

Tobias Schrödel

Ich glaube, es hackt!

Ein Blick auf
die irrwitzige Realität
von Computer,
Smartphone
und IT-Sicherheit



Springer

Ich glaube, es hackt!

Tobias Schrödel

Ich glaube, es hackt!

Ein Blick auf die irrwitzige
Realität von Computer, Smartphone
und IT-Sicherheit

4., aktualisierte und erweiterte Auflage



Springer

Tobias Schrödel
IT Security & Awareness
München
Deutschland

Die 1. und 2. Auflage sind im Imprint von Springer Gabler erschienen,
unter dem Titel: „Hacking für Manager – IT-Sicherheit für alle, die wenig
Ahnung von Computern haben.“

ISBN 978-3-658-10857-1 ISBN 978-3-658-10858-8 (eBook)
DOI 10.1007/978-3-658-10858-8

Die Deutsche Nationalbibliothek verzeichnetet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer

© Springer Fachmedien Wiesbaden 2011, 2012, 2014, 2016

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Lektorat: Stefanie Brich

Foto: Marc-Steffen Unger mit freundlicher Genehmigung von Deutsche Telekom AG

Coverdesign: deblik Berlin

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature

Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden

Inhalt

1	Vorspiel	1
1.1	Von Hackern und Datenschnüfflern – Worum es geht und wie die Spielregeln sind	1
1.2	Du kommst aus dem Gefängnis frei – Was der Leser wissen muss	3
1.3	Oma Kasupke und die Expertenattrappe – Warum IT-Experten im Fernsehen nie die (volle) Wahrheit sagen (können)	5
2	Geldkarten & -automaten	9
2.1	Epileptische Karten – Warum Geldkarten im Automaten so ruckeln	9
2.2	Rot – Gelb – Geld – Wieso die PIN nicht auf der Geldkarte gespeichert ist	10
2.3	Demenzkranker Käse – Wie man sich PINs merken und sogar aufschreiben kann	13
2.4	Hände hoch, keine Bewegung! – Wie Geldautomaten mit Fehlern umgehen	15
2.5	Kommissar Zufall – Wie die Kartenprüfnummer einer Kreditkarte funktioniert	17
2.6	Dummdreist nachgemacht – Warum Kreditkarten kopieren gar nicht so einfach ist	19
2.7	Ganz nah – Wie NFC unser Bezahlverhalten verändern wird	22

3	Office-Anwendungen, Dateien & Betriebssystem	25
3.1	Altpapier und Recycling – Warum gelöschte Dateien gar nicht gelöscht sind	25
3.2	Rohstoffverschwendung im Sinne des Datenschutzes – Wie Dateien wirklich sicher gelöscht werden können	30
3.3	Weitere Informationen finden Sie im Kleinstgedruckten – Was an versteckten Informationen in Word-Dokumenten steht	32
3.4	Wer hat Angst vorm schwarzen Mann – Wie man anonymisierte Textstellen in PDF-Dokumenten sichtbar macht	38
3.5	Wer lesen kann, ist klar im Vorteil – Wie man mit falschen Fehlermeldungen Schadcode installieren kann	42
3.6	Turbolader – Warum der Computer immer langsamer wird und was dagegen hilft	44
3.7	Made in USA – Warum man in sicherheitsrelevanten Bereichen auf Software aus den USA verzichtet	46
3.8	Bildausfall – Warum es heute wirklich keine Ausrede mehr für ein fehlendes Backup gibt	48
3.9	So ein Zufall – Wie Computer zufällige Zahlen erzeugen, obwohl sie das gar nicht können	49
3.10	Fasse dich kurz, Philae – Wie man Daten komprimiert und was es dabei für Unterschiede gibt	51
3.11	Der, die, das, wieso, weshalb, warum? – Warum die Genderdiskussion auch Computerprogramme in Bedrängnis bringt	53
3.12	Einmal um die Sonne bitte – Wie Computer berechnen können, wann ein Schaltjahr ist	55
3.13	Reboot tut gut – Wie ein Computer Zahlen speichert und was ein Overflow ist	57
3.14	Wer hat an der Uhr gedreht? – Welche Auswirkung eine zusätzliche Schaltsekunde auf Computer haben kann	59

