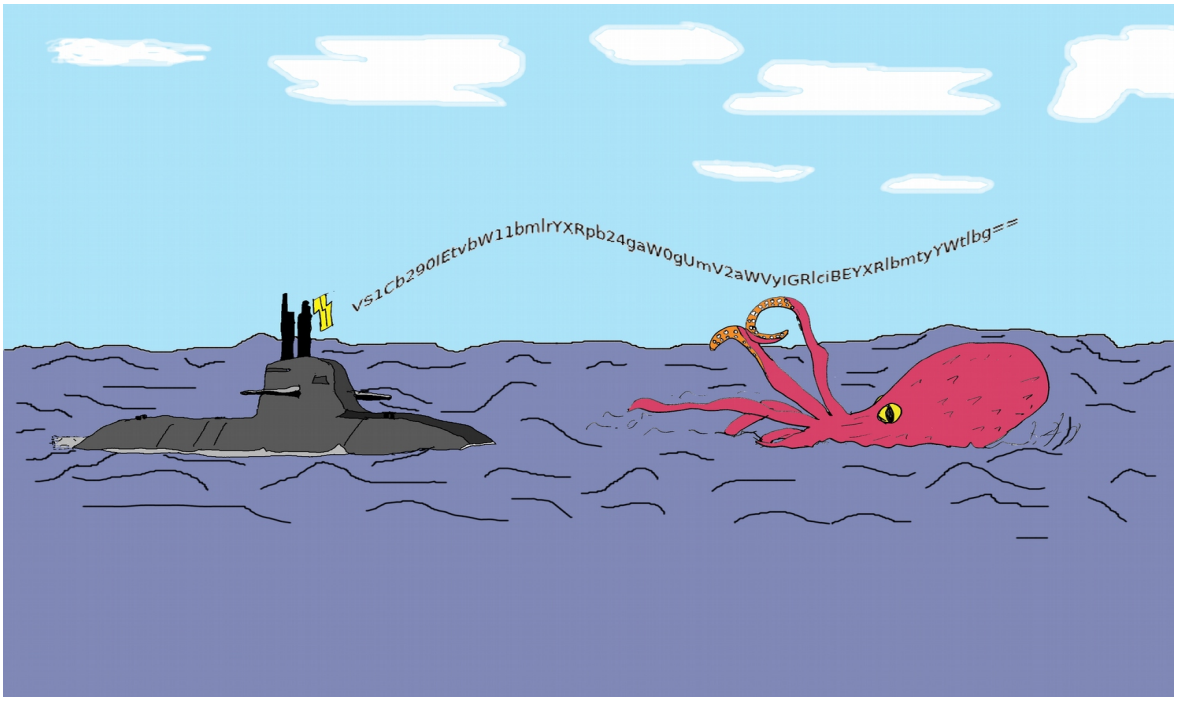
Michael Anders

U-Boot Kommunikation im Revier des Datenkraken

Über sichere Kommunikation mit dem privaten Computer



Dieses Buch ist an Nutzer eines privaten Computers, Note- oder Netbooks gerichtet. Gegenüber einem am Arbeitsplatz genutzten, vom Unternehmen administrierten System eröffnet das privat genutzte System größere Risiken, aber auch wesentlich größere Freiheiten und Chancen. Es geht in diesem Buch darum, diese Freiheiten und Chancen zu nutzen, um die persönliche elektronische Kommunikation erheblich besser gegen Zugriff durch staatliche oder kriminelle Organisationen zu schützen, als das üblicherweise am Arbeitsplatz geschieht.

Hinweis: *Alle im Folgenden im der Papierversion dieses Buches wiedergegebenen Internetadressen sind unter:* https://www.academic-signature.org/buch/uboot_k.php *komfortabel sortiert und anklickbar gelistet.*

Über den Autor:

Prof. Dr. Michael Anders ist Physiker und seit 1993 Dozent an der Fachhochschule Wedel. Seit vielen Jahren ist er Studiendekan des Studienganges Wirtschaftsingenieurwesen in Wedel. Er leitet seit einigen Jahren ein Seminar im Vertiefungsbereich IT und behandelt dort die Themen Anonymität und Verschlüsselung.

Im Jahr 2011 hat er das quelloffene Verschlüsselungswerkzeug Academic-Signature entwickelt, das mit Elliptischer Kurven Algebra Verschlüsselung, digitale Signaturen und Zeitstempel ermöglicht. Das Programm wurde unter der GNU General Public License veröffentlicht (https://www.academic-signature.org). Neben dem wesentlich weiter verbreiteten GnuPG ist es das einzige quelloffene, flexibel einsetzbare eigenständige Werkzeug für hybride Verschlüsselung beliebiger Dateien.

Rechtliches:

Zweck dieses Buches ist, den Leser durch Argumente von der Wirksamkeit bestimmter Schutzmaßnahmen gegen Überwachung zu überzeugen. Der Leser soll durch die Ausführungen im Buch zu fundierten eigenen Entscheidungen befähigt werden. Wenn er die im Buch vorgestellten Werkzeuge und Verfahren nutzt, tut er das auf eigene Verantwortung und nach eigener Abwägung und Entscheidung.

Die Verwendung aller im Buch vorgestellten Techniken und Werkzeuge ist nach dem Kenntnisstand des Autors in Deutschland legal. Dies ist aber nicht in allen Nationen der Fall. Bitte erkundigen Sie sich über die rechtliche Situation in Ihrem Heimatland und nutzen Sie keine im Buch vorgestellten Techniken und Werkzeuge in einem Land, in dem deren Nutzung verboten ist. Der Autor empfiehlt Ihnen schweren Herzens, sich in diesem Fall den demokratiefeindlichen, menschenverachtenden Überwachungspraktiken des betroffenen Landes zu unterwerfen.

In einigen demokratischen europäischen Ländern ist Einsatz und Verbreitung wirksamer Verschlüsselung ohne Regierungslizenz verboten. Dem Autor ist aber nichts davon bekannt, dass in unseren demokratischen Nachbarländern der Versuch unternommen würde, dieses Verbot durchzusetzen.

Alle Angaben in diesem Buch wurden mit angemessener Sorgfalt erarbeitet und überprüft. Trotzdem können Fehler oder Aktualisierungsbedarf nicht ausgeschlossen werden. Deshalb möchte der Autor darauf hinweisen, dass er keine juristische Verantwortung für Schäden übernimmt, die auf fehlerhafte Angaben oder missverständliche Formulierungen im Buch zurückzuführen sein könnten oder die durch von den lokalen Behörden entdeckte, am Ort des Lesers gesetzeswidrige Handlungen entstehen. Der Autor muss auch dringend davon abraten, während der Lektüre frisch gekochten Kaffee zu trinken, Sie könnten sich verbrühen. Auch hierfür wird jede juristische Verantwortung ausgeschlossen.

