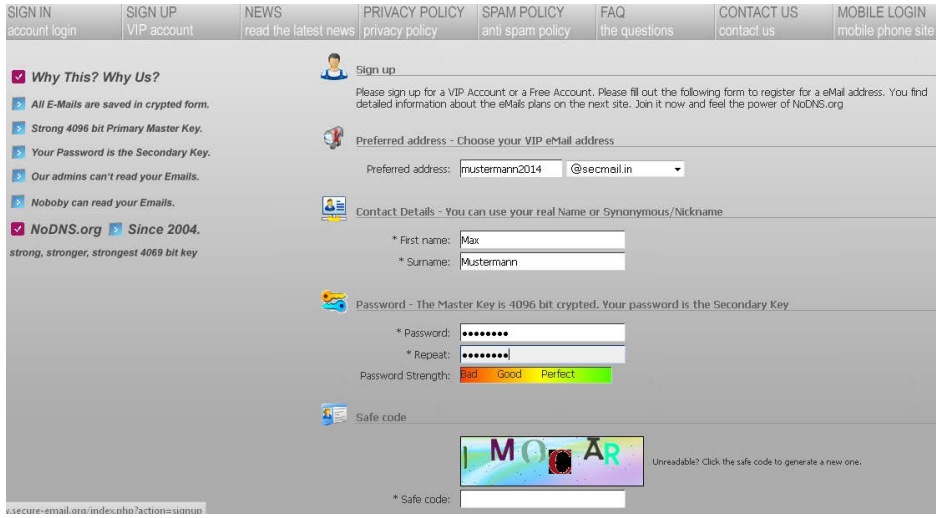


Bild 1.18: Anonymes E-Mail-Konto einrichten

Eine Anbieterliste findet sich hier: *http://www.emailtester.de/anonyme-email-adresse.php*. Möchte man Kosten vermeiden und sich trotzdem anonym bewegen, registriert man sich (anonym, d. h. unter frei erfundenem Namen) z. B. auf *http://www.ok.de*. Um das zu bewerkstelligen, sind allerdings einige Voraussetzungen zu schaffen – die wichtigste: Man sollte sich dort mit einem anonymisierten Browser anmelden, um das Loggen der echten IP-Adresse zu umgehen. Außerdem sollte man bei den erforderlichen Angaben natürlich tunlichst vermeiden, seine echten Daten (Referenz-E-Mail-Adresse, Telefonnummer etc.) anzugeben. Und schließlich: Die dort ankommenden Mails sollten ausschließlich über den Web-Account abgeholt werden und nicht über einen (nicht

anonymen) E-Mail-Client wie z. B. Thunderbird. Hat man das Tor-Netzwerk installiert, kann man unter *tormail.org* ebenfalls einen anonymen E-Mail-Account erstellen, ist aber in der Folge an die Benutzung von Tor gebunden. 2013 hat das FBI wohl den gesamten E-Maildatenbestand gehackt[58]. Auf *http://mail2tor2zyjdctd.onion/register.php#* kann man sich auf Mail2Tor anmelden, das mehr Sicherheit verspricht.

Nicht mit Anonymität, wohl aber mit der klassischen Ende-zu-Ende-Verschlüsselung werben Telekom, GMX.de und Web.de. Der Text der ausgetauschten E-Mails ist verschlüsselt, aber der dem Betreiber bekannte Inhaber kann natürlich immer noch über die Meta-Daten ausspioniert werden, d. h. Cyberkriminelle, Internetprovider wie auch die Dienste wissen, wer mit wem wie oft wie intensiv etc. in Kontakt getreten ist.

Eine witzige Möglichkeit, mit pseudoanonymen E-Mail-Konten zu experimentieren, bietet MaskMe (*https://www.abine.com/maskme*). In der kostenlosen Variante können nach der Installation als Firefox-Add-on beliebig viele Tarnadressen, z. B. *ec6f3ef4@opayq.com*, mit begrenzter Gültigkeit angelegt werden, über die dann in der Folge die getarnte E-Mail-Kommunikation abgewickelt werden kann.

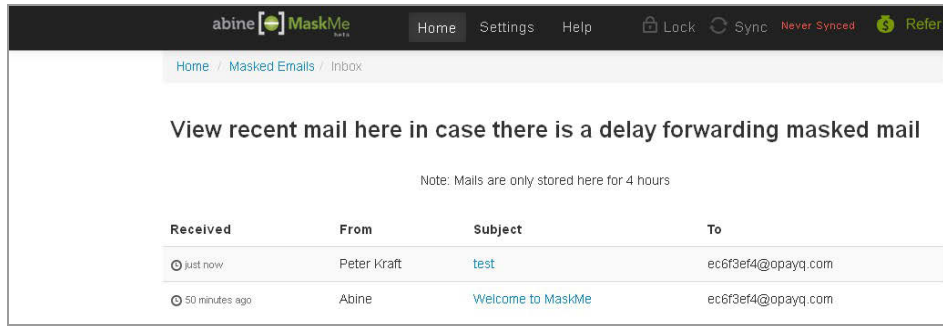


Bild 1.19: Maskierte E-Mails mit MaskMe

Dadurch, dass sich das Add-on im Browser fest verankert, kann immer dann, wenn eine E-Mail-Adresse kurzfristig gebraucht wird, auf einen maskierten E-Mail-Account zugegriffen werden. Die kostenpflichtige Version bietet u. a. die Möglichkeit, seine Telefonnummer zu tarnen.

Ist ein anonymer E-Mail-Account eingerichtet, lauert eine weitere Hürde auch auf den erfahrenen Anwender, nämlich das Verschlüsseln der E-Mail-Inhalte. Eine bewährte, kostenlose Möglichkeit bietet hier der E-Mail-Client Thunderbird (*www.mozilla.org/de/thunderbird*); es gibt auch – für manche vielleicht einfacher einzurichtende – Clients, z. B. The Bat Professional Edition für 39,95 Euro. Wir bevorzugen hier Thunderbird.

Nachdem Thunderbird installiert und die E-Mail-Konten eingerichtet sind, müssen nacheinander das Programm Gpg4win (*www.gpg4win.org/download-de.html*) und das Thunderbird-Add-on Enigmail (*https://www.enigmail.net/download/download-static.php*)

58 *https://gizmodo.com/the-fbi-seized-all-of-tormails-data-and-is-using-it-to-1509838202*

gestartet werden. Gpg4win ist, vereinfacht ausgedrückt, die Open-Source-Variante von PGP (Pretty Good Privacy), dem asymmetrischen Verschlüsselungsprogramm, das Phil Zimmermann 1991 entwickelt hat. Es basiert auf dem Public-Key-Verfahren, d. h., für die Verschlüsselung wird genau ein passendes Schlüsselpaar verwendet, das aus einem öffentlichen und einem geheimen Schlüssel besteht. Wie der Name schon sagt, wird der eine Teil des Schlüssels geheim gehalten, gegebenenfalls auch durch ein Passwort geschützt, während der andere Teil des Schlüssels veröffentlicht bzw. dem Kommunikationspartner über einen offenen Kanal mitgeteilt wird. Statt von Schlüsseln spricht man in dem Kontext auch von »Zertifikaten«. Verdeutlichen wir die prinzipielle Funktionsweise an einem Beispiel. Bob möchte Alice eine verschlüsselte E-Mail senden. Bevor er das tun kann (die technischen Aspekte holen wir weiter unten nach), braucht er ein entsprechendes Schlüsselpaar, das mit geeigneter Software generiert wird. Den geheimen Schlüssel speichert er an einem sicheren Ort, den öffentlichen Schlüssel schickt er jetzt Alice (in einer unverschlüsselten Mail). Mit diesem – öffentlichen – Schlüssel von Bob verschlüsselt jetzt Alice ihre Mail und schickt sie an Bob; im Anhang fügt sie ihren öffentlichen Schlüssel an. Wird diese verschlüsselte Mail jetzt abgefangen, ist sie für den Datenschnüffler wertlos, weil er ja nicht den geheimen Schlüssel von Bob besitzt. Dieser kann aber die Mail von Alice – mit seinem geheimen Schlüssel – entschlüsseln. Mit dem öffentlichen Schlüssel von Alice, den sie an die Mail angehängt hat, kann er nun eine weitere Mail an Alice schreiben, aber dieses Mal verschlüsselt. Um die Sache noch etwas komplizierter zu machen: Woher weiß Bob, dass es Alice ist, die ihm die verschlüsselte Nachricht zukommen ließ? Um die Identität des Absenders zu garantieren, wird die verschlüsselte Mail signiert, d. h., Alice erstellt die Signatur mithilfe ihres geheimen Schlüssels. Da Bob jetzt den öffentlichen Schlüssel von Alice kennt bzw. besitzt, kann er mit dessen Hilfe die Signatur überprüfen, um festzustellen, ob sie tatsächlich von Alice stammt.

So viel zur Theorie. In der Praxis müssen zur Umsetzung einige Installationsschritte vollzogen werden. Gerade für Anfänger nützlich ist das auf der Downloadseite bereitgestellte Gpg4win-Kompendium, in dem Bestandteile von Gpg4win, unter anderem die Verschlüsselungssoftware GnuPG und Kleopatra, die Software für die Schlüsselverwaltung, enthalten sind. Weiterhin enthalten sind ein einfaches E-Mail-Programm (Claws Mail) sowie eine Erweiterung für Outlook 2003 und 2007. Da wir Gpg4win mit Thunderbird einsetzen wollen, ignorieren wir hier diese beide Ergänzungen.

Nach der Installation von Gpg4win wird man mit Kleopatra seine benötigten Schlüssel (unter *Datei/Neues Zertifikat: Persönliches OpenPGP-Schlüsselpaar*) erzeugen. Die erzeugten Schlüssel müssen dann noch einem E-Mail-Konto zugeordnet werden. Das Ergebnis kann so aussehen:

Bild 1.20: Erzeugen eines Schlüsselpaars in Kleopatra

Nachdem diese Hürde genommen ist, soll die Schlüsselfunktionalität in Thunderbird integriert werden. Dafür dient dann die zweite Softwarekomponente: Enigmail. Nach dem Download wird sie über den Add-on-Manager von Thunderbird geladen und eingebunden, zu finden unter dem Menüpunkt *Extras/Add-ons*.

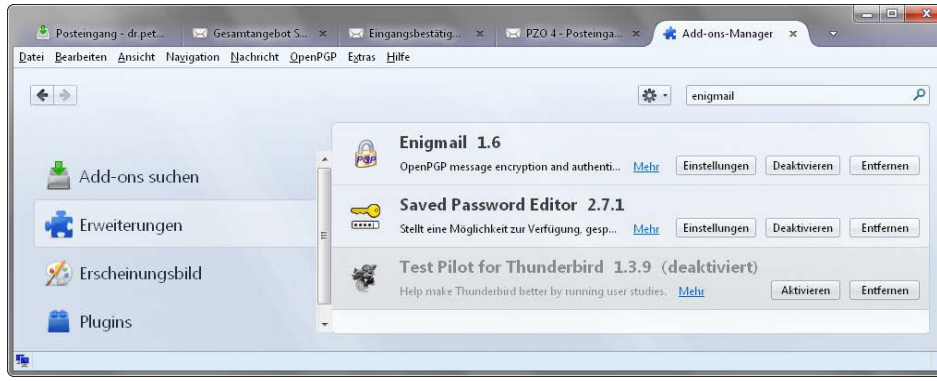


Bild 1.21: Enigmail als Add-on

Die Hauptarbeit ist damit fast getan. Im Anschluss an die Installation von Enigmail findet sich jetzt in Thunderbird ein neuer Menüpunkt.

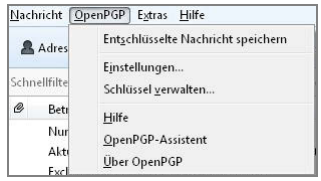


Bild 1.22: Erfolgreiche Integration von Enigmail in Thunderbird

Soll jetzt eine Mail verschlüsselt werden, muss der eigene öffentliche Schlüssel entweder dem Mailpartner geschickt werden, oder – die elegantere Möglichkeit – man veröffentlicht seinen Schlüssel auf einem Schlüsselserver (*Schlüssel verwalten/Schlüsselserver*). Die Schlüsselserver nehmen einem die Mühe ab, seinen öffentlichen Schlüssel immer wieder vorab einem anderen zuzumailen. Außerdem kann man dort auch nach dem Namen bzw.

der E-Mail-Adresse plus Schlüssel seines möglichen Korrespondenzpartners suchen. Das Verschlüsseln (und Signieren) gestaltet sich dann in der Folge relativ problemlos:

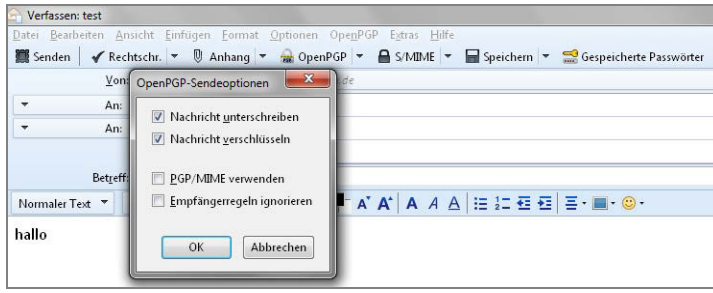


Bild 1.23: Nachricht unterschreiben und verschlüsseln

Ist Enigmail erfolgreich eingerichtet, funktioniert das Entschlüsseln ähnlich einfach. Die mit dem eigenen öffentlichen Schlüssel chiffrierte Mail des Partners kann jetzt durch Eingabe der dem eigenen geheimen Schlüssel zugeordneten Passphrase entschlüsselt werden.