3.15	Mer losse d'r Dom en Kölle. Oder auch nicht. – Warum Fotos (vielleicht) wissen, wo sie aufgenommen wurden	61
4	Passwörter & PINs	65
4.1	Passwort hacken – Wie schlechte Passwörter geknackt und sichere erstellt werden	65
4.2	8ungH4cker! – Wie man sich sichere Passwörter merken kann	70
4.3	Zählwerk – Wie man den gleichen Passwortstamm in verschiedenen Systemen variieren kann	72
4.4	Seltene Zeichen – Wie man sein Passwort noch aufwerten kann	73
4.5	Honigtöpfe – Wie man Ihnen Login-Daten klaut und was Sie dagegen tun können	74
4.6	Das Übel an der Wurzel – Wie man erkennt, ob Passwort-Safes gut sind	77
4.7	Erst eingeschleift, dann eingeseift – Warum selbst gute Passwörter gegen KeyKatcher keine Chance haben	80
4.8	Der Wurm im Apfel – Wie man an der PIN- Eingabe von iPad und iPhone vorbei kommt	83
4.9	Doppelt genährt hält besser – Was die Zwei-Faktor-Authentifizierung ist und welche Vorteile sie hat	86
4.10	Mit dem falschen Wisch ist alles weg – Warum Wischmuster zum Schutz von Handys genauso gut/schlecht sind wie PINs	89
4.11	Cyberwar: Shutdown Deutschland – Der Krieg im Netz läuft schon. Zumindest Stufe 1 von 4 ...	93
5	Internet	97
5.1	Zahlenspiele – Was in einer Minute im Internet alles passiert	97
5.2	Empfänger Unbekannt – Wie man anyonym im Internet surfen kann	99

5.3	Dioptrin und Farbenblindheit – Was sind Captchas und wie funktionieren sie	102
5.4	Du kommst hier net rein – Warum das CAPTCHA eigentlich erfunden wurde	104
5.5	Schlüssel steckt – Warum man keine Passwörter im Browser speichern sollte	106
5.6	Zahlung sofort, ohne Skonto – Wie Abofallen im Internet funktionieren	109
5.7	640 Sextillionen – Warum IP V6 nicht nur Probleme löst	113
5.8	.berlin .berlin Wir surfen nach .berlin – Was man bei den neuen Webseiten-Endungen beachten sollte	116
5.9	Erst gucken, dann anfassen – Wie ein Link im Internet manipuliert werden kann	119
5.10	Drive-by – Wie man sich Viren beim Surfen einfängt und was man dagegen tun kann	122
5.11	Ob groß, ob klein – Warum es im Internet meistens egal ist, ob man Groß- oder Kleinschrift verwendet	125
5.12	Aussage gegen Aussage – Warum man nicht jede Aussage glauben sollte, die irgendwie geschrieben steht	127
5.13	Es wiehert auch im Internet – Warum ein DSL-Anschluss eigentlich nie so schnell ist, wie drauf steht	129
5.14	Gerührt, nicht geschüttelt – Was der Unterschied zwischen Trojaner, Virus und Computerwurm ist	130
5.15	Dunkel und tief – Was das Darkweb (Deepweb) ist	132
5.16	Bitte keine Werbung – oder doch? – Warum Werbe-Blocker zwar praktisch sind, aber kontraproduktiv	133
5.17	Ein eindeutig eindeutiger Fingerabdruck – Wie uns Webseiten mittels Canvas Fingerprinting wiedererkennen	135

5.18	Frechheit! Als ich das las, kochte die Wut in mir hoch – Mit welchen Tricks im Netz um Ihren Klick gekämpft wird	138
5.19	Alle Zwerge sind gleich. Aber manche sind gleicher. – Was Netzneutralität ist und warum sie wichtig ist	140
5.20	Big Data & Das Ende von Glück und Vielfalt – Viele Daten zu sammeln kann verdammt gut sein ... oder verdammt schlecht	141
5.21	Ich weiß, wem Du letzten Sommer geschrieben hast – Welche Daten bei der Vorratsdatenspeicherung erfasst werden	145
5.22	Bitte nicht füttern – Wie (bezahlte) Trolle im Internet stören und wie man sich verhalten sollte	147
5.23	Hört mir eigentlich jemand zu? – Wie man sogar vor Geheimdiensten geheim kommunizieren kann	150
6	Online-Shopping	155
6.1	Alles, außer Tiernahrung – Wie man kostengünstig(er) im Internet einkaufen kann	155
6.2	Es kracht – Wie Fake-Shops funktionieren	158
6.3	Weihnachtseinkäufe – Wie man betrügerische Online-Shops erkennen kann	160
6.4	Auf Pump – Warum gute Online-Shops Ihre Kreditkartendaten gar nicht haben wollen	163
6.5	Personalisierte Werbung – Warum personalisierte Werbung wirtschaftlich positiv, ansonsten aber negativ ist	165
7	Google, Facebook & Co.	169
7.1	Nachmacher – Warum Google gar nicht so innovativ ist, wie wir immer glauben	169
7.2	Golf ist nicht gleich Golf ... – Wie Google anonyme Suchanfragen personalisiert	170
7.3	BigBrother ohne Container – Wie Google hilft, fremde Wohnzimmer auszuspionieren	173