Selbstverständlich ist der Autor für Mitteilungen über etwaige Fehler im Werk oder Aktualisierungsbedarf jederzeit dankbar.

© 2018 Michael Anders, michael.anders@academic-signature.org

ISBN: 978-3-746769-02-8

Herausgeber und Vertrieb: epubli GmbH, Berlin, www.epubli.de

Inhaltsverzeichnis

1 Kommunikation mit dem privaten Computer....7
1.1 Beruflicher und privater Umgang mit dem Computer....7
1.2 Das Angebot der Softwarekonzerne für private Computernutzer....8
1.3 Das Ringen um Zugang zu Ihren privaten Daten....8
1.4 Vereinfachte sichere elektronische Kommunikation in einer Demokratie....11
1.5 Die heutige Situation....12
1.6 Der Preis von Unabhängigkeit und digitaler Selbstbestimmung....13
1.7 U-Boot Kommunikation....13
1.8 Grundstruktur der folgenden Kapitel....15
2 Basisstufe - IT-Selbstbestimmung....16
2.1 Grundprinzipien der IT-Selbstbestimmung....16
2.1.1 Volle Kontrolle des Nutzers über das System....16
2.1.2 Fähigkeit zur sicheren Installation von Software....18
2.1.3 Einsatz der digitalen Signatur....19
2.2 Werkzeuge für die IT-Selbstbestimmung....21
2.2.1 Quelloffene Betriebssysteme....21
2.1.2 Werkzeuge für manuellen Umgang mit digitalen Signaturen: GnuPG....21
2.1.3 Werkzeuge für manuellen Umgang mit digitalen Signaturen: Academic Signature....25
2.2 Übungen für die IT-Selbstbestimmung....27
2.2.0 Vorübungen:....27
2.2.1 ITS_A1, Digitale Signatur mit Academic Signature....28
2.2.2 ITS_A2, Digitale Signatur mit GnuPG....28
2.2.3 ITS_A3, Webseitenzertifikate....29
2.2.4 ITS_A4, Authentifizierung über die Automatismen des Betriebssystems....29
2.2.5 ITS_A5, Manuelle Authentifizierung einer Installationsdatei mit GnuPG....30
2.2.6 ITS_A6, Manuelle Authentifizierung einer Installationsdatei mit Academic Signature....30
2.2.7 ITS_A7, Installieren Sie einen freien Hex-Editor auf möglichst sicherem Weg....31
2.2.8 ITS_A8, Verschlüsselungsfunktionen von Academic Signature und GnuPG....31
2.3 Angriffe auf die IT-Selbstbestimmung....32
2.3.1 Systemd....32
2.3.2 Tendenzen bei Hardware Herstellern und Handel....32
2.3.3 Fremdbestimmung bei Nutzung des Betriebssystems Windows10....33
3 Stufe - rezeptive Anonymität....34
3.1 Was bedeutet rezeptive Anonymität....34
3.2 Geopolitische Aspekte der Anonymisierung digitaler Kommunikation....35
3.3 Anonymität durch untrennbares Vermischen von Datenverkehren....36

3.3.1 Ein einfacher Internetzugriff....36
3.3.2 Der VPN-Server als verschwiegene Zwischenstation....38
3.3.3 Zwiebel Routing, ein Netz verschwiegener Zwischenstationen....42
3.3.4 Anonymität durch anonymen Zugang zum Internet....45
3.4 Werkzeuge für rezeptive Anonymität....46
3.4.1 VPN Gate....46
3.4.2 TOR und TOR-Browser....46
3.4.3 Mail Zugang und TOR-Birdy....47
3.4.4 TAILS....48
3.4.5 I2P "The Invisible Internet Project"....49
3.5 Übungen für die rezeptive Anonymität....51
3.5.1 Rez_A1, Verfolgen Sie den Weg Ihrer Datenpakete zum Server Ihrer Online-Lieblingszeitung....51
3.5.2 Rez_A2, Nutzen Sie selbstbestimmt ein freies VPN für den Internetzugang....52
3.5.3 Rez_A3, Laden Sie den TOR-Browser herunter und installieren ihn auf Ihrem System....57
3.5.4 Rez_A4, Überprüfen Sie die Funktion des TOR-Browsers....58
3.5.5 Rez_A5, Verketten Sie ein VPN mit der Nutzung des TOR Browsers und blockieren Sie die Ausführung von Skripten im TOR-Browser....58
3.5.6 Rez_A6, Rufen Sie Ihre Mails über das Webinterface Ihres Mail Providers ab, ohne Ihren geografischen Standort preiszugeben....59
3.5.7 Rez_A7, Falls Sie den Thunderbird Mailer nutzen, installieren Sie den TOR-Birdy....60
3.5.8 Rez_A8, Finden Sie heraus, wie man für den TOR-Browser einen Ausgangsknoten in einem Land Ihrer Wahl erzwingen kann....60
3.5.9 Rez_A9, Finden Sie eine TOR Darknet Suchmaschine für sogenannte .onion-sites....61
3.5.10 Rez_A10, Bewegen Sie sich im TOR Darknet - nur lesend....61
3.5.11 Rez_A11, Installieren und testen Sie die Anonymisierungsoftware I2P....61
3.5.12 Rez_A12, Erstellen Sie sich zwei TAILS USB-Sticks....62
3.5.13 Rez_A13, Bewegen Sie sich mit TAILS im TOR Darknet - nur lesend....64
3.5.14 Rez_A14, Installieren Sie einen Zugang zu Ihrem "normalen" Mail-Konto in Ihrem TAILS....64
3.5.15 Rez_A15, Lesen Sie in TAILS über den TOR-Browser Ihre Lieblings-Onlinezeitung....65
3.5.16 Rez_A16, Alarmübung....65
3.5.17 Rez_A17, Transferieren Sie Ihr normales GnuPG Schlüsselpaar in Ihr TAILS....65
3.5.18 Rez_A18, Installieren und nutzen Sie Academic Signature in ihrem TAILS....66
3.5.19 Rez_A19, Finden Sie die MAC Adresse der WLAN-Interfaces Ihrer Computer heraus....66
3.5.20 Rez_A20, Finden Sie eine kostenfreie Software zum MAC Address Spoofing....67
3.5.21 Rez_A21, Nutzen Sie TAILS zum MAC Address Spoofing....67
3.6 Angriffe auf die rezeptive Anonymität....67
3.6.1 Angriffstyp 1, Website Fingerprinting....69
3.6.2 Angriffstyp 1, Modulation der Datenrate bei geographisch benachbartem Zielserver....69
3.6.3 Angriffstyp 1, Physische Angriffe auf ausgewiesene TOR Nutzer....70
3.6.4 Angriffstyp 2, NSA Angriff, Kompromittierung des TOR Browsers....71
3.6.5 Angriffstyp 2, MITM-Angriff durch den Ausgangsknoten....71
3.6.6 Angriffstyp 3, Big Data Angriff auf eine fiktive Identität durch statistische Analyse....72