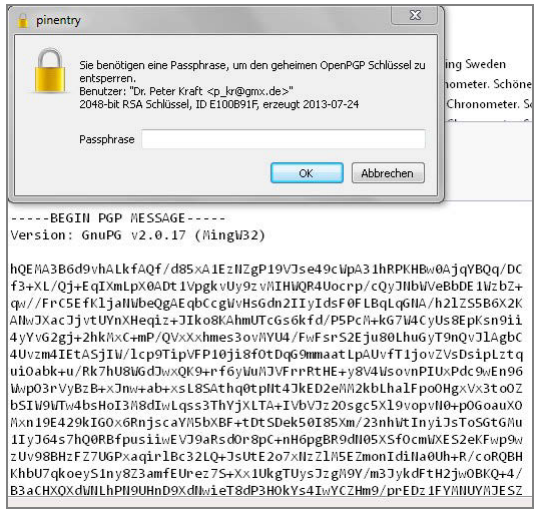


Bild 1.24: Empfangen verschlüsselter Mails

In dem an der Stelle nochmals empfohlenen Privacy-Handbuch ist das Prozedere weit ausführlicher (Kapitel 7, Seite 136 bis 167) beschrieben als hier.

Wem das trotz allem noch zu kompliziert ist: Es gibt weitere Verfahren, seine Kommunikation zu verschlüsseln, z. B. in Form verschlüsselter Zip-Dateien. Sollen Datenschnüffler erst gar nicht merken, dass eine verschlüsselte Kommunikation stattfindet, können steganografische Verfahren eingesetzt werden, z. B. indem man eine verschlüsselte Zip-Datei an ein beliebiges Bild anhängt.

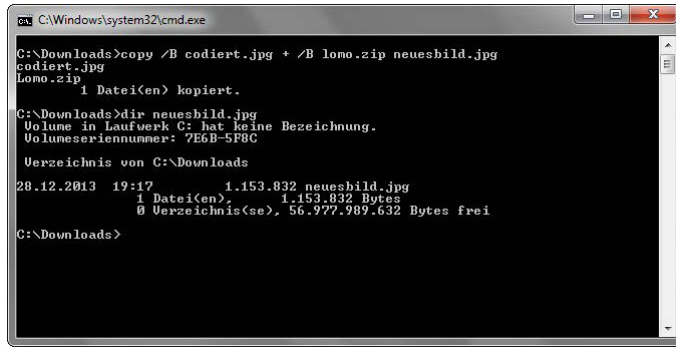


Bild 1.25: Eine verschlüsselte Zip-Datei in einem Bild verstecken

Die ursprüngliche Bilddatei *codiert.jpg* wird mit dem verschlüsselten Archiv *lomo.zip* verbunden. Anschließend kann die neue Datei *neuesbild.jpg* ganz normal mit einem Viewer betrachtet werden. Durch Um- bzw. Zurückbenennen in eine Zip-Datei kann die Datei vom Empfänger dann entschlüsselt werden.

Etwas raffinierter gehen professionelle Tools wie OpenPuff vor.

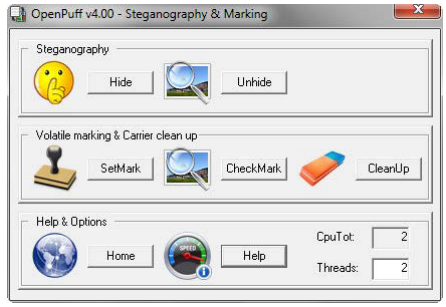


Bild 1.26: Professionelles Steganografietool OpenPuff

Der Leistungsumfang ist beträchtlich (siehe *file:///D:/Downloads/OpenPuff/OpenPuff/html/OpenPuff_Steganography_Home.html*).

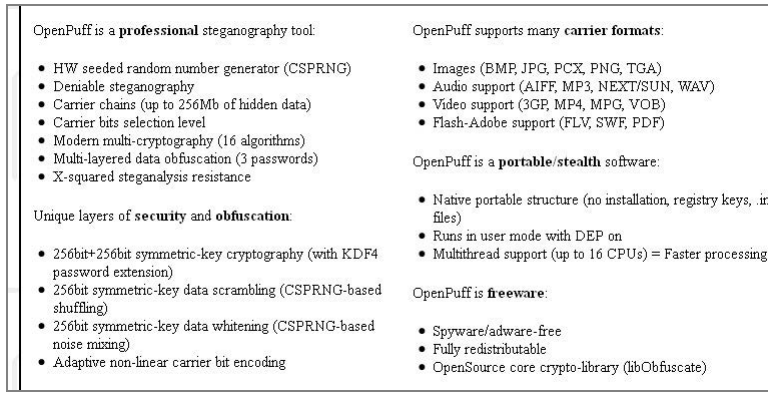


Bild 1.27: OpenPuff-Leistungsumfang

Hin und wieder werden wir auch mal gefragt, was wir von De-Mail halten. In der Regel ist unsere Antwort kurz und bündig: unsicher und für den Privatgebrauch zu teuer. Wenn wir mal das Thema Behördenkommunikation ausklammern, dann ist dieses zur »sicheren, vertraulichen und nachweisbaren« Kommunikation im Internet« (siehe Wikipedia) konzipierte Verfahren wegen fehlender Ende-zu-Ende-Verschlüsselung aus Datenschutzsicht eher wenig brauchbar. Zwar findet auf dem Transportweg eine Verschlüsselung statt, aber an den Endpunkten können Polizei, Nachrichtendienste und andere Zugriff auf die unverschlüsselten Kommunikationsdaten erlangen.

Zwei Empfehlungen möchten wir zu guter Letzt noch aussprechen: erstens ein Stück Hardware gegen Videoüberwachung mit Funkkameras. Das Angebot der Firma JammerWill findet man hier[59]: Es ist ein 8-Band-4Watt-Funkkamera-Störsender, der mit Akku läuft, aber auch ans KFZ-Bordnetz passt. Es versteht sich natürlich von selbst, dass man diese Geräte zwar kaufen und besitzen, aber in Deutschland nicht betreiben darf!

Die zweite Empfehlung geht an Academic Signature[60], ein Verschlüsselungstool auf der Basis von elliptischen Kurven (ECC = Elliptic Curve Cryptograph). Grundsätzlich können wir symmetrische und asymmetrische Verschlüsselungsverfahren unterscheiden. Bei einer symmetrischen Verschlüsselung[61] ist der Schlüssel fürs Ent- und Verschlüsseln identisch. Zum Beispiel basiert die bekannte Container- und Festplattenverschlüsselung Truecrypt (Nachfolger: VeraCrypt) auf einem symmetrischen Schlüssel. Auch wenn man seine Zip-Dateien verschlüsselt, nutzt man diese Technik. Vorteil: die Verschlüsselungsgeschwindigkeit ist in Abhängigkeit vom verwendeten Algorithmus, z. B. AES-255, sehr hoch. Einziges Problem ist der Schlüsseltausch, der in dem Moment notwendig wird, wo die verschlüsselte Nachricht an andere Empfänger verschickt werden soll. Wesentlich

---

59 *http://de.jammerwill.com/frequency-jammers/camera-jammers/wireless-camera-jammers.html.* Die Firma bietet auch – wie es aussieht – recht wirkungsvolle Wifi-Störsender an, mit denen man WLAN-Netze lahmlegen kann und ggf. auch Drohnen stören. Der Betrieb ist in Deutschland natürlich verboten

60 *https://www.fh-wedel.de/~an/crypto/Academic_signature_eng.html*

61 Einen guten Überblick auf die einschlägigen Verschlüsselungswerkzeuge gibt's hier: *http://www.computerbild.de/downloads/sicherheit/verschluesselungssoftware-514*

eleganter lässt sich dies mit dem Einsatz asymmetrischer Verfahren bewerkstelligen. Das Prinzip haben wir schon bei der E-Mailverschlüsselung via PGP/OpenPGP beschrieben. Die dort eingesetzte Technik basiert auf dem Einsatz eines öffentlichen und eines privaten Schlüssels. Hintergrund[62] ist ein mathematisches Verfahren, das auf Multiplikation und Exponentiation auf einem endlichen Körper beruht. Verkürzt ausgedrückt: Wenn der Angreifer den öffentlichen Schlüssel von Bob kennt, mit dem Alice in Kombination mit ihrem geheimen privaten Schlüssel die Nachricht X verschlüsselt, dann ist es mathematisch so gut wie unmöglich, dass der Angreifer aus X und dem öffentlichen Schlüssel von Bob den privaten Schlüssel von Alice berechnen kann. Das Ganze funktioniert als Einwegfunktion, ähnlich wie ein Telefonbuch, aus dem man eine Telefonnummer zu einem gegebenen Namen herauslesen kann, nicht aber den Namen, wenn man nur die Telefonnummer hat.

Elliptische Kurven funktionieren analog, nur wird eine elliptische Kurve über einen endlichen Körper gelegt und die Generierung von privaten und öffentlichen Schlüssel-Operationen auf der Struktur dieser Kurve vorgenommen. Wenn wir die Komplexität der dahinter stehenden Mathematik mal beiseitelassen und uns auf die praktischen Vorteile der ECC kaprizieren, dann können wir festhalten, dass sich die – bei gleicher Sicherheit kürzeren – Schlüssel nach ECC schneller berechnen lassen als die mit konventionellen diskreten Logarithmen erzeugten, was auch für die Implementierung auf Smartcards Vorteile bietet.

Academic Signature (AS) hat im Wesentlichen zwei Funktionen: erstens das Erzeugen und Überprüfen von Signaturen, zweitens die asymmetrische Verschlüsselung von Dateien. Die Installation sowie das Erzeugen von Schlüsselpaaren (privater und öffentlicher Schlüssel) sind auf der Website des Entwicklers Herr Prof. Anders sehr gut dokumentiert – zudem wird der öffentliche Schlüssel des Entwicklers mitgeliefert, so dass man auch die Signatur des Downloadpakets überprüfen kann.

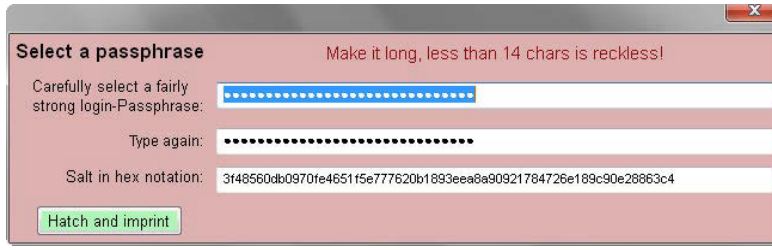


Bild 1.28: Erzeugen der Passphrase als wichtigster Schritt

62 Zu den mathematischen Grundlagen vgl. *https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch* und in der Folge auch *http://www.ecc-brainpool.org/ElliptischeKurven_und_Signatur_Studie.pdf*

Der Zugang zu AS (und den hinterlegten Schlüsseln) funktioniert über eine Passphrase, die beim ersten Anlegen auch gesaltet und gestretched wird, um die Entropie der Eingabe zu erhöhen[63].

Die Arbeit mit dem Programm ist, was die Basisoperationen

- signieren
- Signatur überprüfen
- verschlüsseln
- entschlüsseln

betrifft, relativ simpel. Das Objekt, das überprüft bzw. generiert (verschlüsselt, entschlüsselt) werden soll, wird als Datei geladen, dann wird der öffentliche Schlüssel des Kommunikationspartners geladen und die Operation – das Verschlüsseln – eingeleitet.

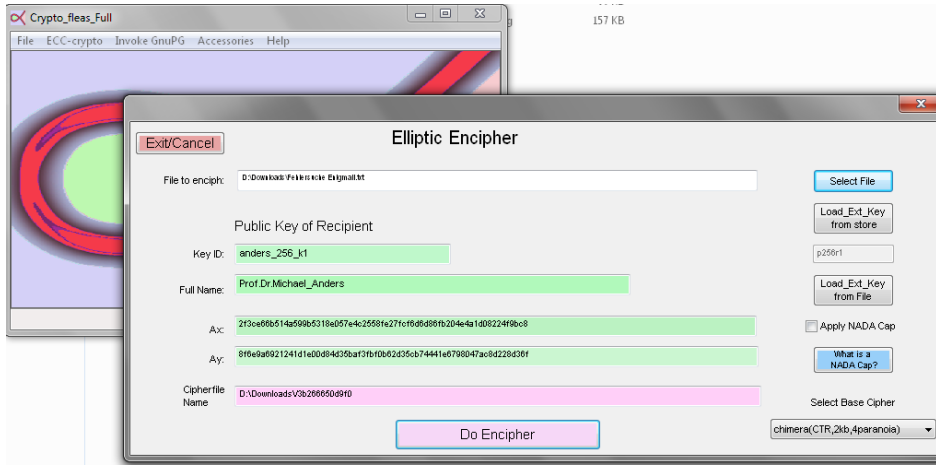


Bild 1.29: Datei + Schlüssel wählen – fertig

Die Originaldatei[64] bzw. der Klartext wird dabei nicht überschrieben; das Chiffrat verrät auch im Namen nichts über den Ursprung der Klardatei. Es ist zwar eine Trivialität, aber nichtsdestotrotz: Chiffrat und Dechiffrat sollten, wenn absolute Vertraulichkeit angestrebt wird, nicht zusammen auf dem Datenträger liegen, d. h. das Dechiffrat, die Originaldatei, sollte, wenn sie nicht mehr gebraucht wird, mehrfach überschrieben und auch sonstige Spüren auf dem Rechner gelöscht werden. Besonders geeignet für dieses Procedere ist Bleachbit[65], das den Rechner von so gut wie allen Spuren befreit.