X	Ich glaube, es hackt!	
7.4	Heiße Hunde – Wie sich Suchmaschinen in den nächsten Jahren verändern werden	175
7.5	Lachst Du noch oder mobbst Du schon – Warum soziale Netzwerke mehr tun müssen, als den Service aufrecht zu erhalten	177
7.6	Das Schaf im Wolfspelz – Warum Facebook total überbewertet ist	182
7.7	Gartenparty – Wer haftet eigentlich, wenn die Tochter über Facebook die ganze Welt einlädt ...	184
7.8	Facebook verkauft private Urlaubsbilder seiner Nutzer – Warum sich Facebook mit seinen AGB so weitreichende Rechte einräumt	185
7.9	Dieser Text ist in deinem Land nicht verfügbar – Wie die Ländersperre bei YouTube funktioniert und überwunden werden kann	187
7.10	Ali Baba und die 1.000 Freunde – Eine Anregung für hilflose Eltern beim Umgang mit ihren Kindern und Facebook	190
7.11	Ausgesperrt – Wie man ohne Passwort fremde Facebook-Accounts kapert und wie man das verhindert	192
7.12	Der König ist tot, es lebe der König – Wie man Facebook-Freunde kaufen kann und erkennt, wer das getan hat	194
8	Online-Banking	197
8.1	Der Bankschalter im Wohnzimmer – Wie sicher ist Online-Banking mit PIN und TAN	197
8.2	Ein Elektron, was kann das schon? – Was man benötigt, um eine sichere Verbindung zu knacken	199
8.3	Der unbekannte Dritte – Wie eine Man-in- the-Middle-Attacke funktioniert	200
8.4	Sicherheitsgetreide – Wie die sichere Schlüssel-Übergabe beim Online-Banking funktioniert	203

8.5	The revenge of the Sparkasse – Wie sich Banken gegen Phishing wehren	205
8.6	Zufällig ausgewählt – Wie die iTAN funktioniert und warum sie eingeführt wurde	207
8.7	Mobiler Hilfssheriff – Was die mTAN besser kann als die iTAN	210
8.8	Verkehrte Welt – Was sich beim sicheren Online-Banking für Sie ändert	212
8.9	Doppelt hält besser – Wie es gelungen ist, das mTAN-Verfahren kaputt zu machen	214
8.10	Im Sandkasten – Wie mit einer kleinen Änderung das mTAN-Verfahren doch wieder sicher ist	217
8.11	Malen statt Zahlen – Welche Ideen es gibt, um Online-Banking noch sicherer zu machen	219
8.12	Rücküberweisung – Welche raffinierten Tricks angewendet werden, um an Ihr Geld zu kommen	221
8.13	Schnäppchenjäger – Warum WesternUnion Moneytransfer und ähnliche Dienste keine Überweisungen sind	224
8.14	Meine Bank hat einfach zu viele Nullen – Warum die IBAN eigentlich gar nicht so schlimm ist, wie sie aussieht	226
9	E-Mail & Spam	229
9.1	Blutleere Gehirne – Wieso wir SPAM-Mails bekommen	229
9.2	Leicht drauf, schwer runter – Wie man keine SPAM-Mails mehr bekommt	231
9.3	Elektronische Postkarte – Warum E-Mails wie Postkarten sind	233
9.4	Chance verpasst – Was Facebook und verschlüsselte E-Mails gemeinsam haben	236
9.5	xbbgxgievkhevfknxuifakxe – Warum wir alle verschlüsseln sollten und das auch einfach geht ...	237

