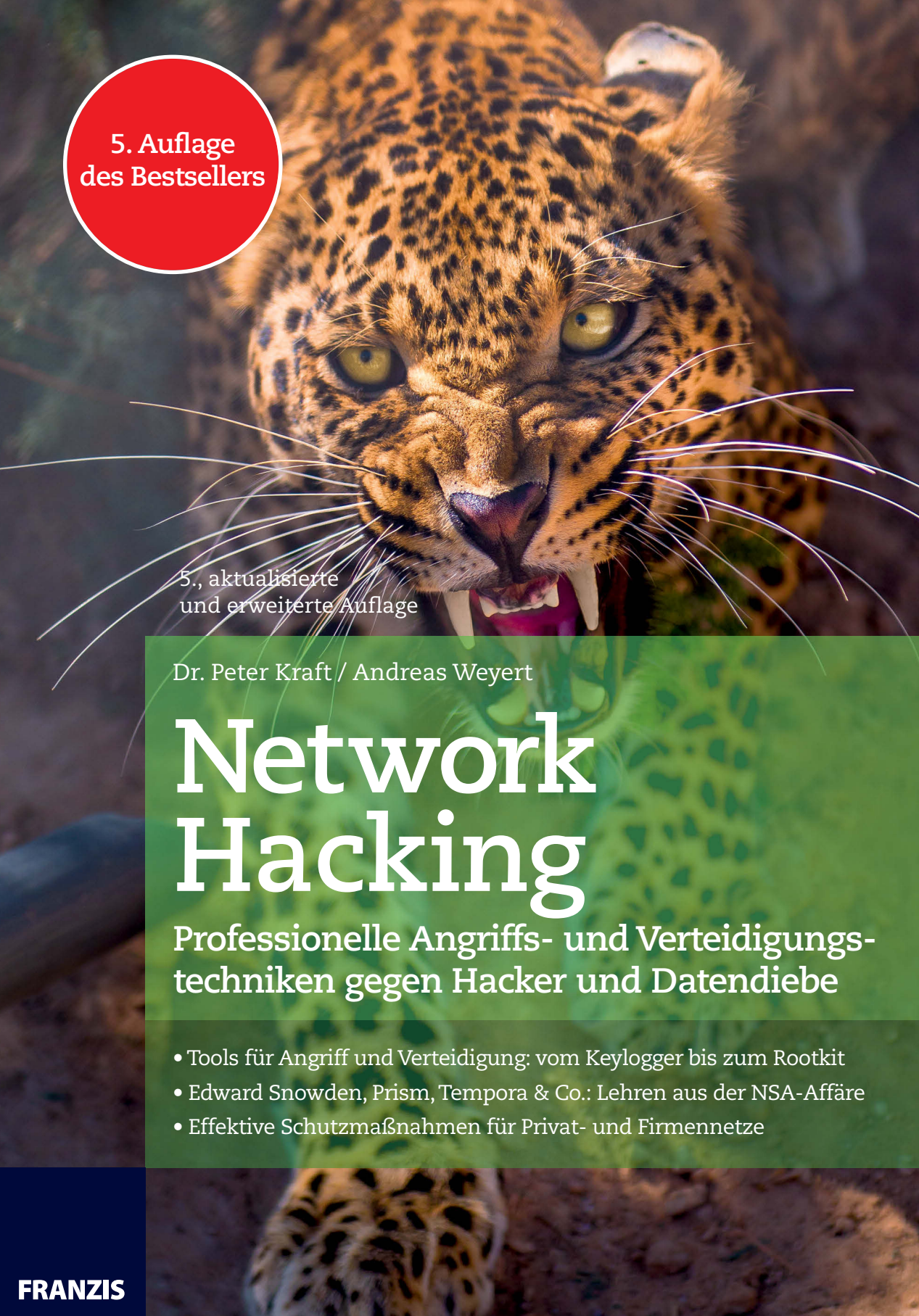

5. Auflage des Bestsellers

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*

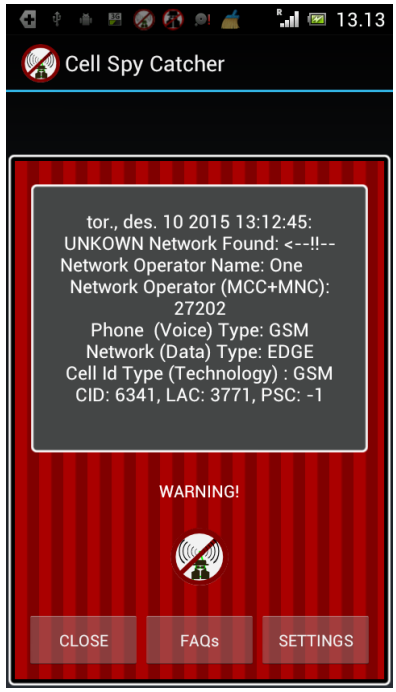

Bild 1.1: Cell Spy Catcher

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*.

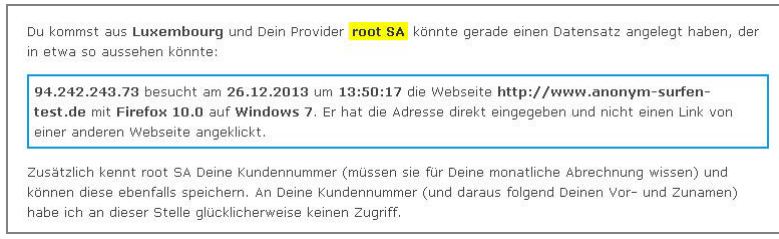

Bild 1.2: IP-Test 1

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*