63 *http://www.fh-wedel.de/~an/crypto/accessories/password_handling01.html*

64 Das Format ist beliebig: Bildatei, Musik, Officedokument …

65 *https://www.bleachbit.org/*

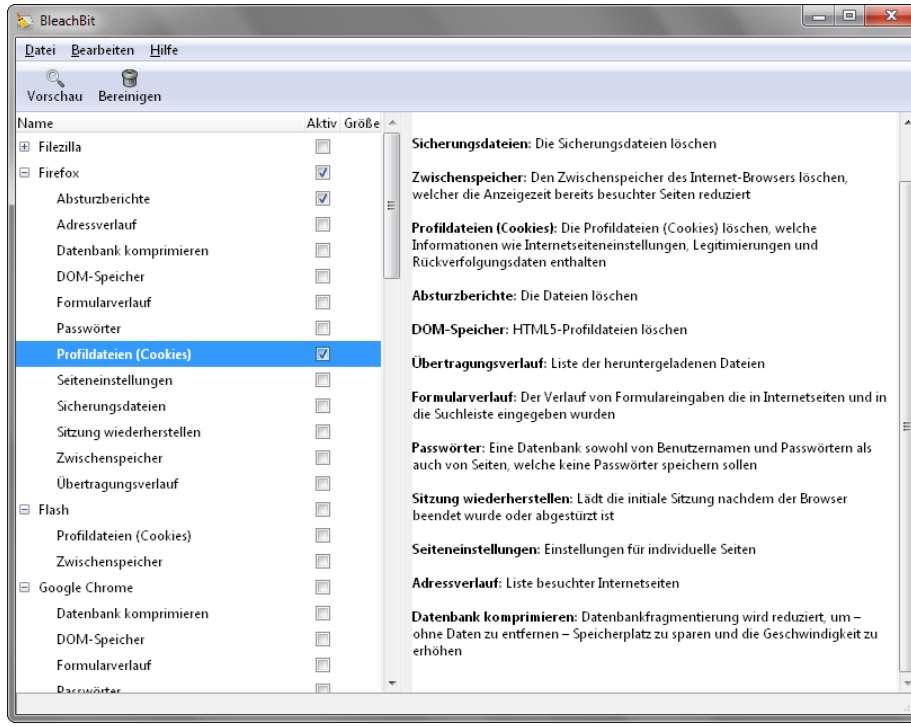


Bild 1.30: Beseitigt (bleicht) alle Spuren

Zu Guter Letzt ein abschließender Tipp: Texte, Dokumente, Dateien, also alles. was Ihnen wichtig ist, sollte nach Möglichkeit auf einem anderen Rechner (mit verschlüsselter Festplatte) liegen als dem, den Sie für Ihre Internetkommunikation nutzen. Ersatzweise tut es auch eine verschlüsselte externe Festplatte, die vom Internetrechner »entkoppelt« werden kann. Geeignet sind Verschlüsselungssysteme wie VeraCrypt. Während des Backups bzw. des Dateitransfers werden sie gemountet, danach wieder entkoppelt.

1.3 Situation aus Sicht der Unternehmen

Seit den Enthüllungen Edward Snowdens, die Aktivitäten der NSA, des GCHQ und anderer »wissenslüsterner« Organisationen betreffend, ist klar geworden, dass es kaum Schutz vor derlei Angriffen gibt, weder für Privatpersonen noch für Unternehmen. Zu vielfältig sind die Möglichkeiten, zu groß das Budget und zu mächtig die Mittel für diese Organisationen, um an die gewünschten Informationen zu gelangen.

Hier stellt sich zuerst die Frage, ob die Spionage durch Geheimdienste überhaupt als Bedrohung zu sehen ist. Diese Frage muss sich jedes Unternehmen selbst beantworten, es sollte dabei aber bedacht werden, dass die »Förderung der heimischen Wirtschaft mit

nachrichtendienstlichen Mitteln«, wie im Auftrag einer Vielzahl von Nachrichtendiensten zu finden, nichts anderes ist als der Auftrag zur Wirtschaftsspionage – und damit auch von den deutschen »Schlapphüten« betrieben wird. Im Folgenden möchten wir zwei markante Fragen erörtern, um anschließend einen Lösungsimpuls zu liefern:

1.3.1 Was macht mich angreifbar?

Geheimdienste nutzen eine Vielzahl von Methoden, um an Informationen zu gelangen. IT-relevant sind hierbei insbesondere die folgenden:

- Ausleitung von Daten an zentralen Internetknotenpunkten, wie beispielsweise den transatlantischen Glasfaserkabeln

Ein angemessener Schutz der Daten erfordert den Einsatz von wirksamen Verschlüsselungstechnologien. Hierbei ist jedoch darauf zu achten, dass sichere Algorithmen, die durch Geheimdienste nicht oder nur mit sehr hohem Aufwand angreifbar sind, eingesetzt werden. So ist beispielsweise SHA-3 (**Keccak**) als Hash-Algorithmus gegenüber den unsicheren MD5 oder SHA-1 zu bevorzugen, AES256 sollte statt 3DES eingesetzt, PFS für IPSEC-VPNs aktiviert werden, und TLS/SSL-Verbindungen sollten auf RC4 verzichten und Forward Secrecy verwenden. Diese Aufzählung ist allerdings nur exemplarisch und erhebt keinen Anspruch auf Vollständigkeit; mehr dazu in den ENISA-Empfehlungen zu Krypto-Verfahren[66].

- Freiwillige oder erzwungene Datenherausgabe durch kooperierende Unternehmen

Mittlerweile ist klar, dass eine Vielzahl von amerikanischen Unternehmen mit Geheimdiensten kooperiert, und zwar mehr oder minder freiwillig. Grundlage hierfür sind insbesondere National Security Letters (NSL), die im Rahmen des Patriot Act in den USA vom FBI einem Unternehmen vorgelegt werden können und dieses zur Herausgabe von Daten verpflichten. Der NSL unterliegt dabei keinem Richtervorbehalt, und es ist dem Unternehmen untersagt, die Herausgabe der Daten oder auch nur den Erhalt des NSL bekannt zu machen. Somit können Kunden von Unternehmen, die amerikanischer Rechtsprechung – oder der eines Landes mit ähnlicher Gesetzgebung – unterliegen, sich nicht sicher sein, dass die Vertraulichkeit ihrer Daten gewährleistet ist. Es verbleibt somit nur die oftmals nicht praktikable oder den Dienstmehrwert einschränkende Möglichkeit, die Daten zu verschlüsseln oder Anbieter zu wählen, die nicht einer solchen Gesetzgebung unterliegen. Die oft internationale Verstrickung der Anbieter untereinander macht dies jedoch häufig nicht möglich.

Wer mit dem Gedanken liebäugelt, seine Daten in die Cloud zu bewegen – beispielsweise bei US-amerikanischen Cloud-Anbietern –, sollte diesen Punkt ganz besonders intensiv im Hinterkopf verankern. Dabei ist die Lösung einfach: Wer möglichen Herausforderungen entgehen möchte, die durch einen NSL entstehen und somit ausländischen Diensten Einblick in unternehmensinterne Daten ermöglichen, sollte ausschließlich

---

66 *www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report*

Cloud-Anbieter beauftragen, die eine Auftragsdatenverarbeitung in einer EU/EWR-Cloud sicherstellen – außerhalb des amerikanischen Einflussbereichs. Doch auch bei deutschen Anbietern ist man vor Überraschungen nicht gefeit: Ein Datenleck[67] in der Telekom-Cloud ermöglichte beispielsweise Zugriff auf fremde Adressbücher. Grundsätzlich sollte man diese realistischen Szenarien bei der Entscheidungsfindung, Daten in die Cloud zu verlagern oder weiterhin »on premise« zu halten, kritisch betrachten.

- Ausnutzung von Hintertüren in der Software

Aus den von Snowden veröffentlichten Materialien geht hervor, dass Hersteller in Zusammenarbeit mit Geheimdiensten Hintertüren in Software und Verschlüsselungsimplementationen eingebaut haben, um Zugriff auf Daten zu ermöglichen. Die Existenz dieser Hintertüren ist kaum nachweisbar, da der Quellcode in der Regel nicht vorliegt. Da somit alle Closed-Source-Softwarehersteller, die entsprechender Gesetzgebung unterliegen, unter Generalverdacht stehen, verbleibt als offensichtlicher Ausweg nur der Einsatz von Open-Source-Software oder von Anbietern aus unverdächtigen Anbieterländern. Diese beiden Möglichkeiten sind allerdings in der Praxis kaum umzusetzen, da die Prüfung komplexer Open-Source-Software auf Sicherheitslücken sehr aufwendig ist und ein Großteil der wichtigsten Sicherheitsanbieter aus dem amerikanischen Raum stammt. Selbst die Größten der Branche geraten mittlerweile in den Strudel: So belegen neue Ermittlungen, dass der US-Geheimdienst NSA 10 Mio. US-Dollar an RSA Security, einen der wichtigsten US-Anbieter von Sicherheitssoftware, gezahlt hat. Demnach sei das Geld dafür bestimmt gewesen, dass das Security-Unternehmen den umstrittenen Zufallsgenerator Dual_EC_DRBG in die Software BSAFE standardmäßig implementiert. Hiermit sollte eine von der NSA entwickelte Krypto-Backdoor eingebaut werden, wie die Nachrichtenagentur Reuters berichtete.[68] Zwar möchten wir keine Panik schüren, aber vor diesem Hintergrund bekommt die vor Jahren geulkte angebliche Fehlermeldung »Can't find NSA-Backdoor. Please reinstall Windows« eine ganze neue Bedeutung.

- Infiltration des Opfers mit Spionagesoftware

Auch Geheimdienste nutzen das klassische Arsenal von Cyberkriminellen, indem sie ihre Opfer gezielt mit Schadsoftware infiltrieren. Das bekannteste Beispiel in diesem Zusammenhang ist sicher der Stuxnet-Wurm[69], der sich über USB-Wechselmedien auf den Zielsystemen verbreitet hat und – neben einer Manipulation der Leittechnik der Urananreicherungsanlage in Natanz und des Kernkraftwerks Buschehr – erheblichen Kollateralschaden verursachte. Aber auch andere Techniken wie Social-Engineering, Drive-by-Downloads oder Spear-Phishing-E-Mails werden eingesetzt. Die NSA soll beispielsweise weltweit über 50.000 Computernetzwerke mit Schadsoftware infiltriert haben, um an nicht öffentliche Informationen zu gelangen.[70] Die Informationen gehen aus einer Präsentation der NSA aus dem Jahr 2012 hervor, die im Mix aus Über-

---

67 *http://www.wiwo.de/technologie/digitale-welt/deutsche-telekom-neue-brisante-datenlecks-bei-cloud-dienst/14949042.html*

68 *www.reuters.com/article/2013/12/21/us-usa-security-rsa-idUSBRE9BJ1C220131221*

69 Nachfolger: Duqu

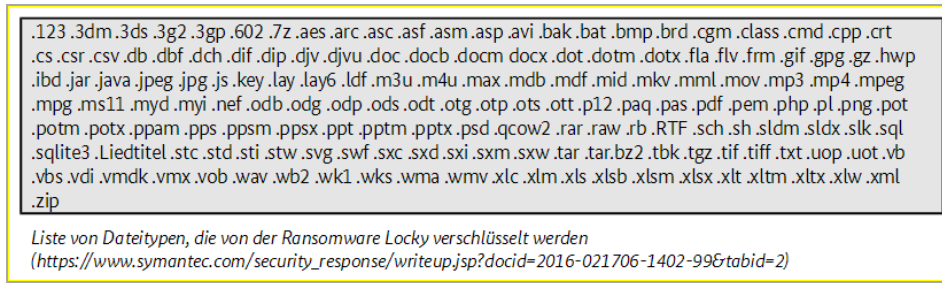
70 *www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software*

wachungsmaßnahmen neben Unterseekabeln und NSA-Standorten auch Zugriffe durch »Computer Network Exploitation« – also ausgespähte Computernetzwerke – nennt.

Für diese Art von Angriffen werden die gleichen Schutzmaßnahmen wie in der traditionellen Cybersecurity empfohlen, also Virenscanner, IPS-Systeme, URL-Filter und Ähnliches. Diese Schutzmaßnahmen sind jedoch prinzipbedingt reaktiver Natur und sollten zwingend durch neue, verhaltensanalysierende Systeme ergänzt werden. Nur so ist ein Schutz, auch vor neuartigen Attacken und APTs, zu gewährleisten.