9.6	Ich sehe was, was Du nicht siehst – Wie man Adressen bei Rundmails eingibt	239
9.7	Nicht lesen! – Was von Datenschutz-Klauseln am Ende einer Mail zu halten ist	242
9.8	Urlaub – Was eine Abwesenheitsnotiz für Informationen enthalten sollte	244
9.9	Rotwein – Wo das @-Zeichen in der E-Mail ursprünglich herkommt	245
9.10	Emotionen 2.0 – Wieso Smileys heute eine ziemlich wichtige Rolle spielen	247
10	WLAN & Funknetze	251
10.1	Never Touch a Running System – Welches die richtige WLAN-Verschlüsselung ist	251
10.2	Geschwindigkeit ist keine Hexerei – Warum das WLAN mal langsam sein kann, und wie man das ändert	254
10.3	Wenn einer eine Reise tut ... – Wie das WLAN Signal in den Zug kommt	258
10.4	Datenklau durch Kartoffelchips – Wie man mit einer Chipsdose eine WLAN-Richtfunkantenne bauen kann	259
10.5	Live-Schaltung ins Nachbarhaus – Wie man mit einem Babyfon fremde Schlafzimmer ausspioniert	262
10.6	Fenster oder Gang? – Warum Funktastaturen zwar bequem, aber unsicher sind	265
11	Filme, Musik & Fernsehen	269
11.1	Jäger und Sammler – Wie man seine CD-Sammlung legal kopieren kann	269
11.2	Unerhört – Wie das mp3-Verfahren funktioniert	272
11.3	Ein Kapitel nur für Männer – Wie Pay-TV im Hotel funktioniert	275
11.4	Public Viewing – Was die Filmindustrie nicht bekämpfen kann	277

11.5	Fernsehen nur für mich – Wie IP-TV das Fernsehen revolutionieren wird	279
11.6	Volle Batterien – Wie man Infrarotlicht sichtbar machen kann	281
11.7	Erster! – Warum beim Fernsehen manche eher jubeln	283
11.8	Wir schalten um zu Olympia – Warum live im Fernsehen nicht unbedingt live ist	286
11.9	Ohne Visum – Warum es bei der DVD einen Ländercode gibt	288
12	Biometrie	289
12.1	Biometrischer Reisepass – Wie man den Fingerabdruck aus dem Reisepass entfernt	289
12.2	Filigrane Linien – Wie man mit Holzleim Fingerabdrücke imitieren kann	293
12.3	Sicherheit auf Knopfdruck – Warum der geknackte Fingerabdrucksensor des iPhone trotzdem gut ist	295
12.4	Links ist da, wo der Daumen rechts ist – Was das persönliche Tippverhalten über einen verrät	297
12.5	Hinterteil – Welche Methoden angedacht sind, um Menschen biometrisch zu erkennen	301
13	Unterwegs	303
13.1	Blitz – Warum Blitzer-Warner verboten sind, aber trotzdem erlaubt	303
13.2	Bitte lächeln – Warum Dash-Cams immer beliebter werden	305
13.3	Endlich Steuerfrei – Warum das selbstfahrende Auto nicht nur eine technische Herausforderung ist	306
13.4	ConferenceCall im Großraumwagen – Wie man im Großraumwagen etwas Privatsphäre bekommt	308
13.5	Wuuup, Wuuup – Wie die funkgesteuerten Schlüssel bei Autos funktionieren	310

13.6	Knochenspiegel – Wie man die Reichweite eines Funkschlüssels erhöhen kann	312
14	Telefon, Handy & Co.	315
14.1	Ganz schön mies – Warum seit Jahren Handys abgehört werden können und keiner etwas dagegen tut	315
14.2	Das Merkel-Handy – Wie Crypto-Handys funktionieren	319
14.3	Telefonbuch online – Wie man per Bluetooth an das gespeicherte Telefonbuch eines Handys kommt	326
14.4	Frisch erpresster Datensalat – Warum auch ein Mac einen VirensScanner braucht	331
14.5	Ungeziefer am Körper – Wie man Bluetooth-Headsets als Wanze missbrauchen kann	334
14.6	Pakete ohne Zoll – Was man bei Voice-over-IP beachten sollte	338
14.7	Deine ist meine – Wie man mit VoIP fremde Rufnummern zum Telefonieren verwenden kann	340
14.8	Kein Schwein ruft mich an – Fangschaltung kann jeder, nicht nur die Polizei	342
14.9	Komfortrauschen als Lebensretter – Warum unsere Handys mit Absicht rauschen	345
14.10	0180-GUENSTIG – Wie man bei kostenpflichtigen Servicenummern zum Nulltarif anruft	347
14.11	Umziehen – Warum beim Umzug der Telefonanschluss oftmals nicht mit umzieht	348
14.12	Nach Hause telefonieren – Warum ein Handy klingeln kann – egal wo es sich auf der Welt befindet	351
14.13	Das macht alles keinen SIM – Warum wir bald keine SIM Karte mehr brauchen und das nicht nur Vorteile hat	354