3.6.7 Angriffstyp 3, Big Data Angriff durch Modulation der Datenrate....72
3.6.8 Angriffstyp 3, Trojanische Knoten....73
4 Stufe - expressive Anonymität....74
4.1 Fiktive Identitäten....74
4.2 Gefahren bei Nutzung kommerzieller Dienste und bei Bezahlvorgängen....74
4.3 Werkzeuge für expressive Anonymität....76
4.3.1 Chat Konten....76
4.3.2 Was ist ein Jabber Konto....76
4.3.3 Pidgin als Jabber Client und TOR....77
4.3.4 TOR Verbindung im Rendezvous Typ....78
4.3.5 Anonymes e-Mail Konto, Betrieb über ein Webinterface im TOR-Browser....80
4.3.6 Anonymes e-Mail Konto, Verringerung der Angriffsfläche durch gemeinsames Nutzen eines Mail/Speicher-Kontos....82
4.3.7 Serverloser Nachrichtenaustausch über Onionshare....83
4.4 Übungen für die expressive Anonymität....85
4.4.1 Exp_A1, Erstellen Sie und Ihr Kommunikationspartner jeweils anonym ein Chat Konto, und Chatten Sie anonym über den Client Pidgin....85
4.4.2 Exp_A2, Übertragen Sie 2 bis 3 kurze Textdateien ohne schützenswürdigen Inhalt anonym im Chat an das Partner Konto....88
4.4.3 Exp_A3, Erstellen Sie und Ihr Kommunikationspartner jeweils anonym ein e-Mail Konto und transferieren Sie e-Mails mit und ohne Dateianhänge....88
4.4.4 Exp_A4, Chatten Sie mit dem Werkzeug Ricochet über TOR nach dem TOR Rendezvous Prinzip (primäre Anonymität)....89
4.4.5 Exp_A5, Tauschen Sie eine Datei mit einem Partner über Onionshare aus (TOR Rendezvous Prinzip, primäre Anonymität)....89
4.4.6 Exp_A6, Suchen Sie im Internet nach einem Dokument, das die Auswahl und Aufbauprozedur des TOR Rendezvous Pfades erläutert. Lesen und verstehen Sie es....90
4.4.7 Exp_A7, Legen Sie ein Susi Mail Konto im alternativen Darknet I2P an und tauschen Sie Nachrichten und Dateianhänge mit einem durch TOR anonymisierten e-Mail Konto aus einer vorigen Übung aus....91
4.4.8 Exp_A8, Üben Sie den anonymen Kauf eines elektronischen Gerätes (Smartphone, Notebook o.ä.)....91
4.5 Angriffe auf die expressive Anonymität....93
4.5.1 Nonymisierende Information in übertragenen Daten....93
4.5.2 Big Data Angriffe....93
5 Stufe - Vertraulichkeit....98
5.1 Symmetrische Verschlüsselung....98
5.1.1 Stretching....100
5.1.2 Salting....100
5.1.3 Konkrete Abschätzung von Cracking-Zeiten und Kosten....101
5.1.4 Hilfe durch zusätzliche Kostentreiber....104
5.1.5 Der letzte Pfeil im Köcher....105
5.2 Asymmetrische Verschlüsselung....106
5.3 Hybride Verschlüsselung....107
5.4 Kombination von Anonymität und Vertraulichkeit....108

5.4.1 Primäre und sekundäre Anonymität bei vertraulicher Kommunikation....108
5.4.2 Starter-Kommunikation "out of band"....110
5.4.3 Anonyme verschlüsselte elektronische Kommunikation mit Unbekannten....110
5.5 Werkzeuge für Vertraulichkeit....111
5.5.1 Ergänzung des Chat Client Pidgin durch das Verschlüsselungs-Plugin OTR....111
5.5.2 Verschlüsselung durch GnuPG....113
5.5.3 Ergänzung des Thunderbird Mailers durch Enigmail....118
5.5.4 Verschlüsselung durch Academic Signature....118
5.6 Übungen für die Kombination von Anonymität mit Vertraulichkeit....122
5.6.1 A&V_A1, Symmetrische Verschlüsselung mit einem Office Paket....123
5.6.2 A&V_A2, Matrioschka Verschlüsselung mit (p)7zip....123
5.6.3 A&V_A3, Symmetrische Verschlüsselung mit GnuPG....124
5.6.4 A&V_A4, Symmetrische Verschlüsselung mit Academic Signature....125
5.6.5 A&V_A5, Einsatz des OTR-Plugins für die Verschlüsselung anonymisierter Chats....126
5.6.6 A&V_A6, Klonen Sie den anonymisierten Zugang zu einem OTR geschützten XMPP Chat Konto....127
5.6.7 A&V_A7, Ergänzen Sie fiktive Mail Identitäten um jeweils eigene Schlüsselpaare für asymmetrische Verschlüsselung und digitale Signatur....130
5.6.8 A&V_A8, Minimieren Sie die dem Angreifer gegenüber zugänglichen Informationen im GnuPG Chiffrat....131
5.6.9 A&V_A9, Minimieren Sie die dem Angreifer gegenüber zugänglichen Informationen im Academic Signature Chiffrat....132
5.6.10 A&V_A10, Anonymer Nachrichtenaustausch über einen geteilten Zugang zu Speicherplatz im Netz....133
5.6.11 A&V_A11, Nonymer Mailaustausch mit durch GnuPG geschützten Inhalten....134
5.6.12 A&V_A12) Transfer einer Mail mit Dateianhang zwischen pseudonymen Mail Konten mit GnuPG Automatismen....136
5.6.13 A&V_A13, Transfer einer mittelgroßen Datei zwischen pseudonymen Mail Konten mit manueller Verschlüsselung....138
5.6.14 A&V_A14, Transferieren Sie eine große Datei geschützt und anonymitätserhaltend über XMPP Chat Konten....140
5.6.15 A&V_A15, Resilenz gegen Big Data Angriffe durch fliegenden Wechsel von Chat Konten....141
5.6.16 A&V_A16, Transfer einer Datei von einem pseudonymen I2P SusiMail Konto zu einem anderen pseudonymen Mail Konto mit manueller Verschlüsselung....144
5.6.17 A&V_A17, U-Boot-Kommunikation: Transfer einer beliebig grossen Datei im Rendezvous Typ per Onionshare, Starter Kommunikation "out of Band"....147
5.6.18 A&V_A18, U-Boot-Kommunikation: Transfer einer beliebig grossen Datei im Rendezvous Typ per Onionshare, verabredungsgetrieben....149
5.7 Angriffe auf die Kombination von Anonymität mit Vertraulichkeit....154
5.7.1 Angriff auf Vertraulichkeit und Anonymität: Das NOBUS Prinzip....154
5.7.2 Big Data Komplementärangriff, Antikorrelation mit nonymer Aktivität....156
5.7.3 Anekdotische Indizien für die Verwundbarkeit von TOR Anonymisierung....158
6 Einige Bemerkungen zum Ende....160
7 Schlusswort....162
8 Glossar und Stichwortverzeichnis....163