1.3.2 Datenerpresser – wie Ransomware auch Unternehmen schädigt

In den letzten beiden Jahren hat sich eine Schädlingsgattung explosionsartig vermehrt, die in der Vergangenheit eher auf private Nutzer abzielte, jetzt aber auch verstärkt Unternehmen ins Visier nimmt. Gemeint sind die Erpressertrojaner (Kryptotrojaner) bzw. die Ransomware. Berüchtigt sind hier insbesondere Locky, CryptoLocker, Cryptowall, Teslacrypt, Bart, Zepto, CTB-Locker und andere[71]. Mitte 2015 explodierte die Anzahl der Schädlinge wie auch die der Infektionen, die nicht auf Privathaushalte beschränkt blieben. Unabhängig von der Schädlingsfamilie ist der Ablauf vergleichbar. Die Infektion erfolgt über einen Drive-By-Download mit Exploit-Kits, einen verseuchten E-Mailanhang wie z. B. einer Word-Datei mit Makros oder einen infizierten USB-Stick. Betroffen sind vor allem Windows-Rechner; mittlerweile sind Apple-, Android- und Linuxsysteme ebenfalls betroffen.



Liste von Dateitypen, die von der Ransomware Locky verschlüsselt werden (https://www.symantec.com/security_response/writeup.jsp?docid=2016-021706-1402-99&tabid=2)

Bild 1.31: Ransomware: die wichtigsten Angriffsobjekte

1. Nach der Infektion startet ein Schadprogramm, das alle relevanten Benutzerdokumente verschlüsselt. Die heute hauptsächlich eingesetzten Verschlüsselungstechnologien (AES-256, RSA-2048,ECDH (Elliptic Curve Diffie-Hellman) sind in der Praxis nicht zu überwinden.
2. Es werden auch die Dateien verschlüsselt, die sich auf Netzlaufwerken oder portablen Datenspeichern befinden.

[71] Eine Übersicht vom BSI findet man hier: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.html*

3. Nachdem alle relevanten Dateien verschlüsselt sind, erscheint auf dem Bildschirm die Erpressernachricht mit dem Hinweis, dass Dateien verschlüsselt sind und gegen eine Lösegeldzahlung (meistens Bitcoin) wieder freigeschaltet / entschlüsselt werden. Häufig wird zudem zeitlicher Druck aufgebaut: Falls nicht innerhalb der nächsten Tage gezahlt wird, erhöht sich das Lösegeld bzw. werden die Dateien überhaupt nicht mehr entschlüsselt.
4. Versuche, die Verschlüsselung mit Bordmitteln oder einem von AV-Anbietern bereitgestellten Patch aufzuheben, laufen ins Leere, da die Implementierung der Verschlüsselungsalgorithmen immer perfekter wird.
5. Nach Zahlung des Lösegelds erhält man einen Link, eine Zahlenkombination o.ä., mit dem man seine Dateien wieder entschlüsseln kann.

Der angerichtete Schaden durch dieses »Geschäftsmodell« geht in die dreistellige Millionenhöhe. Was Privatleuten schon den Schlaf raubt, insbesondere wenn sie auf kein Backup zurückgreifen können, zieht bei Unternehmen jede Menge Kollateralschäden nach sich: bei Kunden, Lieferanten, Patienten, Steuerbehörden etc. – nicht zu reden von dadurch verursachten Störungen in der Kette der Leistungserbringung. Für eine Entschlüsselung (von Privat-PCs) werden in der Regel einige hundert Euro fällig. Unternehmensziele (Ämter, Krankenhäuser, Banken etc.) sind wesentlich lukrativer: »Realizing the potential for higher profits, cybercriminals are increasingly targeting the business space. We have seen this trend emerge in other attack campaigns, such as:

- Business email compromise (BEC) scams, which attempt to trick C-level executives into making large wire transfer payments
- Bug-poaching attacks, which involve attackers compro-mising corporate servers, stealing data (as proof of compromise), and requesting a fee for information on how the attack was carried out
- The Carbanak gang, which target banks directly rather than bank customers«[72]

Es wird zwar behördlicherseits immer wieder empfohlen, keineswegs zu zahlen, aber dieser idealistische Appell führt oft ins Leere. Daten sind heute wie Kapital. Wer sich darauf verlässt, dass die IT die Daten vom Vortag wieder einspielt, riskiert den Verlust von bisweilen Hunderten von Arbeitstagen. Sind Produktionsabläufe gestört und weitere Folgeschäden zu erwarten, wird man den Erpressern nachgeben. Ist das Lösegeld bezahlt, können die Opfer im wohlverstandenen Selbstinteresse der Erpresser meistens schnell wieder über ihre Daten verfügen.

Andere Abhilfe ist nicht in Sicht, weshalb es sich für die potenziellen Opfer stets rechnet, geeignete Vorsorge zu ergreifen. Bekanntlich sitzt die größte Schwachstelle zumeist vor dem Rechner. Hier haben Unternehmen durchaus Handlungsbedarf. Schnelle Eingreiftruppen (Incident Response Teams) müssen geschult, spezielle Prozesse initiiert werden, um nicht im Schadensfall vom Chaos überrollt zu werden.

---

72 *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf*, S. 17

Gegen verseuchte E-Mailanhänge wie auch gegen gefährliche Internetlinks kann man technisch zumindest bedingt vorgehen, z. B. mit geeigneten Filtern, die gefährliche Anhänge und Links vom Anwender fernhalten. Eine zusätzliche Sicherheitsmaßnahme sind gehärtete Backup-Prozesse.

1.3.3 Was man gegen IT-Risiken noch tun kann

Zwar ist es möglich, die Gefahren weitestgehend zu adressieren, aber ein umfassender Schutz ist praktisch nur selten durchsetzbar, sodass wir an dieser Stelle lediglich sinnvolle Denkanstöße geben können.

Die Dynamik der Unternehmen erzwingt den Einsatz neuer Technologien und Geschäftsprozesse, deren Sicherheitsimplikationen oft unbekannt sind und die das Unternehmen verwundbar machen. Eine Rückkehr zu traditionellen, leichter kontrollierbaren und somit vermeintlich sichereren Systemen – wie beispielsweise dem Mainframe – ist nur bedingt realisierbar. Der erste Schritt besteht somit darin, sich der potenziellen Risiken bewusst zu werden, diese in Bezug auf die Geschäftsrelevanz zu bewerten und angemessene Sicherheitsmaßnahmen zu etablieren. Das verbleibende Restrisiko muss bestimmt und Strategien müssen definiert werden, wie im Schadensfall vorzugehen ist. Eine professionelle »Incident Response« wird zum entscheidenden Faktor, wenn das Unternehmen Opfer eines Angriffs wurde. Sie setzt sich aus folgenden Schritten zusammen:

1. **Sammeln und Auswerten aller Informationen**
   - Logfiles
   - Monitoringsysteme
   - SIEM-Lösungen
   - Forensik
   - Mitarbeiter befragen
2. **Ermittlung des Schadens, Bestimmung der Situation**
   - Welche Systeme wurden angegriffen?
   - Wurden Daten gestohlen oder manipuliert?
   - Konnten die betroffenen Systeme vom Netz genommen, wiederhergestellt und zurück in die Produktion genommen werden?
   - Welche Auswirkungen hat der Vorfall auf das Unternehmen und auf seine Reputation?
   - Informationspflichten
   - Gesetzliche Veröffentlichungspflichten beachten
   - Bei Verlust von Kundendaten proaktiv informieren
   - Unterstützung bei staatlichen Organisationen suchen

3. **Revision der Sicherheitsstrategie**
   - Ist die Strategie, selbst wenn sie Best-Practice-Empfehlungen entspricht, den aktuellen Anforderungen noch gewachsen?
   - Sensibilisierung des Managements anhand des Vorfalls. Informationssicherheit muss denselben Stellenwert erhalten wie Arbeitssicherheit (Security vs. Safety).
   - Informationssicherheit schützt nicht nur Daten, sondern auch, z. B. im Fall von Industriesteueranlagen (SCADA), das Leben der Bevölkerung.

1.3.4 Welche Sicherheitsarchitektur ist angemessen für mein Unternehmen?

Die Sicherheitsarchitektur vieler Unternehmen gleicht heutzutage leider einem Flickenteppich. Historisch bedingt wurden Systeme aufgebaut, die vor Bedrohungen mit Managementsichtbarkeit schützen oder Anforderungen der Compliance befriedigen sollten. Eine am Geschäftsrisiko orientierte Sicherheitsarchitektur und der Aufbau entsprechender Managementsysteme finden aber erst langsam Einzug in die Unternehmen. Aber oft setzen diese Fortschritte auf dem Status quo auf, ohne diesen zu hinterfragen: Ist ein zwei-, drei- oder x-stufiges Antivirenkonzept noch sinnvoll? Welchen Sicherheitsgewinn bringt eine zweistufige Firewall nach BSI-Empfehlung? Welche Impulse lassen sich aus der ISO 27001 umsetzen? Ein Nicht-Hinterfragen des Etablierten führt zu einer Fortschreibung nicht sinnvoller Unternehmenssicherheitsstandards, zu falscher Budgetierung und trügerischer Sicherheit.

Leider gibt es nicht »die« ideale Sicherheitsarchitektur, die nur integriert werden muss, um fortan sicher zu sein. Es gibt vielmehr eine Vielzahl von Best-Practices, die auf Tauglichkeit für das eigene Unternehmen geprüft werden müssen und sich dann möglicherweise als sinnvoll herausstellen können.

Dazu gehören essenzielle Schutzmaßnahmen sowohl technischer als auch organisatorischer Art:

1. **Technisch**
   - Konsequente Segmentierung des Netzwerks und Schaffung von Zonen mit definierten Vertraulichkeitsstufen
   - Stateful Firewall mit Next-Generation-Features
   - Proxysysteme zur Absicherung des Websurfens
   - E-Mail-Security-Systeme
   - Umfassender AV-Schutz
   - Monitoring-, Reporting- und Logauswertungen
2. **Organisatorisch**
   - Orientierung an einem Standard wie ISO/IEC 27001 oder BSI IT-Grundschutz mit optionaler Zertifizierung.

- Akkurate und vollständige Dokumentation aller Systeme und Prozesse
- Etablierung eines Chief Information Security Officer (CISO), einem Verantwortlichen für Informationssicherheit

Die Position des CISO in der Unternehmenshierarchie kann entweder innerhalb der IT, im Risikomanagement oder direkt unterhalb der Geschäftsführung sein, beispielsweise als Stabsstelle. In der Literatur wird die letzte Variante empfohlen, in der Praxis jedoch sind alle Varianten anzutreffen.

Die Umsetzung dieser Best-Practices allein ist jedoch nicht ausreichend, sondern muss um unternehmensspezifische Sicherheitsmaßnahmen, die sich an den Geschäftsprozessen orientieren, ergänzt werden. Best-Practices stellen hierbei die Summe von Erfahrungen mit einer Technologie dar. Dies erfordert einen Reifungsprozess über einen Zeitraum, der zu lang ist, um aktuellen geschäftskritischen Bedrohungen zu begegnen. Ein Unternehmen darf sich heute nicht mehr nur auf die etablierten Methoden verlassen, sondern muss die eigene Sicherheitsarchitektur um individuelle Sicherheitsprozesse und -lösungen ergänzen. Sicherheit muss dabei vom Management als strategisches Thema gesehen werden, und die Sicherheitsbeauftragten müssen hinreichend ermächtigt werden. Der Verantwortliche für Informationssicherheit muss hierzu in jedes relevante Projekt frühzeitig mit eingebunden werden und über ein Vetorecht verfügen.

Der CISO darf selbstverständlich nicht nur ausschließlich für technische Themen konsultiert werden. Bereiche wie Mergers & Acquisitions sind ebenso relevant für die Informationssicherheit wie unterschiedliche Compliance-Anforderungen aus den Fachabteilungen – und selbst das wäre oftmals nur der berühmte Tropfen auf den heißen Stein, wie persönliche Erfahrungen aus Beratungsprojekten zur Weiterentwicklung der Informationssicherheit im Mittelstand belegen. Weitere Hinweise zur Entwicklung der Informationssicherheit lassen sich dem letzten Kapitel dieses Buchs, »Company Networking«, entnehmen.

Teil I: Tools: Werkzeuge für Angriff und Verteidigung

Wir stellen hier einige Tools vor, mit denen man relativ schräge Dinge machen kann. Aber denken Sie daran: Wenn Sie unsere Experimente praktisch nachvollziehen wollen, sollten Sie vorab einige Sicherheitsüberlegungen anstellen. Der wichtigste Punkt betrifft Ihre eigene Sicherheit. Etliche der hier vorgestellten Tools fallen, zumindest aus der Sicht von Virenscannern, ziemlich eindeutig in die Kategorie Malware. Praktisch gesprochen: Allein schon auf der Suche nach den Tools gehen Sie das Risiko ein, infiziert zu werden. Da viele dieser Tools nur im Darknet zu finden sind, wissen Sie nie genau, ob sie nicht mehr Funktionen bereithalten, als Ihnen lieb ist.