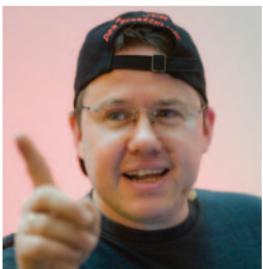
14.14	Dieser Anruf wird zu Schulungszwecken aufgezeichnet – Was mit unserem Anruf im CallCenter passiert	356
14.15	Wie sag ich's meinem Chef – Wie man beim Handy direkt auf der Mailbox landet	359
14.16	Geschenkt ist nicht umsonst – Warum In-App-Käufe problematisch und sinnvoll zugleich sind	361
14.17	Die Mutter aller Sicherheitslücken – Warum man Updates auch für alte Geräte immer einspielen sollte	364
14.18	Oh freuet euch sehr – aber nicht zu früh – Welche neuen Krankheiten uns die Smartphones von heute bescheren	366
15	Der Faktor Mensch	369
15.1	Sauber machen – Wie man geschützte Objekte betreten und dort Dokumente stehlen kann	369
15.2	Fach-Chinesisch für Frau Schneider – Wie man Laien unter Druck setzt, um an geheime Daten zu gelangen	372
15.3	Finderlohn – Wie man Mitarbeiter dazu bewegt, einen Trojaner im Firmennetz zu installieren	375
15.4	Früher war alles besser – Warum man Kinder zum Lügen animieren sollte	378
15.5	Was weg ist, ist weg – Wie sich die Rechtsprechung verändern und an virtuelle Welten anpassen muss	380
15.6	Gewinnsucht – Wie man Menschen dazu bringt, User-ID und Passwort zu verraten	383
15.7	Promi-Bonus – Wie mit Social Engineering persönliche Daten abgegriffen werden	384

16	Hardware	389
16.1	Mein Drucker hat Masern – Was man bei Farblaser-Ausdrucken alles herausfinden kann	389
16.2	Yum Kotyen dieses Kezboard – Warum nicht alle Tastaturen auf dieser Welt gleich sind	391
16.3	Aufhebungsvertrag für Dokumente – Warum Kopiergeräte immer eine Zweitkopie erstellen	394
16.4	Rasterfahndung – Wie man Webcams als Bewegungsmelder nutzt	396
16.5	Rattenscharf – Wie Digitalkameras schärfere Bilder als die Wirklichkeit erzeugen	398
16.6	Anti-Feature – Mit welchen Tricks wir zum Kauf von teurem Original-Zubehör gezwungen werden	400
16.7	Duftwasser – Wie die Hersteller erklären, warum Druckertinte so teuer ist	402
16.8	Hinterher ist man immer schlauer – Wie man leere Drucker doch noch mal zum Drucken bewegen kann	403
16.9	Und sie dreht sich doch ... – Wie Sensoren Bewegungen erkennen und wissen, wann jemand vorbei läuft	406
16.10	Hab dich! – Wie man seinen gestohlenen Laptop wieder bekommt	408
16.11	Apfel oder Fenster – Warum ein Mac nicht grundsätzlich sicherer ist als ein Windows PC	412
16.12	Rohstoffe – Was seltene Erden sind und wozu sie gebraucht werden	413
16.13	Auf Sand gebaut – Warum Seltene Erden gar nicht so selten sind	415
16.14	Abgesoffen – Warum eine technische Angabe nichts mit der Wirklichkeit zu tun haben muss	417