1 Kommunikation mit dem privaten Computer

1.1 Beruflicher und privater Umgang mit dem Computer

Am Arbeitsplatz wird die IT-Abteilung sich im Idealfall gut um die IT-Sicherheit der Arbeitsplatzrechner gegen Kriminelle, aber im Regelfall leider weniger gut um die Vertraulichkeit der beruflichen Kommunikation kümmern. Zur Herstellung von Sicherheit gegen Kriminelle wird die IT-Abteilung die Rechte der Mitarbeiter auf den bereitgestellten Systemen stark beschränken und den Mitarbeitern vernünftige und - besonders im Passwortbereich - auch teilweise absurde Pflichten auferlegen. Wer kennt nicht Anweisungen, etwa drei unterschiedliche Passwörter für drei verschiedene Systeme mit jeweils Sonderzeichen, Großbuchstaben und Zahlen in gewisser Mindestlänge zu nutzen, mindestens alle 60 Tage zu ändern, aber ganz bestimmt nirgends zu notieren. Man hat als Mitarbeiter im Gegenzug aber das beruhigende Gefühl, nicht für die Sicherheit und Funktionalität der IT verantwortlich zu sein. Bei der kommerziellen IT-Sicherheit im Unternehmensumfeld liegt notwendigerweise der Fokus auf ganz anderen Stellen, als bei der in diesem Buch behandelten sicheren Kommunikation im privaten Umfeld. Ich möchte jetzt diese Unterschiede herausarbeiten.

Bei der Unternehmenssicherheit ist das Hauptproblem, die in diesen Dingen unmotiviertesten und am wenigsten kundigen Mitarbeiter von der Gefährdung der Unternehmens-IT durch Dummheiten abzuhalten, die Möglichkeiten für diese zu begrenzen, massiven Schaden anzurichten und notfalls solche Schäden wenigstens möglichst früh zu bemerken. Die unkundigen und als Kollateralschaden auch alle anderen Mitarbeiter müssen in ihren Möglichkeiten beschränkt und in ihren Arbeitsabläufen kanalisiert werden. Sie müssen davon abgehalten werden, beispielsweise in Outlook berüchtigte Mailanhänge des Prinzen aus Nigeria anzuklicken. Durch regelmäßige Systemupdates und rigorose Blockade nicht für notwendig erachteter Kommunikationsmodi (Blockade von Ports in der Firewall) muss gleichzeitig die Anzahl der für Angreifer nutzbaren Softwarefehler in Grenzen gehalten werden. Westliche staatliche Dienste werden wider besseres Wissen als Bedrohung der vertraulichen Kommunikation meist vernachlässigt. Die Gefahr der Informationslecks durch illoyale Unternehmensinsider wird als wesentlich bedrohlicher eingestuft. Deshalb würde in diesem Kontext die Verfügbarkeit von Ende zu Ende Verschlüsselung für kommunizierende Mitarbeiter eher als Bedrohung der Unternehmenssicherheit, denn als Schutz gegen Industriespionage gesehen. Das sind wenig günstige Rahmenbedingungen für einen effektiven Schutz der Mitarbeiterkommunikation.

Wenn man sich aber, wie in diesem Ratgeber, mit der Sicherheit privater digitaler Kommunikation befasst, ist man in einer komfortableren Situation als im Unternehmensumfeld. Wer dieses Buch in die Hand nimmt, ist hoch motiviert und an der Sicherheit der eigenen Kommunikation interessiert. Ich kann beim Leser zwar anfangs nicht auf allzu große IT-Kenntnis oder gar kryptographische Fachkenntnis, dafür aber auf Interesse und geistige Beweglichkeit vertrauen und kann Experimentierfreude begrüßen. Das ist eine ausgezeichnete Ausgangsposition.

Beim Umgang mit dem privaten Computer sind Sie selbst in der Pflicht, durch umsichtiges Verhalten die Risiken zu minimieren, Opfer von Internetkriminalität zu werden und Schäden durch Angriffe in Grenzen zu halten. Zur Umsicht gehört, keine Speichermedien mit unklarer Vorgeschichte mit dem System zu verbinden und vernünftigen Umgang mit Passwörtern zu pflegen. Weiterhin sollte man ein System, mit dem Bankgeschäfte oder Einkäufe getätigt werden

oder diesbezüglicher e-Mail Verkehr betrieben wird, nicht zum ungeschützten Surfen auf "Blinki-Bunti-Schmuddelseiten" verwenden. Wenn man dies verinnerlicht und sich ähnliche Restriktionen auferlegt, wie sie im beruflichen Umfeld erzwungen werden, kann man auf einem privaten System eine dem beruflichen Umfeld vergleichbare Sicherheit erreichen. Man könnte darüber hinaus sogar vielleicht noch die üblichen Ratschläge zur regelmäßigen Datensicherung befolgen und einen aufmerksamen Blick auf die Logs des Systems, vielleicht sogar auf den ein- und ausgehenden Datenverkehr haben und bei Auffälligkeiten sofort einschreiten.

Solche Maßnahmen der allgemeinen umsichtigen Verwendung des Computers werden in diesem Ratgeber aber nur am Rande thematisiert. Hier wird der Fokus auf der Vertraulichkeit Ihrer elektronischen Kommunikation liegen. Bei den später folgenden Ausführungen wird unterstellt, Ihr privates System sei sicher und keine staatliche oder kriminelle Organisation habe ohne Ihre ausdrückliche Zustimmung Zugriff auf Ihren Computer.

1.2 Das Angebot der Softwarekonzerne für private Computernutzer

Die Maßnahmen zur allgemeinen Systemsicherheit erfordern eine gewisse Mühe und ein gewisses Verständnis auf Nutzerseite. Um dem Nutzer die Mühe und die meist ungeliebte Suche nach Verständnis zu erleichtern, tendieren die Hersteller der gängigen kommerziellen, für Privatnutzer gedachten Betriebssystemen dazu, die Systeme immer mehr gegenüber dem Nutzer zu verschließen und für Fernwartung aufzubereiten. Diese Fernwartung läuft dann ohne Mitwirkung und Information des Nutzers im Hintergrund ab. Eine solche Fernwartung ohne Nutzerkontakt wird aber niemals die Sicherheit und Flexibilität herstellen, wie man sie bei einem durch einen kundigen Menschen administrierten System erreichen kann.