Wenn Sie jetzt denken, dass Sie prinzipiell sehr gut gerüstet sind und die zuverlässigsten und neuesten Antimalware-Tools, Firewalls etc. installiert haben, kommt schon die nächste Ernüchterung. Die meisten Hackertools lassen sich nur dann zur Zusammenarbeit bewegen, wenn Sie Ihr Visier hochklappen. Aktivierte Firewalls oder Online-Virenwächter werden Ihnen im schlimmsten Fall die Tools schneller löschen, als Sie diese aus dem Internet runterladen; mindestens aber werden sie Sie wirkungsvoll vom Experimentieren abhalten und entsprechende Aktionen der Hackertools deaktivieren. Halten Sie das bitte nicht für eine Übertreibung. Ich (PK) hatte eine schöne Sammlung von Schädlingen für weitere Experimente auf meiner Festplatte versammelt. Als ich kurze Zeit später darauf zugreifen wollte, waren die meisten davon nicht mehr vorhanden. Ein Antivirustool hatte sie umbenannt und in Quarantäne verschoben. Als ordentlicher Mensch hatte ich natürlich ein Backup gemacht. Aber als ich jetzt die Verzeichnisse öffnen wollte – das alte Spiel, wieder war alles weg. Deshalb müssen Sie im Prinzip drei ziemlich widersprüchliche Ratschläge befolgen:

- Laden Sie Hackertools nur von vertrauenswürdigen Quellen – es gibt durchaus Hacker- oder Security-Seiten wie *http://packetstormsecurity.org* oder *www.exploit-db.com* (The Exploit Database, EDB), die es sind.
- Prüfen Sie, bevor Sie die Dateien anklicken, ob nicht mehr Malware an Bord ist, als da sein sollte.
- Deaktivieren Sie fallweise Ihren Online-Schutz, um die Tools in ihrer gesamten Bandbreite testen zu können (und lassen Sie hinterher einen oder mehrere Scanner über Ihr System laufen).

Wir raten dringend an, dass Sie diese Tests nur auf einer in sich gekapselten virtuellen Maschine ausführen, z. B. von VMware; ersatzweise tut es auch eine separate bootfähige Festplatte, die Sie nach den Experimenten mit einem Imagebackup wieder in den ursprünglichen Zustand zurückversetzen. Berücksichtigen sollten Sie hierbei auch

weitere im Netzwerk befindliche Rechner, natürlich auch den Zugang zum Internet: Starten Sie einen aktuellen Wurm und sind die restlichen Maschinen Ihres Netzwerks verwundbar, dann eskaliert das ursprünglich zu wissenschaftlichen Zwecken angedachte Szenario zu einem GAU.

Eine letzte Warnung müssen wir Ihnen auch noch mit auf den Weg geben. Die meisten der hier vorgestellten Tools – auch wenn sie etwas angejahrt sind – haben ein (immer noch) erhebliches Angriffspotenzial mit der realen Möglichkeit, weniger gut geschützte Systeme bzw. deren Anwender zu schädigen. Das wiederum ist *kein* Kavaliersdelikt, sondern kann zu strafrechtlichen Konsequenzen führen. Wenn Sie aus Gründen der besseren Nachvollziehbarkeit kontrollierte Angriffe starten wollen, dann bitte ausschließlich in Ihrem eigenen Netzwerk oder nach vorheriger Rücksprache mit Ihren »Testkandidaten«.

Was die aktuelle Werkzeugsammlung betrifft: Sie finden hier unterteilt in zehn Rubriken Tools aus der Windows- und der Linux-/Unix-Welt. Unsere Auswahl ist natürlich subjektiv. Wir haben die Programme ausgewählt, mit denen wir in der Praxis gearbeitet haben und noch arbeiten. Darunter sind sehr gängige Werkzeuge wie Nmap, OpenVAS oder das Metasploit Framework, aber auch ausgefallenere Tools wie USBDUMPER2 und der Stealth Recorder. Bei den kommandozeilenbasierten Linux-Tools haben wir relevante Eingabeparameter und auch das Ausgabeformat in den meisten Fällen vollständig aufgelistet. Wem die Routine mit diesen Tools fehlt, der hat somit gleichzeitig auch ein kleines Nachschlagewerk parat. Wir wünschen Ihnen viel Freude beim Testen und bei der Netzwerkerforschung.

Bei der Überarbeitung ist uns ein unliebsamer Effekt begegnet: Innerhalb weniger Wochen können die »Lieferadressen« von Underground-Tools (selbst wenn sie älteren Ursprungs sind) einfach von der Bildfläche verschwinden. So geschehen mit USB Switchblade bzw. 7zBlade. Wir haben uns bemüht, gültige Bezugsquellen anzugeben. Es liegt aber in der Natur der Sache, dass die Halbwertszeit dieser Seiten beschränkt ist. Im Zweifelsfall, der hoffentlich Einzelfall bleiben wird, werden Sie selbst also nach bestimmten hier vorgestellten Tools über die Suchmaschine Ihrer Wahl suchen müssen.

Noch eine letzte Anmerkung zum Stichwort »Redundanz«. Den hier aufgeführten Tools werden Sie zum großen Teil (aber nicht ausschließlich) in unseren Angriffsszenarien begegnen – und sie im konkreten Angriffskontext erleben. Aber wir werden dort wie auch beim Thema Prophylaxe einige weitere Werkzeuge benutzen, die Sie hier nicht finden, weil wir diesen Rahmen nicht sprengen wollten. Es geht uns weniger um die Tools, die in bestimmten Zusammenhängen austauschbar sind, als vielmehr um die konkrete Durchführung und das dafür notwendige Know-how.

2 Keylogger: Spionage par excellence

Der Begriff »Keylogger«, auf Deutsch: Tastaturrekorder, klingt auf den ersten Blick eher harmlos. Keylogger sind aber eine der größten Gefahren, denen sich Privatpersonen und Firmen heute ausgesetzt sehen. Keylogger existieren als Hardware- und als Softwareausführung.[73] Ihr Zweck ist derselbe – alles aufzuzeichnen, was der Anwender auf der Tastatur seines PCs eingibt:

- CMOS-Passwörter
- Benutzeraccounts
- PIN-/TAN-Kombinationen fürs Online-Banking
- Log-in-Daten für diverse Webdienste (E-Mail-Accounts, Forenanmeldungen etc.)
- Passwörter zum Verschlüsseln von Festplatten, Verzeichnissen, Dateien
- Zusätzlich natürlich alle Texte in Eingabemasken, Formularen, Chatrooms etc.

Manche Keylogger speichern auch Screenshots, damit der Angreifer auch die anderen visuellen Aktivitäten seiner Opfer mitverfolgen kann. Besonders heimtückisch sind Keylogger, die als Hardwaremodul zwischen Tastatur und Rechner eingeschleift werden und dabei alle Daten von der Tastatur mitschneiden, bevor sie über das Betriebssystem an das jeweilige Anwenderprogramm übergeben werden. Die Softwarefraktion geht einen anderen Weg: Meist wird hier ein Treiber installiert – vorzugsweise auf Kernelebene – der vom Benutzer völlig unbemerkt alle Eingaben abfängt, aufzeichnet und dann an das jeweilige Programm übergibt. Die Keylogger, die wir hier vorstellen, sind Stand-alone-Produkte. Daneben findet sich die Funktionalität von Keyloggern auch in diversen Malware- und Spywareprogrammen, insbesondere in Trojanern und RATs (Remote Access Tools). Die Funktionalität der SW-Keylogger ist ziemlich ausgereift. So gibt es Programme, die nicht nur Sessions mitschneiden (mit Screenshots oder auch als kleine Filme), Tastatureingaben protokollieren, die Eingaben verschlüsseln und ihre Spuren mittels Rootkits tarnen, sondern auch Spezialentwicklungen, um gezielt Daten auszulesen und diese dann durch die Firewall nach außen schmuggeln zu können.

Keylogger lassen sich natürlich auch zu Verteidigungszwecken nutzen, beispielsweise um Betrugsfällen und dem Ausspionieren von Firmengeheimnissen auf die Spur zu kommen. In Deutschland fallen diesbezügliche Aktivitäten (im Übrigen wie fast alle hier

---

73 Eine gute Übersicht über die »besten« Softwarekeylogger findet man hier: *www.keylogger.org/monitoring-software-review*

beschriebenen Tools) unter das Strafgesetzbuch § 202a – Ausspähen von Daten – und sind damit strafbewehrt bzw. nur in geregelten Ausnahmefällen zulässig.

2.1 Logkeys

Anbieter	*http://code.google.com/p/logkeys*			**Preis**		–		
Betriebssystem(e)	Linux/Unix			**Sprachen**		Englisch		
Kategorie(n)	Keylogger			**Oberfläche**		**GUI**		**CMD** x
Größe	< 1 MB	**Installation/ Kompilation**		Nein/ Ja	**Schnittstellen**			
Usability	■■■□□			**Know-how**		■■■□□		

Bei *Logkeys* handelt es sich um einen Keylogger für Linux, der sowohl auf seriellen als auch auf USB-Tastaturen läuft. Logkeys erfasst und protokolliert sämtliche Eingaben, die auf der Tastatur eingegeben werden. Logkeys übersetzt die eingegebenen Zeichen in das ASCII-Format.

Der Einsatz von Logkeys mit den Parametern

- `-s start logging keypresses`
- `-o log output to FILE [/var/log/logkeys.log]`

bringt durch die Eingabe von `logkeys --start --output /var/log/logkeys.log` z. B. folgendes Ergebnis:

```
sh-3.2# cat /var/log/logkeys.log
Logging started ...

2010-03-10 19:35:18+0000 > uname -a
2010-03-10 19:35:35+0000 > ps -aux
2010-03-10 19:46:46+0000 > useradd -m hweber
2010-03-10 19:46:55+0000 > passwd hweber
2010-03-10 19:47:22+0000 > maxtor19<LShft>!
2010-03-10 19:47:29+0000 > maxtor19<LShft>!
(...)
2010-03-10 19:47:47+0000 > aptitude update
2010-03-10 19:48:05+0000 > exit
sh-3.2#
```

Bild 2.1: Logkeys beim Aufzeichnen von Tastatureingaben

2.2 Elite Keylogger

Anbieter	*www.widestep.com*			**Preis**	Trial, ab 49 €			
Betriebssystem(e)	Windows			**Sprachen**	Englisch			
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 5 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■■□□			

Nach unseren Tests gehört der *Elite Keylogger* V. 5.3 (Stand 2013) nach wie vor zu den besten (Funktionalität) und technologisch fortgeschrittensten Vertretern seiner Art. Er zeigt, was heute in dem Bereich machbar ist, um selbst misstrauische und erfahrene PC-Anwender unbemerkt und effektiv auszuspionieren. Da es sich beim Elite Keylogger um ein kommerzielles Produkt handelt, ist er ziemlich gut getarnt vor den meisten Viren- und Malware-Scannern. Sein Tarnmantel ist so gut, dass er mit herkömmlichen Betriebssystemmitteln nicht entdeckt werden kann. Die einzige Möglichkeit, ihm beizukommen, ist der Einsatz von Anti-Rootkit-Software.

Besonders hervorzuheben ist seine Fähigkeit, die protokollierten Daten applikationsspezifisch auswerten zu können, d. h., man sieht auf einen Blick, welche Briefe in Word geschrieben, welche Tabellen in Excel angelegt, welche E-Mails mit welchen Inhalten verschickt bzw. in welchen Chats welche Dialoge geführt wurden. Das erleichtert die Auswertung nicht unbeträchtlich. Ein herausragendes Feature ist die Verteilung der Logs auf andere Rechner im Netz. Man muss sich nicht mehr per E-Mail informieren lassen (und gegebenenfalls verdächtige Meldungen der Firewall riskieren), um in aller Ruhe Daten sammeln und auswerten zu können. Der fürs Unsichtbarmachen zuständige Kerneltreiber wird in regelmäßigen Abständen aktualisiert.