16.15	Rohlinge – Warum die beschreibbare CD bereits nach kurzer Zeit zum Auslaufmodell wurde	418
16.16	Die dritte Dimension – Wie 3D-Drucker unser Leben verändern werden	420
16.17	Aus die Maus – Warum die Computermaus den Umgang mit dem Computer revolutioniert hat	422
16.18	Größer, schneller, weiter – Warum Innovationen nicht jeden Monat erscheinen können	424
17	Historische Geschichten	427
17.1	Das Ende ist nah – Warum es das Jahr-2000-Problem gab und welche Probleme noch kommen	427
17.2	Altmodisch – Warum alte Spionagetechniken selbst heute noch wichtig sind	429
17.3	Kurzfassung – Wie man beim Telegrafieren Geld sparen konnte	430
17.4	Die Griechen haben angefangen – Wie man Daten ohne Computer verstecken kann	432
17.5	Vigenère und Kasiski – Wie nach 300 Jahren die sicherste Verschlüsselung der Welt geknackt wurde	434
17.6	Ideenklau von Lord Playfair – Wie eine Urheberrechtsverletzung vor 150 Jahren begangen wurde	436
17.7	Deutsches Liedgut – Wie man Passwörter besser nicht macht	437
17.8	Kopierschutz für Bücher – Wie früher das Urheberrecht geschützt wurde	439
17.9	Das griechische Rätsel – Warum die Enigma nie geknackt wurde und es trotzdem jeder glaubt	441

XVIII	Ich glaube, es hackt!	
17.10	Karotten sind gut für die Augen – Warum Geheimhaltung so wichtig ist und wie Legenden geboren werden	444
	Stichwortverzeichnis	449

Über den Autor



Tobias Schrödel Jahrgang 1971, ist „Deutschlands erster Comedyhacker®“. Der Münchener beschreibt seit über 15 Jahren technische Systemlücken so einfach und verständlich wie möglich. Der gezielte Einsatz ungewöhnlicher Stilmittel machen seine Vorträge zu einem besonderen Erlebnis, so dass auch Laien Spaß an der IT-Sicherheit bekommen. Als Redner über IT-Themen wird er mittlerweile weltweit gebucht. Seit 2011 ist Tobias Schrödel das stern TV-Gesicht, wenn es um IT-Sicherheit und Computer geht. Technische Zusammenhänge erläutert er aber immer wieder auch für andere TV-Sendungen (z.B. WISO, Explosiv, Akte).

Der ausgebildete Fachinformatiker war viele Jahre als technischer Consultant für IT-Security bei T-Systems, einem der größten international operierenden Dienstleister für Informations- und Kommunikationstechnologie, tätig und weiß daher, wovon er spricht. Bevor er in den Konzern Deutsche Telekom AG wechselte, war Tobias Schrödel bei United Parcel Service für die Entwicklung von Logistik-Lösungen im Enterprise Business Bereich verantwortlich.

Neben seinem Buch, das in der 1.Auflage unter dem Titel „*Hacking für Manager*“ mit dem internationalen getAbstract

Award als Wirtschaftsbuch des Jahres 2011 ausgezeichnet wurde, veröffentlicht er immer wieder Fachartikel in IT-Zeitschriften. Schrödel, selbst Ausbilder für IT-Berufe, prüft seit mehr als einem Jahrzehnt angehende Fachinformatiker für die IHK München und hielt zudem viele Jahre Gast-Vorlesungen an der Ludwig-Maximilian-Universität in München.

Persönlich beschäftigt sich der gebürtige Münchener mit historischer Kryptoanalyse und Sicherheitslücken in alltäglichen IT und Elektronik-Produkten. Er möchte dabei Anwender sensibilisieren und zum Nachdenken anregen. Als Experte für historische Geheimschriften hat er nach über 450 Jahren einen Weg zu gefunden, um kurze Vigenère-Schriften zu entschlüsseln und besitzt eine umfangreiche Bibliothek mit alten Büchern über Kryptographie und Geheimschriften.

Schrödel schreibt einen wöchentlichen Blog, der auch als Kolumne in einer norddeutschen Zeitung erscheint und der für viele Kapitel Ideengeber war. Updates zum Buch, Kommentare und neue Themen können Sie dort nachlesen:

<http://www.ich-glaube-es-hackt.de>

1

Vorspiel

1.1 Von Hackern und Datenschnüfflern – Worum es geht und wie die Spielregeln sind

Blicken Sie seit Edward Snowdens Enthüllungen überhaupt noch durch? Die NSA knackt SSL, sammelt Metadaten und hört dank mangelnder Sicherheit der A5/1-Verschlüsselung auch Handygespräche über GSM ab.