Die Fernwartbarkeit am Nutzer und Besitzer vorbei bringt leider auch eine starke Versuchung für Softwarehersteller, diesen unkontrollierten Zugang zum privaten System für allerhand lästige Marketingaktivitäten und Handel mit abgezogenen Nutzerdaten zu missbrauchen. Die Marketing-aktivitäten sind hierbei der für uns Nutzer offen sichtbareTeil.

1.3 Das Ringen um Zugang zu Ihren privaten Daten

Für eine Minderheit der Nutzer, die die volle Kontrolle über ihr System und ihre Daten behalten wollen, ist die Gefahr des Machtmissbrauchs, die zunehmende Beschränkung der Rechte am eigenen System und die allzu bereitwillige Kooperation der Softwarekonzerne mit den Nach-richtendiensten ihrer Heimatländer ein großes Ärgernis.

Ein Beispiel: *Mitte Oktober 2017 wurde öffentlich bekannt, dass in vielen sogenannten TPMs (Trusted Platform Module) eine fehlerhafte Bibliothek für die Generierung von RSA-Schlüsseln verwendet wurde:*

(https://crocs.fi.muni.cz/public/papers/rsa_ccs17 *).*

Der Fehler führt zu unsicheren RSA-Schlüsselpaaren. Es handelte sich aber nicht um einen Fehler im Zufallszahlengenerator.

Das TPM ist ein in Desktop Computern und Notebooks eingebauter Chip, der auch zur Prüfung digitaler Signaturen vor der Ausführung von heruntergeladenen Installations- oder Updatedateien verwendet wird. Die fehlerhafte Bibliothek liegt in der Firmware, das ist auf dem Chip selbst vorliegende, gegen Manipulation von außen gesondert geschützte Software.

Der Fehler erhielt die offizielle Kennung CVE-2017-15361 und den Namen ROCA, Return of Coppersmith's Attack. Auch Infineon TPMs wurden 5 Jahre lang mit dem fehlerhaften Programm ausgeliefert. Nun muss man wissen, dass ein RSA-Schlüssel dadurch erzeugt wird, dass zwei lange Primzahlen gesucht werden. Dabei wird, ausgehend von einer Zufallszahl entsprechender Länge, meist durch einfaches Hochzählen und jeweiliges Anwenden eines probabilistischen Primzahltests, die nächste Primzahl gewählt. Das Produkt der zwei Primzahlen, zusammen mit einer frei gewählten, meist deutlich kleineren Zahl, dem sogenannten öffentlichen Exponenten, ist im Wesentlichen der öffentliche Schlüssel. Kenntnis der beiden Primfaktoren ist der private Schlüssel.

Wenn nun der Zufallszahlengenerator, wie verbreitet wurde, nicht betroffen war, stellt sich folgende Frage: Was hat die Software der fehlerhaften Chips für ungewöhnliche Kriterien, nicht die jeweils nächsten Primzahlen nach einer Zufallszahl, sondern andere, handverlesene, zu leichter knackbaren Schlüsseln führende Primzahlen auszuwählen? Die von Infineon verbreitete Erklärung, so habe eine schnellere Primzahlerzeugung erreicht werden sollen, erscheint mir absurd - die Schlüsselerstellung passiert meist ein, höchstens ein paar mal in der Lebenszeit des Chips und dauert im Chip vielleicht eine Minute. Ich vermute, dass bewusst eine Hintertür für staatliche Akteure eingerichtet war.

Als die Sicherheitsforscher der Masaryk Universität in Brünn, der britischen Sicherheitsfirma Enigma Bridge und der Ca' Foscari Universität in Venedig die Lücke entdeckten, musste auf Seiten der staatlichen "Bedarfsträger" mutmaßlich rasch gehandelt werden, um den Schaden zu begrenzen. Selbstverständlich waren die betroffenen TPMs vom amerikanischen NIST und vom deutschen BSI bei deren Einführung als sicher zertifiziert worden.

*Auch ohne besondere Kenntnisse in Kryptographie kann jeder verstehen, dass eine vorhergehende Einschränkung der Auswahl auf wenige spezielle Primzahlen dem Angreifer das Ermitteln der tatsächlich im privaten Schlüssel verwendeten Primzahlen erleichtert, wenn dem Angreifer die Art der Einschränkung bekannt ist. Bei jedem seriösen Audit einer Implementation des RSA-Algorithmus würde man als einen der ersten Punkte klären, wie die verwendeten Primzahlen bestimmt werden und ob tatsächlich aus der vollen Primzahlmenge zufällig ausgewählt wird. (Auf alles andere als ein klares "Ja" zur letzten Frage würden normalerweise einige Augenbrauen sehr weit hochgezogen werden.) Die Tatsache, dass das offensichtlich nicht geschehen ist, ist sehr beunruhigend. Bezüglich der staatlichen IT-Sicherheitsbehörden BSI und NIST muss man sich nun entscheiden, ob man die beteiligten Mitarbeiter für Saboteure oder für inkompetent hält. In einem Artikel in Zeit-Online wurde sehr vorsichtig die zweite Variante angedeutet. Der Vorgang wurde dort als peinlich für das BSI bezeichnet (*https://www.zeit.de/digital/datenschutz/2017-10/infineon-verschluesslung-personalausweis-tpm-bsi-zertifiziert *). Ein weiteres Nachhaken von Seiten des investigativen Journalismus erfolgte leider nicht.*

Nun müssen Sie, lieber Leser, für sich den hier als Beispiel dargestellten Vorfall selbst bewerten und einordnen. Ich persönlich neige dazu, die Mitarbeiter des BSI und des US-amerikanischen NIST nicht gleichzeitig für inkompetent zu halten und vermute Sabotage.

Natürlich müssen Sie diese Einschätzung und meine kritische Sicht auf das Agieren der Behörden BSI und NIST nicht teilen. An dieser Stelle möchte ich ausdrücklich alle Leser dieses Buches, unabhängig von ihrer Sicht auf solche Ereignisse, willkommen heißen. Bei den Lesern, die der von

meiner Meinung abweichenden Auffassung zuneigen, die offiziellen Stellen und großen Firmen hätten in aller Regel recht, seien ehrlich und es seien viele unberechtigte Verschwörungstheorien in Umlauf, möchte ich mich vorauseilend für gelegentliche Wertungen in meinen Ausführung entschuldigen. Bei den Schlusskapiteln 6 und 7, nach dem Abschluss meiner eher politisch neutralen technischen Passagen, werde ich meine persönlichen Wertungen aber erneut deutlich und unmissverständlich formulieren. Es könnte allerdings selbst in dem technisch orientierten Hauptteil des Buches passieren, dass mir hier und da wertende Adjektive in den Text hineingeraten sind, die Ihnen vielleicht nicht gefallen. Bitte sehen Sie mir das nach, letztlich hat meine persönliche Betroffenheit über den Umgang unserer politischen Führungen mit den Enthüllungen von Edward Snowden mir den Antrieb zum Verfassen dieses Buches gegeben. Es ist aber primär ein technisches Buch.