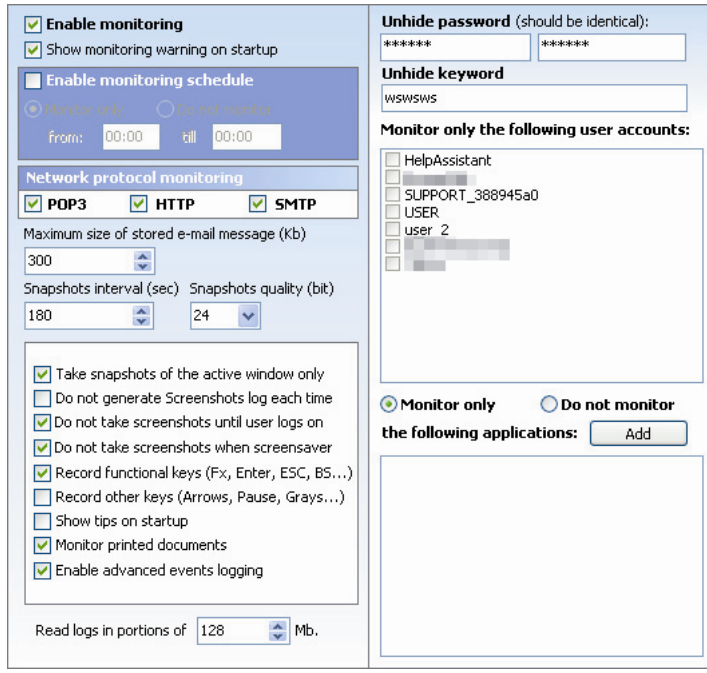


Bild 2.2: Komfortabel und unsichtbar

2.3 Ardamax Keylogger

Anbieter	*www.ardamax.com*			**Preis**		Trial, ab 44,95 €		
Betriebssystem(e)	Windows			**Sprachen**		Englisch		
Kategorie(n)	Keylogger			**Oberfläche**		**GUI**	x	**CMD**
Größe	> 5 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■■□□			

Nicht vom Leistungsumfang, wohl aber von der Dateigröße einer der kleinsten (und unauffälligsten) Keylogger. Die Bedienung ist sehr simpel; in wenigen Minuten ist der Keylogger konfiguriert und unsichtbar gemacht. Zwei Highlights haben uns besonders gut gefallen:

- Die Möglichkeit, ein Remote- bzw. Servermodul zu konfigurieren, das man z. B. mit einem anderen nützlichen Programm bündeln und einem ahnungslosen Opfer zuschicken kann. Vorteil: Man muss den Keylogger nicht vor Ort installieren.
- Die Eingabe eines künstlichen Verfalldatums. Das kann sehr nützlich sein, wenn man sein Opfer nur über eine definierte Zeitspanne überwachen kann oder muss. Danach deinstalliert sich das Programm völlig unbemerkt.

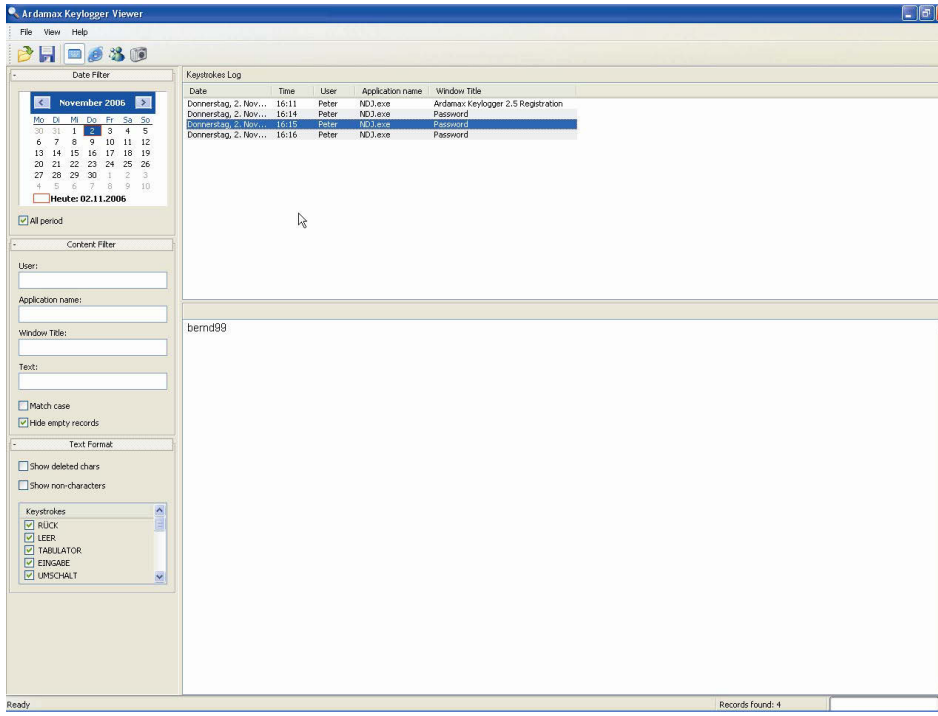


Bild 2.3: Auswertungsfenster Keylogger

Die Logs sind verschlüsselt; man kann sie sich als HTML-Report per E-Mail zuschicken oder über einen FTP-Server bzw. relativ leicht übers LAN an eine geheime Adresse verschicken lassen.

2.4 Stealth Recorder Pro

Anbieter	Über Distributor lieferbar, z. B. *http://stealth-recorder-pro.en.softonic.com/*		**Preis**	Trial, ab 22,21 $			
Betriebssystem(e)	Windows		**Sprachen**	Englisch			
Kategorie(n)	Keylogger		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 500 KB	**Installation**	Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**	■■■□□			

Eigentlich kein Keylogger im strengen Sinn des Wortes, sondern eine Audiowanze mit verblüffendem Funktionsumfang. Ziel des Angriffs sind Gespräche, die in der Nähe des Rechners oder Notebooks geführt werden. Eigene Tests ergaben, dass selbst mit einem günstigen Notebook alles aufgezeichnet werden kann, was im Umkreis von mehr als 10 m

gesprochen wird. Möglich wird dies durch eine neuartige Boostertechnologie, die den Input eines handelsüblichen Mikrofons um mehr als das 100-Fache verstärken kann.

Die Software zeichnet – in Abhängigkeit des gewählten Umgebungspegels – jedes gesprochene bzw. geflüsterte Wort im mp3-Format (unterschiedliche Qualitätsstufen wählbar) auf und versendet diese Dateien per E-Mail oder FTP. Ein besonderes Schmankerl ist die Fernabfragemöglichkeit. Dadurch ist es einem Angreifer von außen möglich, über einen definierten Port auf die MP3-Dateien zuzugreifen. Man muss die Software nicht unbedingt einem potenziellen Opfer aufs Notebook oder den Rechner packen, sondern kann sie auf seinem eigenen Notebook installieren und in Meetings platziert einsetzen. Bei vielen Notebooks besteht ja der Vorteil darin, dass man kein separates Mikrofon braucht, sondern dieses bereits eingebaut ist.

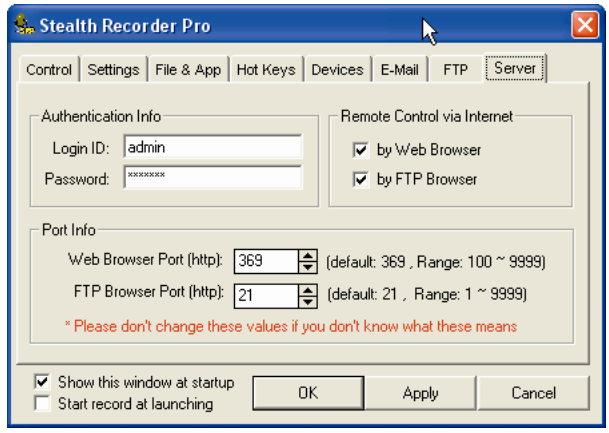


Bild 2.4: Zugriff auf die Audiowanze von außen

2.5 Advanced Keylogger

Anbieter	*www.mykeylogger.com/de*			**Preis**	49,95 € (Demo verfügbar)			
Betriebssystem(e)	Windows			**Sprachen**	Deutsch			
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 15 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■□		**Know-how**		■■■□□			

Ein eigenständiges Hackerprodukt mit gewissen Vorzügen. Z. B. kann man den erzeugten Remote-Installer noch mit einem anderen, harmlosen Produkt, z. B. einer kleinen Videodatei, bündeln, damit das Opfer keinen Verdacht schöpft. Zusätzlich kann man die Abhöraktion zeitlich begrenzen, quasi mit einem Verfalldatum versehen, was die Gefahr, entdeckt zu werden, ebenfalls minimiert.

Bild 2.5: Keylogger als Komfortpaket

Vom selben Anbieter gibt es jetzt den »Powered Keylogger« mit größerem Funktionsumfang (€ 69,95)

2.6 Hardware-Keylogger

Anbieter	*ebay.com* oder *keelog.com*			**Preis**	ab 45,00 €			
Betriebssystem(e)	unabhängig			**Sprachen**	Englisch			
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 2 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■■□□			

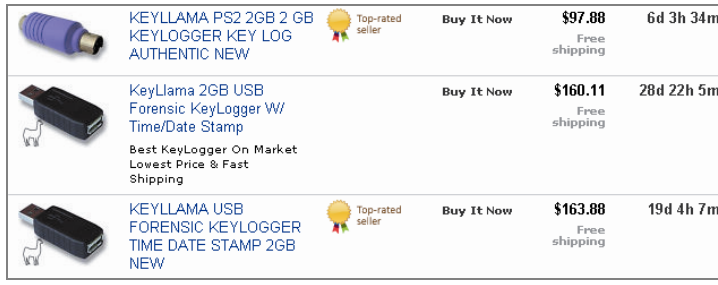


Bild 2.6: Hardware-Keylogger bei eBay

Hardware-Keylogger können wahlweise am PS2- oder am USB-Port des Zielrechners eingeschleift werden. Optional gibt es auch Module, die nachträglich in die Tastatur ein-

gebaut werden, oder spezielle Tastaturen. Da diese Keylogger auf Hardware basieren, können sie mit keiner Software entdeckt werden. Sie speichern je nach Ausführung bis zu einige Millionen Zeichen inklusive CMOS-Passwort, Verschlüsselungscodes für die Festplatte etc. Wenn man sie wieder vom Rechner abzieht, können sie später in geschützter Umgebung mit einem mitgelieferten Programm oder einem simplen Texteditor ausgelesen werden. Weiterentwickelte Hardware-Keylogger können die aufgezeichneten Tastaturschläge auch direkt per Funk versenden.

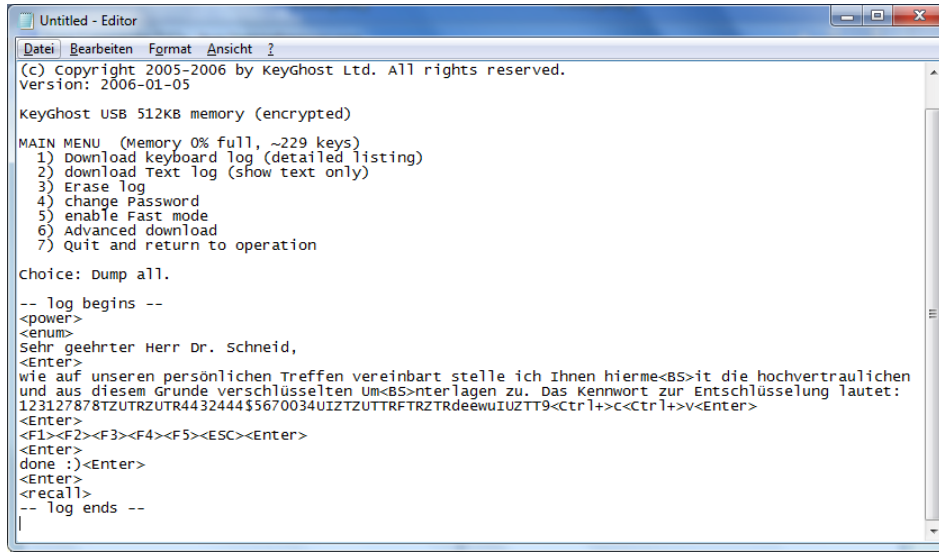


Bild 2.7: Auslesen des Hardware-Keyloggers

Hardware-Keylogger zählen zu den gefährlichsten Spionagetools, weil sie a) einfach und preiswert zu beschaffen, b) schnell zu installieren und c) relativ einfach auszuwerten sind. Außerdem helfen sie, den Verschlüsselungsschutz von Festplatten mit PBA (Pre Boot Authentication) zu brechen. Die Abwehrmöglichkeiten sind beschränkt: Eine »Clean-Desk-Policy«, die visuelle Inspektion des Rechners in regelmäßigen Abständen und der Einsatz von Smartcards und Tokens in Kombination mit einer Festplattenverschlüsselung können helfen, den Schaden zu begrenzen.

2.7 Abwehr – generelle Tipps

Grundsätzlich sind bei den Abwehrstrategien zwei Szenarien zu unterscheiden: Prophylaxe auf der einen und Unschädlichmachen auf der anderen Seite. Im ersten Fall droht der unmittelbare Angriff von Keyloggern, im zweiten Fall ist er bereits erfolgt.

Hardware-Keylogger abzuwehren ist eine der anspruchsvollsten Verteidigungsmaßnahmen, da hier allein mit Software wenig auszurichten ist.[74] In der Praxis kommen prinzipiell nur drei Maßnahmen in Betracht:

1. **Physikalische Schutzmaßnahmen**
   Sensible PCs werden vor feindlichen Zugriffsversuchen physisch geschützt (z. B. durch Personenkontrolle, Wegschließen etc.), bzw. die Hardware (PC-Gehäuse und Peripherie wie Tastaturen etc.) wird regelmäßig auf Manipulationen untersucht.

2. **Festplattenverschlüsselung mit Pre Boot Authentication via Chipkarte, USB-Stick etc. (2-Faktoren-Authentifizierung)**
   Diese Maßnahme verhindert, dass das Startpasswort ausgespäht und damit die Bootkontrolle über den PC übernommen werden kann, da grundsätzlich nur die Tastatureingabe, aber nicht der Hardwareschlüssel der Chipkarte mitprotokolliert werden kann.