Fremdwörter, Fachbegriffe und Abkürzungen ohne Ende. Früher war das „Hacken“ von Systemen noch einfach. Da wurde mit der spanischen Münze aus dem Urlaub der Kaugummiautomat überlistet. Das Geldstück hatte die gleiche Größe wie der Groschen, wog in etwa das selbe, war aber nur einen Bruchteil wert und brachte damit eine enorme Gewinnspanne – prozentual gesehen.

Das hat noch jeder verstanden und der Trick mit der spanischen Münze wurde nur unter der Hand weitergereicht, von Kumpel zu Kumpel. Ich verrate Ihnen in diesem Buch, wie das mit den Kaugummis in der virtuellen Welt – im so genannten Cyberspace – funktioniert. Dabei versuche ich, das ganze so einfach und verständlich wie möglich zu halten. Also keine Sorge, es

geht hier nicht nur um Bits und Bytes. Sie müssen weder Computerfachmann noch IT-Profi sein.

Da draußen lauern übrigens weitaus mehr Möglichkeiten gehackt zu werden, als wir uns vorstellen. Die Technik, die uns heute überschwemmt, lässt uns gar keine Chance mehr, alles so abzusichern, dass wir auch wirklich sicher sind.

Manche Lücken stecken im Detail, andere Systeme hingegen sind so offen, wie das sprichwörtliche Scheunentor. Wir müssen uns allmählich Gedanken machen, ob wir jeder neuen Technik weiterhin mit dem Grundvertrauen eines Kindes begegnen können und dürfen.

Möchten Sie im Hotel kostenlos Pay-TV sehen? Oder den Fingerabdruck aus Ihrem neuen Reisepass entfernen? Nutzen Sie Bluetooth und tragen dadurch unfreiwillig eine Wanze am Körper? Wollen Sie endlich verstehen, wie das mit der PIN bei der Geldkarte funktioniert oder warum gelöschte Daten gar nicht gelöscht sind? Dieses Buch erklärt Ihnen all das verständlich.

Allerdings geht es nicht nur um das Knacken irgendwelcher Verschlüsselungen oder gar von Zugangsbeschränkungen. Manches, was uns heute noch spanisch vorkommen mag, hat durchaus einen ernsten Hintergrund. Einige Geräte sind absichtlich komplizierter als sie sein müssten. Oft ist aber die Umständlichkeit ganz bewusst implementiert, um die Sicherheit des Systems zu erhöhen. Es sagt uns nur niemand, warum das so ist.

Leider sind nicht alle IT-Menschen in der Lage, die Gründe ihres Tuns verständlich zu äußern und zu erklären. Deshalb können wir manche ihrer Vorgaben nicht nachvollziehen und halten es für Gängelei, wenn Passwörter alle vier Wochen geändert werden müssen und obendrein immer komplizierter sein sollen. Tatsächlich gibt es fast immer – für uns unverständliche – Gründe.

Die dahinter stehenden Motive sind in Wirklichkeit nicht viel schwieriger zu verstehen als der Kaugummi-Trick mit der spanischen Münze. Drehen wir den Spieß also um. Ich erkläre Ihnen in diesem Buch, wie das alles funktioniert und mache Sie so auch ein wenig selbst zum Hacker. Dadurch sind Sie in der Lage, sich zu schützen und zu erkennen, welchen Risiken Sie ausgesetzt sind (Abb. 1.1).

1.2 Du kommst aus dem Gefängnis frei – Was der Leser wissen muss

Der Autor weist ausdrücklich darauf hin, dass die Anwendung einiger, die in diesem Buch vorgestellten, Methoden illegal ist oder anderen Menschen wirtschaftlich schaden kann.

Dieses Buch stellt keine Aufforderung zum Nachmachen oder gar zur Durchführung illegaler Handlungen dar. Auch dann nicht, wenn eine ironische Schreibweise dies an mancher Stelle vermuten lässt.

Einige der vorgestellten Techniken sind relativ alt. Das ändert jedoch nichts an der Tatsache, dass sie heute noch funktionieren. Ich beschreibe sie, weil durch sie auch dem normalen PC-Anwender die Augen geöffnet werden.

Der Sinn und Zweck dieses Buches ist die Erhöhung der Aufmerksamkeit („Awareness“) des Lesers bei der Nutzung und dem Einsatz von IT im privaten und geschäftlichen Umfeld. Dies ohne die Vermittlung unnötiger technischer Tiefen und Begriffe, die wirklich keinen interessieren.

Es ist kein Lehrbuch für IT-Profis und Informatiker.