Leider ist die Sicht auf die Arbeit unserer westlichen Nachrichtendienste und auf das Agieren der Internetkonzerne ziemlich polarisiert. Der eine betrachtet mich und meine Mitstreiter als Haufen wirrer Verschwörungstheoretiker. Die Seite, zu der ich mich zugehörig fühle, ist dagegen in Gefahr, jeden Kritiker quelloffener und freier Software und jeden konzern- oder behördennah argumentierenden Vertreter als faschistoiden Bespitzelungsverfechter zu sehen. Wenn man auf dem Gebiet der Technik virtuell die Klingen kreuzt, gibt es aber die Chance, sich über technikzentrierte Diskussionen auch wieder politisch näherzukommen. Wir Abhör- und Datensammelgegner müssen uns in die Gedankenwelt unserer Angreifer hineinversetzen, um in der Abwehr gut zu sein. Außerdem müssen wir ständig unsere Feindbilder auf den Prüfstand stellen, unangemessen überbordendes Misstrauen macht unsere Abwehr nicht besser.

Falls Sie, lieber Leser, aber eher zur anderen Seite gehören und uns Überwachungsgegner für unangemessen misstrauische Anarchisten halten, sollten Sie dennoch gelegentlich auch gedanklich in unsere Haut schlüpfen. Auch Sie sollten Ihre Feindbilder hinterfragen. Wie fühlen Sie sich damit, von Behörden überwacht zu werden, die es als Geheimnis behandelt wissen wollen, welchen Umfang und welche Intensität diese Überwachung hat? Vielleicht hinterfragen Sie sogar für einen Moment einmal kritisch, ob die eine oder andere zunächst von Ihnen begrüßte Maßnahme nicht in Wirklichkeit tatsächlich den Weg auch in Ihre Unfreiheit und in eine Diktatur ebnen könnte. Auf jeden Fall heiße ich Sie, so wie Sie sind, als Leser willkommen und auch Sie sollten vom technischen Teil dieses Buches profitieren können.

Zum Schluss möchte ich jetzt diejenigen Leser begrüßen, die ich von Beginn an als Adressaten vor Augen hatte. Sie sind intelligente Computerlaien, haben aber durchaus Interesse an Computerdingen und dem Internet. Sie sind nicht ideologisch festgelegt und Ihre Bewertung des eingangs dieses Abschnittes vorgestellten Fehlers im TPM Ihres Computers ist noch im Fluss. Sie sind sich aber gewisser Fakten bewusst: Es gab die Snowden Enthüllungen im Jahr 2013. Westliche staatliche Dienste waren außer Rand und Band. Ob sie sich heute demokratiekonform verhalten oder es verdeckt heute noch schlimmer treiben, wissen wir nicht. Die Vorsicht legt aber nahe, sich gegen den letzteren Fall zu wappnen. Weiterhin gibt es als Bedrohung feindliche Nachrichtendienste und die stetig wachsende, ganz normale Internetkriminalität. Sie möchten deshalb die Fähigkeit zu sicherer, verdeckter Kommunikation erwerben und später vielleicht auch weitergeben. Herzlich willkommen, genau für Sie habe ich dieses Buch geschrieben.

Unabhängig davon, wie Ihr Interesse für dieses Buch begründet ist, werden alle Leser mit etwas Sorgfalt und der Suche nach Verständnis mit Ihrem privaten Computer ein Niveau an Selbstbestimmung und Sicherheit der Kommunikation erreichen können, das bei fremdadministrierten oder gar hersteller-fern-administrierten Systemen undenkbar ist. Abgesicherter elektronischer Kontakt mit schillernden Kommunikationspartnern und Webseiten wird möglich, der

am Arbeitsplatz mit gutem Grund off limits, sehr weit off limits ist. Weiterhin ist ein Schutz der Vertraulichkeit der elektronischen Kommunikation gegen Kriminelle und sogar staatliche Akteure möglich, der im beruflichem Umfeld niemals erreichbar ist, meist dort von der Unternehmensleitung gerade nicht erwünscht ist und häufig genug vom Unternehmen aktiv verhindert wird.

1.4 Vereinfachte sichere elektronische Kommunikation in einer Demokratie

Für Bürger einer freiheitlichen Demokratie (oder Herrschende in einer Diktatur), deren Privatsphäre vom Staat respektiert wird, ergibt sich ein einfaches Bild. Die Notwendigkeit von Anonymität entfällt, wirksame Verschlüsselung kann offen und selbstbewusst eingesetzt werden.

Es muss lediglich auf Basis eines unter voller Kontrolle des Nutzers stehenden Systems ein Werkzeug zur starken Verschlüsselung installiert und fachgerecht verwendet werden. Die heute verbreiteten Verschlüsselungswerkzeuge sind für diesen Rahmen entwickelt worden. Das Bewahren von Anonymität spielte bei der Entwicklung keine Rolle. Bei einem Einsatz in feindlicher Umgebung brechen oder gefährden sie die Anonymität der Nutzer.

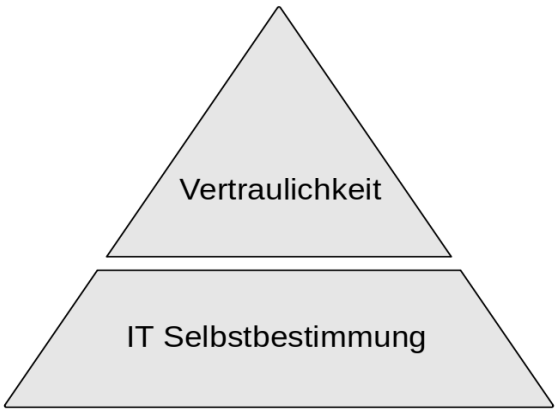


Abbildung 1: Pyramide freier Bürger für sichere elektronische Kommunikation

In den westlichen Demokratien haben wir lange geglaubt, das Streben nach der Vervollständigung der hier dargestellten Pyramide der Freien reiche aus, d.h. nutze Linux und verschlüssele Mails mit GnuPG, chatte über Jabber Server.

Leider wird bereits diese simple Vorgehensweise häufig als kompliziert dargestellt, von vielen Bürgern auch so empfunden und deshalb abgelehnt. Selbst unter diesen vereinfachten Bedingungen haben die Mehrzahl der Firmen und Einzelpersonen bereits leichtfertig die Basis der Pyramide vernachlässigt und sich, obwohl nach eigener Einschätzung frei, der Ausspähung durch externe IT-Unternehmen, der staatlichen Dienste der Sitze dieser Unternehmen und unbekannter Datenhändler unterworfen. Sie nutzen proprietäre Betriebssysteme, deren Quellcode der Allgemeinheit gegenüber nicht offengelegt wird und missachten damit die Basis einer sicheren elektronischen Kommunikation.