3. **Einsatz virtueller, mausgesteuerter Tastaturen & Passwortsafes**
   Hardware-Keylogger speichern nur reale Tastendrücke, aber keine Mausbewegungen bzw. Mausklicks und keine Inhalte der Zwischenablage.

Ohne physikalische Absicherung bleiben die Maßnahmen 2 und 3 allerdings Stückwerk. Man wird zwar mehr oder weniger zuverlässig das Ausspähen von Anmeldekennungen und Passwörtern verhindern können, schwerlich aber die Kompletteingabe größerer Textmengen, da virtuelle Tastaturen nicht für die Eingabe größerer Textmengen gedacht sind.

Softwarebasierte Keylogger sind zwar grundsätzlich einfacher abzuwehren, bergen aber auch größere Gefahrenpotenziale (breitere Einsatzmöglichkeiten, fast unbeschränkte Speichermöglichkeiten, Fernzugriff, auch von Laien leicht einzusetzen). Ist der PC verschlüsselt bzw. der Zugang physikalisch erschwert, kommen als Infektionsquellen nur speziell präparierte Datenträger (CD, DVD, USB-Sticks, Festplatten etc.) oder verseuchte Webseiten und Mailanhänge in Betracht. Da im Bereich der Industriespionage häufig dedizierte Lösungen eingesetzt werden, laufen gängige signaturbasierte Malware-Scanner häufig ins Leere. Zu bedenken ist auch, dass kommerziell vertriebene Versionen wie z. B. der Advanced Keylogger nach der Installation von klassischen Malware-Scannern[75] gerne »übersehen« werden, da es sich um »legale« Produkte handelt. Hier helfen dann Speziallösungen[76] wie der kernelbasierte Anti Keylogger Elite, der auch unbekannte Keylogger in Echtzeit schachmatt setzt. Schwächer sind virtuelle Tastaturen (da auch Mausbewegungen in Kombination mit Screenshots aufgenommen werden können). Einfache Lösungen, um das Ausspähen von Kennungen und Passwörtern via Internetbrowser zu erschweren, sind Add-ons wie Key Scrambler & Co.

---

74 Ausnahme: USB-Keylogger, vgl. Aufsatz »Detecting Hardware Keyloggers« by Fabian Mihailowitsch; Download unter: *http://de.wikipedia.org/wiki/Keylogger*

75 Gnadenlos versagt haben hier: Avast, Malwarebytes, TDSSL, SUPERAntiSpyware, Threatfire, Spybot – Search & Destroy

76 Manchmal tut es auch ein simples Tool wie der KL-Detector, um eine Spur aufzunehmen: kostenlos unter: *http://kl-detector.de.uptodown.com*

Da die Softwareprophylaxe immer einem gewissen Unsicherheitsfaktor unterliegt, sollten fortschrittliche Diagnosetechniken wie Anti-Rootkits, Netzwerkmonitore, IDS etc. eingesetzt werden. Eine weitere simple Möglichkeit ist der Ausbau einer verdächtigen Bootpartition/-platte. Da hier kein Rootkit mehr die protokollierten Mitschnitte schützt, kann man eine datumsbasierte Dateisuche starten (größere Dateien der letzten Tage), um Protokolldateien von Keyloggern zu entdecken. Sind diese Dateien nur auf der ausgebauten Platte zu entdecken, nicht aber im laufenden Betrieb, kann man mit einiger Sicherheit davon ausgehen, dem Übeltäter auf die Schliche gekommen zu sein.

Glossar

Academic Signature
Ein Verschlüsselungstool auf der Basis von elliptischen Kurven (ECC = Elliptic Curve Cryptograph) für das Erzeugen und Überprüfen von Signaturen und die asymmetrische Datei-Verschlüsselung.

AES-128
Zum Verschicken verschlüsselter Texte und verschlüsseltem Telefonieren sowie für anonymes Surfen über ein VPN.

APT-Angriffe
Advanced Persistent Threads (APT) sind Versuche, kritische IT-Strukturen gezielt und permanent zu kompromittieren.

Ardamax Keylogger
Ein von der Dateigröße her kleiner, aber leistungsstarker Keylogger. Die Bedienung ist einfach. In wenigen Minuten ist der Keylogger konfiguriert und unsichtbar gemacht.

Audiowanze
Ein Audiorecorder greift mithilfe eines PCs akustische Informationen ab. Typische Vertreter wie der Total Recorder können zwar auch Aufzeichnungen von angeschlossenen Mikrofonen machen, aber nicht unbemerkt im Hintergrund aufzeichnen, geschweige denn die Audioprotokolle in festgelegten Abständen zum Angreifer senden.

Bad Exit Nodes
Austrittspunkte, an denen die Informationen im Klartext vorliegen, sofern diese nicht SSL- oder TLS-verschlüsselt sind.

Behaviour Blocker
AV-Scanner, die gestartete Programme nach einem definierten Regelset beobachten. Zeigen diese ein auffälliges Verhalten, beispielsweise Kernelaktivitäten oder Querzugriffe auf andere Programmressourcen, werden sie blockiert.

Big Data
Global abfischbare Daten, unabhängig von Freund-Feind-Überlegungen, werden verstaatlicht und nach Wohlwollen und politischen Opportunitätsgesichtspunkten neu verteilt.

Bleachbit
Ein Systembereinigungs-Tool, das den Rechner von so gut wie allen Spuren befreit.

Bot-Netze
Sie dienen unterschiedlichen Zwecken, angefangen mit der Funktion als Spam-Schleudern, über den Klick-Betrug bis hin zu konzentrierten Angriffen auf Webseiten (DDOS-Attacken).

BTF-Sniffer
Wenn man »nur« mal sehen will, was der Mitarbeiter oder Kollege an seinem Rechner so treibt, kann man das mit dem BTF-Sniffer tun. Eines der »besten« offiziellen Überwachungstools und Freeware.

Cain & Abel
Der in Software gegossene Albtraum von Systemverwaltern und Netzwerkadministratoren. Der Passwort-Sniffer und -Cracker kommt sehr schnell zur

Sache. Selbst Admin-Passwörter können über verschiedene Methoden inklusive des Einsatzes von Rainbow Tables geknackt werden.

Canvas Fingerprinting

Beim Besuch einer Website wird dem Browser mittels Javascript ein versteckter Text übergeben. Anhand der Verarbeitung ergibt sich ein »relativ« eindeutiger Fingerprint.

Chipdrive Smartcard Office

Wer den Umgang mit Zertifikaten, Zertifikatspeichern, Private Keys und Public Keys scheut und eine deutschsprachige Oberfläche bevorzugt, findet mit dem Chipdrive-Produkt eine angemessene Lösung. Chipdrive erfordert die Anschaffung eines Kartenlesers. Auch fürs E-Banking ist der Reader eine Option, zumal er von den meisten Experten als die einzig wirklich sichere Lösung für diesen Zweck angesehen wird.

Clean-Desk-Policy

Die visuelle Inspektion des Rechners in regelmäßigen Abständen und der Einsatz von Smartcards und Tokens in Kombination mit einer Festplattenverschlüsselung können helfen, Schaden zu begrenzen.

CMOSPwd

Ein einfaches, aber wirkungsvolles Werkzeug, um die Kontrolle über einen fremden PC zu erlangen, ohne dass dafür ein Keylogger eingesetzt oder zum Schraubenzieher gegriffen werden muss. Einzige Voraussetzung ist, dass der PC sich booten lassen muss.

De-CIX

Der größte Internetknoten der Welt, De-CIX in Frankfurt, war seit 2008 im Fadenkreuz des BND und indirekt auch der NSA.

Defacement

Als Defacement bezeichnet man in Hackerkreisen das Entstellen (engl. = de-face) bzw. Verunzieren von fremden Webseiten. Manche Hacker haben daraus ein richtiges Hobby gemacht und verewigen sich mit ihren Kunstwerken dann im Digital Attacks Archive auf *www.zone-H.org*.

Distributed Password Recovery

Linear skalierbarer Passwort-Cracker, der bis zu 64 CPUs oder Prozessorkerne sowie bis zu 32 GPUs in einem Rechner unterstützt.

DNS-Leaktest

Ein Online-Test, der DNS-Leaks erkennt und das VPN absichert.

Drive-by-Exploits

Sicherheitslücken auf den Opfer-PCs werden gezielt ausgenutzt und Schadsoftware mittels entsprechender Browser-Plugins ausgeführt.

Driftnet

Bei dem bereits im WLAN-Kapitel kurz vorgestellten Driftnet handelt es sich um ein Tool, das den Netzwerkverkehr abhört und alle übertragenen Bilder bequem auf dem Rechner des Angreifers anzeigt.

DoS- und DDoS-Attacken

Attacken auf die Verfügbarkeit eines Netzsystems, z. B. den Internetauftritt eines Markenanbieters. Ziel dieser Angriffe ist es, den Zielserver so zu überlasten, dass er keine Dienste (nach außen) mehr anbieten kann. Auf diese Weise sollen Erpressungsversuche unter-

mauert oder die Infrastruktur eines politischen Gegners geschädigt werden.

DSniff-Suite

Eine Sammlung wertvoller Tools, die das Herz des Netzwerkforschers höher schlagen lassen.

Elite Keylogger

Kommerzieller Keylogger, der die Eingaben des Benutzers protokolliert. Gut getarnt vor den meisten Viren- und Malware-Scannern. Sein Tarnmantel ist so gut, dass er mit herkömmlichen Betriebssystemmitteln nicht entdeckt werden kann – außer mit Anti-Rootkit-Software.

Ende-zu-Ende-Verschlüsselung

Auch wenn der Text ausgetauschter E-Mails verschlüsselt ist, kann der dem Betreiber bekannte Inhaber immer noch über die Meta-Daten ausspioniert werden. So wissen Cyberkriminelle, Internetprovider, aber auch die Dienste, wer mit wem wie oft und wie intensiv in Kontakt getreten ist.

Essential NetTools

Umfassendes Netzwerkanalysetool mit Anzeige ankommender und ausgehender Verbindungen.

EverCookies

Von der Werbewirtschaft speziell für diejenigen entwickelt, die normale Tracking-Cookies blockieren. Sie zeichnen sich dadurch aus, dass sie aus mehreren Komponenten bestehen, die sich nach einer Cookie-Löschaktion selbst wieder restaurieren.

Geolokation

Klingt harmlos, kann aber den sicheren Tod bedeuten, den z. B. zwei deutsche Staatsbürger am 4.10.2010 in Pakistan erlitten. Es gilt als zweifelsfrei erwiesen, dass eine Hellfire-Rakete mittels IMSI-Catcher ein Mobiltelefon mitsamt IMEI und IMSI orten und es samt Benutzer zerstören kann.

Handy-Scrambler

Ein externes Zusatzgerät, das die Telefonate verschlüsselt. Für die Verschlüsselung ist ein MDP2-ASIC-Chip zuständig, der Sprache in Rauschen umwandelt,

Hardware-Keylogger

Können wahlweise am PS2- oder am USB-Port des Zielrechners eingeschleift werden. Optional gibt es auch Module, die nachträglich in die Tastatur eingebaut werden, oder spezielle Tastaturen. Da diese Keylogger auf Hardware basieren, können sie mit keiner Software entdeckt werden.

Hashcat

Ein GPGPU-basierter, multi-Hash-fähiger Passwortknacker der besonderen Art. Zum einen überzeugt er mit Geschwindigkeit, zum anderen versteht sich das Programm auf ein wahres Feuerwerk von über 160 unterschiedlichen Algorithmen.

Hydra

Ein Passwort-Cracker, der mittels Wörterbuchattacke versucht, die Kennwörter entfernter Log-ins verschiedenster Dienste zu ermitteln. Hydra zeichnet sich durch die Möglichkeit aus, parallele Attacken auf diverse Dienste zu fahren.

I2P

Invisible Internet Project gehört zu den anonymen P2P-Netzwerken, in denen der Datenverkehr mehrfach verschlüsselt über wechselnde Stationen des Netzes geleitet wird.

iKey
Kompaktes 2-Faktoren-Authentifizierungstoken, das manipulationssicher ist und die Generierung und Speicherung von Schlüsseln sowie die Verschlüsselungsfunktionalität und den Support für digitale Signaturen übernimmt.

IMSI-Catcher
Erlaubt Strafverfolgern sowie Nachrichtendiensten das Mithören und Mitschneiden der gesamten Mobilfunkkommunikation im Erfassungsbereich des IMSI-Catchers.

John the Ripper
JtR ist ein sehr universeller und schneller Passwortknacker, der für sehr viele Betriebssystemplattformen verfügbar ist.

Keylogger
Auf Deutsch, Tastaturrekorder, sind eine der größten Gefahren, denen sich Privatpersonen und Firmen heute ausgesetzt sehen. Ihr Zweck ist, alles aufzuzeichnen, was der Anwender auf der Tastatur seines Rechners eingibt.

Kismet
Extrem leistungsfähiger passiver WLAN-Sniffer zum Aufspüren von Funknetzen, der auch in der Lage ist, versteckte Hotspots zu entdecken.

Lanspy
Leistungsfähiger und schneller IP-Scanner, der sowohl zur Analyse des eigenen Netzwerks als auch externer Netzwerke eingesetzt werden kann. Die Scanergebnisse werden in sehr übersichtlicher Form präsentiert.