1.5 Die heutige Situation

Spätestens seit den Enthüllungen von Edward Snowden im Frühsommer 2013 wissen wir, dass wir uns in einem Übergangsprozess von freien Bürgern zu Digitaluntertanen befinden, der schon relativ weit fortgeschritten ist. Leider sind kaum Tendenzen erkennbar, dass dieser Prozess verzögert oder gar aufgehalten würde. Er schreitet stetig weiter voran und erfordert, dass wir uns als Privatpersonen aufwendig, in einem ausgefeilteren Muster, als nach der Pyramide der freien Bürger, gegen den Abhörstaat schützen müssen. Nur dann werden wir auch zukünftig als einfache Bürger mehr als nur die Illusion einer sicheren Kommunikation genießen können.

Eine unvollständige Strategie könnte zunächst beispielsweise nur die Verschlüsselung der Kommunikation in den Vordergrund stellen. Laut eigener Aussage bzw. eigenen Drohungen der Nachrichtendienste, die im Nachgang zu den Snowden Enthüllungen ganz offen ausgesprochen wurden, interessieren sich die Dienste besonders für diejenigen Bürger, die ihre Kommunikation verschlüsseln (deshalb solle man das nicht tun). Naheliegend und den Diensten zuzutrauen wäre es, dieses Interesse durch Verwanzen unserer Computer zu befriedigen. Dies kann durch einen Dienst recht einfach bewerkstelligt werden, wenn die Zielperson und deren Internetzugang dem Dienst bekannt ist. Staatliche Nachrichtendienste unterhalten Sammlungen von der Allgemeinheit unbekannten Sicherheitslücken aller verbreiteten Betriebssysteme, über die sie in diese Systeme Malware einbringen und damit Daten aus- und einschleusen können. Die neu gegründete Behörde ZITiS soll in Deutschland so die Verwanzbarkeit unserer Systeme durch den Staat sicherstellen. Ein der Obrigkeit bekannter missliebiger Bürger hat kaum eine Chance, sich gegen solche Angriffe des eigenen Staates zu schützen. Belastbare Anonymität im Internet vor einer Brandmarkung als "Dissident" ist der einzige Schutz.

Als Reaktion auf die Snowden-Enthüllungen sind, besonders für Messenger Dienste, verschlüsselte -nicht anonymisierende- Varianten breit in den Markt eingeführt worden und einige werden publikumswirksam von staatlichen Behörden und Diensten wegen deren Verschlüsselung als Ärgernis bezeichnet.

Bei genauem Hinsehen gibt es für mich aber bei allen weit verbreiteten kommerziellen Produkten Anlass zu Misstrauen. Ein bestimmter Messengerdienst (Signal) macht praktisch alles richtig und wird auch von der Mehrzahl der Experten empfohlen: Quelloffen, nur standardisierte Verschlüsselungsalgorithmen, Finanzierung durch Spenden und staatliche Zuwendungen, regelmäßige Audits, teilweise reproduzierbarer "Build-Prozess", einfach in der Benutzung. Aber genau dieser Messengerdienst läuft zwingend über zentrale Server, ist inkompatibel mit Anonymität und legt die Metadaten gegenüber dem Betreiber des Servers offen. Der Server-betreiber sichert die vertrauliche Behandlung dieser Daten zu, ist aber Partner in einer Zusammen-arbeit mit WhatsApp und unterliegt der US Jurisdiktion....

Dennoch, wer sich nicht wirklich durch den eigenen Staat oder die US-Administration bedroht fühlt und niemals Anonymität braucht oder die Beschäftigung mit der Sicherheit der eigenen Kommunikation als lästig empfindet, möge solche Dienste nutzen und sich sicher fühlen. Aber auch solche Computernutzer sollten sich ernsthaft zumindest um die Basisstufe in der Kommu-nikationspyramide der freien Bürger bemühen.

Dieser Ratgeber ist vor allem für die anderen Menschen gedacht, die die Kontrolle über ihre Daten und über die Sicherheit ihrer elektronischen Kommunikation selbst in der Hand behalten möchten

und die auch ein Grundinteresse an den Prinzipien der Anonymisierung und der Verschlüsselung haben. Dieses Buch hat den Zweck, dem Leser nachhaltig und in den Grundzügen produktunabhängig Verständnis über Anonymisierung und Vertraulichkeit, insbesondere über deren Zusammenspiel, zu vermitteln und ihn zu guten eigenen Entscheidungen zu befähigen.

1.6 Der Preis von Unabhängigkeit und digitaler Selbstbestimmung

An dieser Stelle möchte ich betonen, dass Unabhängigkeit und Selbstbestimmung wie immer, so auch in diesem Gebiet, einen Preis haben. Wir müssen für ein Mehr an Autarkie ein Stück weit auf die Bequemlichkeit unseres sonst extrem arbeitsteiligen Lebens verzichten und uns auch in ungeliebten Tätigkeiten üben. Dass dies im analogen Leben gilt, ist eine Binsenweisheit. Wer im Analogen das Rebellenleben von Robin Hood im Sherwood Forest führen will, muss neben Bogenschießen auch Knöpfe annähen und Unterhosen waschen können. Genauso muss, wer sich als digitaler Rebell sehen möchte, selber Workarounds für Macken des Computers finden, das System zur Not über die Konsole administrieren und in gewissem Maße auch selber Systemfehler bereinigen können. Wer diese Tätigkeiten auf Dauer an Personen delegieren muss, denen er (oder sie) nicht vertrauen kann, verliert die Kontrolle über sein System und über seine Daten.

Für mich ist der in der Vorübung V2 nur kurz angetippte Konsolenbetrieb das ungeliebte digitale Pendant zum analogen Waschen von Unterhosen im Sherwood Forest. Ich versichere Ihnen aber, dass ich alles darangesetzt habe, in diesem Buch den Anteil solchen Gefummels auf das kleinstmögliche Maß zu beschränken. Ein in Computerdingen kundiger, vertrauenswürdiger Freund, der nicht nur Arbeiten abnimmt, sondern auch anleitet, aber Ihnen nicht einfach seine Meinung überstülpt, könnte Ihnen hier eine sehr große Hilfe sein. Überschätzen Sie aber nicht die Kenntnisse Ihres Computer-Wizard-Freundes in Kryptographie. Belastbare Kenntnisse in diesem Gebiet sind rar gesät.

Aus eigener Kraft kundig zu recherchieren, die Qualität von Quellen einzuschätzen und die Ergebnisse am eigenen System umzusetzen ist dagegen eine unverzichtbare Schlüsselkompetenz. Ich werde mich deshalb im Ablauf der Übungen dieses Buches zum Ende hin immer mehr von der Angabe detaillierter Schritt für Schritt Anleitungen zurückziehen und den Übenden mehr und mehr zum eigenständigen Recherchieren und Umsetzen animieren.