Logkeys
Bei Logkeys handelt es sich um einen Keylogger für Linux, der sowohl auf seriellen als auch auf USB-Tastaturen läuft. Logkeys erfasst und protokolliert sämtliche Eingaben, die auf der Tastatur gemacht werden. Logkeys übersetzt die eingegebenen Zeichen in das ASCII-Format.

MAC-Adresse
Bei einer MAC-Adresse handelt es sich um eine weltweit eindeutige Hardwareadresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient.

Malware
Internetinfektionen können grundsätzlich auf mehreren Wegen erfolgen, nämlich über E-Mails, präparierte Webseiten oder spezielle Webservices. Am häufigsten erfolgt der Angriff mit speziell präparierten E-Mails.

Medusa
Medusa ist ein schneller, parallel arbeitender und modular aufgebauter Log-in-Brute-Forcer, der mittels Wörterbuchattacke versucht, die Kennwörter entfernter Log-ins verschiedenster Dienste zu ermitteln.

Metasploit Framework
Das Metasploit Framework ist eine auf der Programmiersprache Ruby basierende Entwicklungs- und Testumgebung für diverse Exploits, Payloads, Opcodes und Shellcodes.

Ncrack
Ein flexibler Log-in-Brute-Forcer und ein Tool zum Network Authentication Cracking.

Nmap
Der Rolls Royce unter den Portscannern, zum Scannen und Auswerten von Hosts. Nmap beherrscht neben diversen Scantechniken das aktive Fingerprinting,

mit dem das auf dem Zielhost eingesetzte Betriebssystem erkannt werden kann.

Ophcrack
Passwort-Cracker für Windows-Benutzerkonten, der auf Rainbow Tables basiert. Für Ophcrack existiert eine ganze Reihe von Tables (auch deutschsprachigen Varianten) für das Passwort-Cracken.

p0f
Das p0f-Tool dient der passiven Erkennung der im Einsatz befindlichen Betriebssysteme.

OpenVAS
Umfassende Tool-Sammlung für die Sicherheitsanalyse in Netzwerken.

Optix Pro
Multilinguales, mit vielen Features ausgestattetes Remote Administration Tool, das laut den Entwicklern in der Lage ist, 73 AV-Tools sowie 37 Personal-Firewalls auszuschalten.

Poison Ivy
Sehr einfach einzurichtendes Servermodul (für Zielrechner bzw. Victim) inklusive Manual mit einer Vielzahl von Fernsteuerungsmöglichkeiten.

Portscanner
Portscanner testen, welche Dienste ein mit TCP/IP oder UDP arbeitendes System nach außen anbietet. Ihre Berechtigung haben sie vorzugsweise dort, wo man schnell seine eigenen Rechner auf mögliche Dienste und deren Verwundbarkeit checken will.

Proxys
Proxys oder Proxyserver sind die Datenverkehrsvermittler für Computernetze. Sie klinken sich für gewöhnlich zwischen Client (z. B. Internetbrowser) und Server ein mit dem Ziel, den Datentransfer zu protokollieren, zu beschleunigen oder zu anonymisieren.

Proxy Hunter
Will man bestimmte IP-Bereiche nach offenen Proxys abscannen, nimmt man entweder das gleichnamige Tool Proxy-Hunter oder den integrierten Proxy Hunter des AccessDivers.

PWDUMP
Gestattet das Auslesen und Speichern von Windows-Passwörtern, die in der SAM-Datei in Form von Hashes gespeichert sind. Als Anwender erspart man sich damit das mühselige Extrahieren dieser Daten aus der Registry.

PW-Inspector
Leistungsfähiges Tool zum Optimieren von Passwortlisten. Nur selten sind aus dem Internet bezogene Passwortlisten für den jeweiligen Einsatzzweck optimiert. Auch Dubletten nehmen unnötig viel Zeit und Rechenpower in Anspruch, ohne jedoch zu einem besseren Ergebnis zu führen.

Rainbow Tables
Rainbow Tables ermöglichen eine schnelle, probabilistische Suche nach dem einem Hashwert zugeordneten Klartext, z. B. einem Passwort, ohne dass alle für diesen Zeichenraum möglichen Hashwerte aufwendig errechnet werden müssen.

Ransomware
Verhältnismäßig junge Schädlingsgattung, auch als Erpresser-Trojaner bezeichnet, die sich explosionsartig vermehrt und auf private Nutzer abzielt, aber auch verstärkt Unternehmen ins Visier nimmt.

Remote Commander
Ein offizielles Managementtool zur Überwachung von Remote-PCs. Das Tool muss auf dem zu überwachenden Rechner nicht installiert werden, es werden keine Treiber und keine zu installierenden Programme auf dem Remote-PC benötigt.

Rootkits
An sich ein alter Hut; in der Unix-Welt existieren sie bereist seit Beginn der 90er-Jahre. Dahinter verbirgt sich eine raffinierte Tarntechnik, mit der ein Angreifer einen fremden Rechner übernehmen und steuern kann, ohne dass diese Aktivitäten vom User bemerkt würden.

Security-Scanner
Im Gegensatz zu den klassischen Portscannern verfügen Security-Scanner über weitergehende, datenbankgestützte Möglichkeiten und eine offene, erweiterbare Architektur, um ein Zielsystem nach bekannten sowie brandneuen Schwachstellen zu scannen.

Security Suite
Ein deutschsprachiges Produkt, das Wechseldatenträger sowie alle PKCS#11-fähigen Geräte und ausgewählte Smartcards, Keys, Magnetkarten und berührungslose Systeme unterstützt.

Selektoren
Selektoren sind Merkmale wie E-Mailadressen, Mobilfunknummern, Schlüsselwörter, MAC- und IP-Adressen etc., mit denen das Netz nach aus Sicht der Geheimdienste relevanten Informationen durchsucht werden soll.

Skriptkiddies
Oft die jüngere, unausgereifte Ausgabe der Hacker: talentiert, IT-Basis-Knowhow, an schnellen Erfolgen und Publicity interessiert, wobei sie im Großen und Ganzen die Folgen ihrer Handlungen oft nicht überblicken.

Snarfing
Die im Rahmen des Snarfing zur Verfügung stehenden Möglichkeiten sind schier unbegrenzt. So kann z. B. der gesamte Datenverkehr mitgeschnitten, manipuliert und ausgewertet werden, was insbesondere bei ungeschützter Kommunikation ein nicht unerhebliches Problem darstellt. Snarfing geht häufig mit der Verteilung von Schadsoftware einher.

Sniffer
Der Gattungsbegriff für alle Tools, die Datenpakete innerhalb des Netzwerkverkehrs abgreifen und analysieren können. Für Admins sind Sniffer unverzichtbare Analysewerkzeuge, um Netzwerkstörungen und Einbruchsversuchen auf die Spur zu kommen. Zudem sind Sniffer hocheffiziente, im Einsatz kaum zu entdeckende Spionagetools.

Social Engineering
Das Dreieck »User-ISP-Mail-Acount« bildet das Angriffsziel für Social Engineering. Die zentrale Frage lautet immer: Wer kennt die Log-in-Daten für den FTP-Zugriff?

Tails
Steht für »theamnesicincognitolive system« und ist ein Live-Betriebssystem, das von USB-Stick oder DVD gestartet wird, um anonym ins Internet gehen, E-Mail und Messanger nutzen zu können, ohne irgendwelche Spuren zu hinterlassen.

SAMInside
Mit dem in Assembler geschriebenen SAMInside können Benutzerpasswörter in allen neueren Windows-Versionen schnell und unkompliziert wiederhergestellt werden.

Stealth Recorder Pro
Eine Audiowanze mit verblüffendem Funktionsumfang. Ziel des Angriffs sind Gespräche, die in der Nähe des Rechners oder Notebooks geführt werden.

Tor
Wer sich nicht von einem Anbieter abhängig machen möchte, kann auf Anonymisierungsdienste wie Tor Onion Router zurückgreifen. In Kombination mit einem modizierten Firefox-Browser in Form des »Tor-Browsers« verfügt man dann über einen sehr guten Basisschutz für anonymes Surfen.

Turkojan
Trojanerbaukasten aus einer türkischen Hackerschmiede, der sich mit vielen Features multilingual präsentiert. Im Netz existieren viele Videos, die anschaulich zeigen, wie man sich das Servermodul für den Opfer-PC zusammenklickt.

VNCrack
VNCrack ist ein Passwort-Cracker, der Attacken auf VNC-Server und/oder auf mitgeschnittene VNC-Password-Challenges durchführt. Hierbei bedient sich VNCrack Wörterbuch- und Brute-Force-Angriffen.

Wardriving
Systematische Suche und Entdeckung möglichst vieler ungeschützter Funknetze mittels eines Fahrzeugs, Notebooks und WLAN-Sniffers.

Winfingerprint
Ein Fingerprinting-Tool, das nach Eingabe einer IP-Liste, einer IP-Range des Hosts oder der Netzwerkumgebung andere ans Netz angeschlossene Rechner scannt und je nach Voreinstellung einen ausführlichen Report über das Zielsystem ausgibt.

WPA2-Enterprise
Ermöglicht zusätzliche Authentifizierungsmethoden durch die Verwendung von EAP und TTLS. Für Unternehmen mit schutzbedürftigen Inhalten ohnehin eine grundsätzliche Pflicht.

Xkeyscore
Spionagesoftware der NSA. Da passt es ins Bild, wenn der Verfassungsschutz dieses mächtige Massenüberwachungs-Werkzeug seit über drei Jahren testet, obwohl der Inlandsgeheimdienst laut Gesetz nur Einzelpersonen überwachen darf.

Xprobe2
Beherrscht aktives Fingerprinting, mit dem das auf dem Zielhost eingesetzte Betriebssystem erkannt werden kann. Dabei kombiniert Xprobe2 verschiedene Methoden unter Benutzung des ICMP-Protokolls von einer errechneten Wahrscheinlichkeit bis hin zur Einbindung einer Signaturdatenbank.

XSS-Angriff
Ein XSS-Angriff (Cross Site Scripting) dienst der Verbreitung von Spam und Malware. Betroffen sind alle Websites mit dynamischen, aus Datenbanken generierten Seiteninhalten.

Stichwortverzeichnis

M

N

S

X

Y

Z

Dr. Peter Kraft / Andreas Weyert

Network Hacking

Die zwei Jahre, die seit der vierten Neuauflage von »Network Hacking« vergangen sind, waren geprägt von einer ungeheuren Dynamik. So wird es niemanden überraschen, dass die Bedrohung durch Cyber-Attacken unvermindert anhält und sich auch die Angriffslast auf weiterhin hohem Niveau bewegt. Neu hinzugekommen sind u. a. Angriffe auf das »Internet der Dinge« durch beispielsweise ZigBee-Würmer. Je mehr unsere Alltagsdinge wie Auto, Heizung und Kühlschrank vernetzt werden, desto mehr neue Bedrohungsszenarien sind denkbar.

Die Tools der Cracker und Datenpiraten

Detailliert stellen die Autoren die gesamte Bandbreite der Werkzeuge vor und demonstrieren, wie Keylogger die Eingaben ahnungsloser Benutzer mitschneiden, Passwort-Cracker Zugangskennungen knacken, Remote-Access-Tools PCs in Zombies verwandeln und Rootkits Malware verstecken.

Motive und Strategien der Angreifer

Kein Datenpirat ist wie der andere. Ihre Motivation und ihre Methoden zu verstehen ist ein wichtiger Schritt zum effektiven Selbstschutz. Die Autoren schildern unterschiedliche Szenarien, wie Datendiebe vorgehen und welche Schwächen der Netzwerkinfrastruktur sie ausnutzen. Ausgehend vom jeweiligen Bedrohungsszenario, wird auch die konkrete Abwehrstrategie vorgestellt.

So sichern Sie Ihr Netzwerk

Die Autoren geben fundierte Empfehlungen für eine proaktive Sicherheitsstrategie. Viele Schritte sind sogar kostenlos möglich, etwa die Überprüfung des Sicherheitsstatus oder das Abschalten nicht benötigter Dienste auf Windows-PCs. Darüber hinaus erhalten Sie leicht nachvollziehbare Ratschläge für die Auswahl geeigneter Security-Tools und für das Erstellen wirksamer Sicherheitsrichtlinien in Unternehmen

Aus dem Inhalt:

Über die Autoren:

Dr. Peter Kraft ist Geschäftsführer von synTeam Dr. Kraft & Partner. Seit mehr als zehn Jahren berät er Kunden in Fragen der Organisationsentwicklung und -optimierung. Er ist Autor mehrerer erfolgreicher Bücher zum Thema IT-Sicherheit und NLP.

Andreas G. Weyert ist BSI-Auditteamleiter, Auditor für ISO 27001 und begeisterter Netzwerkforscher. Beim internationalen Logistik-Anbieter Hellmann Worldwide Logistics entwickelt er als Information Security Manager die Bereiche Informationssicherheit und Risk-Management. Für den Franzis Verlag ist er seit 2002 als Sachbuchautor tätig.

Auf www.buch.cd

Feature-Listen und Bedienparameter der im Buch vorgestellten Hacking-Tools.

ISBN 978-3-645-20531-3

Besuchen Sie unsere Website
www.franzis.de

FRANZIS