Wem eine Liste heute empfohlener und heute zu vermeidender Anwendungen und Apps wichtig ist und wer ohne allzu tiefe Suche nach Verständnis viele Datenlecks schnell schließen möchte, dem ist sicherlich mit dem Ratgeber zur "Digitalen Selbstverteidigung" vom Schweizer Pendant des CCC schneller geholfen, als mit diesem Buch. Ein Link zu diesem guten Ratgeber kann leicht mit der Suchmaschine Ihres Vertrauens gefunden werden. Sie werden damit allerdings keinen vollen Schutz und kein Verständnis erreichen.

1.7 U-Boot Kommunikation

Die ideale Kommunikation, zu der mit diesem Ratgeber angeleitet werden soll, lässt sich gut mit einem Bild aus der Seefahrt veranschaulichen. Ein mächtiger Gegner (ein staatlicher Nachrichtendienst, kurz der "Datenkrake") überwacht die Oberfläche des Meeres (das Internet). Ein ungekennzeichnetes U-Boot taucht auf (Ihr Computer geht anonym online), setzt eine Boje mit

einer perfekt verschlüsselten Nachricht ab und taucht wieder ab (geht offline). Ein nicht gekennzeichnetes U-Boot taucht eine gewisse Zeit später auf (der Computer Ihres Partners), nimmt die Boje mit der Nachricht auf und taucht wieder ab.

Der mächtige Gegner kann - wenn er sie rechtzeitig findet - die Boje untersuchen, beschädigen oder entfernen und mit der Entfernung seine Entdeckung und die Überwachung offenlegen. Er kann aber weder erkennen, nach welchem Verfahren die auf der Boje befindliche Nachricht verschlüsselt wurde, noch ob es sich überhaupt um ein Chiffrat (eine verschlüsselte Nachricht) handelt. Er weiß nicht, wer die Nachricht gesendet hat, kennt den Inhalt der Nachricht nicht und hat keine Information darüber, wer die Nachricht empfangen hat oder empfangen sollte. Er hat einzig die Information, dass vermutlich an ihm vorbei kommuniziert wurde oder werden sollte.

Ich verfolge mit diesem Ratgeber das Ziel, eine solche perfekt geschützte Kommunikation zu erreichen, sozusagen mit Ihnen zusammen den für intelligente Laien erreichbaren Gipfel der sicheren elektronischen Kommunikation zu erklimmen. Wenn Sie dann später Ihre eigene Alltagskommunikation absichern wollen, wird natürlich auch der Komfort eine Rolle spielen und Sie werden im Alltag für sich selbst Ihren persönlichen Kompromiss zwischen Komfort und Sicherheit, je nach Intensität der Bedrohung, finden können. Bei Bedarf sollen Sie aber wissen, wie es wieder ganz nach oben geht; Sie waren schon mal da und kennen den Weg.

Ich sehe auf dem Weg zu einer dem Seefahrtsbild analogen perfekt geschützten elektronischen Kommunikation vier abgrenzbare Fertigkeitsstufen, die aufeinander aufbauen und jeweils die Beherrschung der darunter liegenden Fertigkeitsstufen voraussetzen.

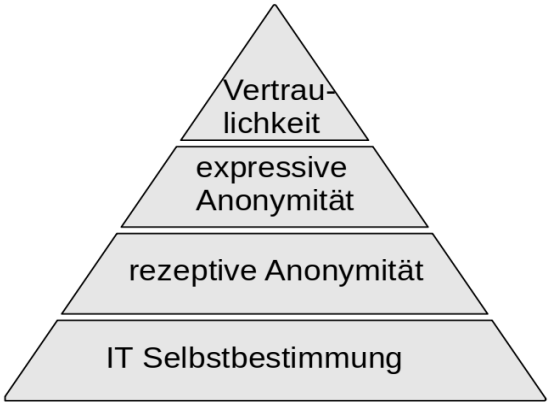


Abbildung 2: Pyramide der sicheren elektronischen Kommunikation, gesichert gegen einen Abhörstaat. Kurz hier auch Pyramide des Dissidentenschutzes genannt.

Im Folgenden wird es in diesem Ratgeber um das Streben nach Vervollständigung dieser Pyramide der sicheren elektronischen Kommunikation gegen den Abhörstaat gehen. Ich nenne diese Pyramide auch die "Pyramide des Dissidentenschutzes".

1.8 Grundstruktur der folgenden Kapitel

Die Pyramide der sicheren elektronischen Kommunikation aus den vier Fertigkeitsstufen wird systematisch, Schritt für Schritt, Fertigkeitsniveau für Fertigkeitsniveau aufgebaut. Hierbei kann erst auf Basis bestehender, belastbarer Anonymität die Vertraulichkeit durch eine anonymitätskompatible Verschlüsselung eingeführt werden.

Die Fähigkeit zur sicheren elektronischen Kommunikation ist nur durch einen systematischen Lernprozess zu erreichen, der nicht durch einfaches Durchlesen eines Ratgebers absolviert werden kann. Das geht so wenig, wie man durch Durchlesen eines Buches über das Klavier das Klavierspielen erlernen kann. Jedes durch theoretischen Rahmen und praktische Übungen vorgestellte Fertigkeitsniveau ist nur durch gewisse Anstrengung zu erreichen. Aber jedes erklommene Niveau eröffnet neue Möglichkeiten der Verweigerung der digitalen Unterdrückung und bringt ganz nebenbei erhöhte Widerstandskraft gegen gewöhnliche Internetkriminalität.

Für jedes Fertigkeitsniveau werden zuerst abstrakt die Ziele und erforderlichen Maßnahmen beschrieben. Im darauf folgenden Teil werden bezüglich des Fertigkeitsniveaus konkrete Vorschläge gemacht, mit welchen ausschließlich kostenfreien Werkzeugen sich zum heutigen Zeitpunkt die jeweiligen Ziele meines Erachtens am besten erreichen lassen. Es folgen Vorschläge für Übungen mit den Werkzeugen, die Ihnen diese Fertigkeiten praktisch erschließen. Zum Abschluss jedes dem Fertigkeitsniveau zugeordneten Kapitels weise ich auf die meiner Meinung nach wichtigsten Angriffspunkte und Verwundbarkeiten hin.

Hierbei beschränke ich mich auf Werkzeuge für die Desktopsysteme Linux und Windows. Viele von diesen Werkzeugen könnten aber auch auf Apple Computern genutzt werden. Bezüglich Smartphonesystemen besitze ich bei weitem nicht genug Erfahrung, um zur Basis der Pyramide, der IT-Selbstbestimmung, auf diesen Systemen anleiten zu können. Diese werden in diesem Buch deshalb nicht von mir behandelt.