Abb. 1.1 Dieser Kaugummiautomat von 1966 konnte mit ausländischen Münzen überlistet werden. Eine Sicherheitslücke, die mit Einführung des Euro geschlossen wurde

1.3 Oma Kasupke und die Expertenattrappe – Warum IT-Experten im Fernsehen nie die (volle) Wahrheit sagen (können)

Seit dem tragischen Unglück in Fukushima weiß jedes Schulkind, wie ein Atomkraftwerk funktioniert. N24 und n-tv überboten sich gegenseitig in grafischen Darstellungen, die kinderleicht erklären, wie so ein Siedewasser-Reaktor läuft – wenn er nicht gerade beschädigt ist.

Nur: War das auch alles wirklich richtig dargestellt? Die Teilchenphysiker unter Ihnen haben sicherlich sofort festgestellt, dass da hunderte Messfühler, Pumpen und sonstiges Zeugs auf der Grafik fehlen. Denn wenn es tatsächlich sooo einfach wäre, dann hätte sicherlich auch schon jeder Schurkenstaat ein eigenes Atomkraftwerk und müsste das Know-how nicht teuer aus Russland, China oder der EU einkaufen.

Macht nix, denken Sie vielleicht, es ging ja darum, das Prinzip zu erklären und auch für Nicht-Atomphysiker verständlich darzustellen, was da gerade passierte.

Nun, dieses Vorgehen versuche ich auch zu nutzen. Sei es in diesem Buch bei der Erklärung komplexer Themen, aber vor allem auch im Fernsehen, wenn ich als so genannter Experte etwas für Nicht-Informatiker und Computer-Laien erklären soll.

Es geht nicht darum, alles hundertprozentig korrekt zu erläutern, es geht darum, dass auch ein Laie versteht, was da gerade passiert. Dazu muss man ein paar Eventualitäten, ein paar Randbedingungen unter den Tisch fallen lassen.

Was aber bedeutet das für einen Wissenschaftler, einen echten Experten? Er wird die Darstellung als ungenau, ja eventuell sogar als falsch klassifizieren. Und das Schlimme daran ist, dass das auch noch stimmt. Der Experte hat Recht.

Nun hat eine schematische Darstellung eines Siedewasser-Reaktors aber einen Vorteil: Jeder versteht, worum es geht. Auch Oma Kasupke.

Oma Kasupke ist eine fiktive Person, die in den Köpfen der TV-Redaktionen als Dummy-Zuschauer herhalten muss. Sie ist der DAFZ – der dümmste anzunehmende Fernsehzuschauer. Und bei jeder Erklärung soll der Experte an Oma Kasupke denken. Würde sie verstehen, was er sagt? Wenn nein, verliert sie den Faden und damit auch den Bezug zur Sendung und schaltet um. Das ist der GAU, diesmal nicht für Reaktoren, sondern für Redaktionen.

Gerade IT-Experten haben es im Fernsehen schwer. Von 4 Mio. Zusehern sind sicherlich ein paar hunderttausend dabei, die sich selbst auch als Computer-Spezialist bezeichnen würden. Und sie alle merken, dass der Experte im Fernsehen Unsinn redet, wenn er sagt, dass als Schutz gegen den unbefugten Zugriff auf die eigene Webcam erst einmal Firewall und Virenschutz installiert werden sollten.

Das ist deshalb unsinnig, weil es nicht hundertprozentig schützt, es gibt sicherlich ein gutes Dutzend Angriffsvektoren um fremde Webcams zu steuern – Rootkits zum Beispiel, gegen die hilft kein VirensScanner und keine Firewall.

Der TV-Experte redet also Unsinn. Nur warum? Hat er keine Ahnung? Nein, in Gedanken ist er bei Oma Kasupke. Er hat sich vorher mit der Redaktion abgestimmt, was man dem Großteil der Zuschauer einer Sendung tatsächlich zumuten kann und was für einen Großteil der Zuseher tatsächlich Hilfe bietet.

Nun gibt es neben Oma K. halt noch die anderen, die sich dann in Foren oder Webseiten auslassen und sich fragen, wie es dieser Vollpfosten ins Fernsehen geschafft hat. Schließlich ist das ja kein Experte, sondern nur eine Expertenattrappe.

Wahrscheinlich haben diese Menschen noch nie selbst Fernsehen gemacht. Da sind sie die Laien. Sie vergessen, dass nicht sie alleine die Zielgruppe eines TV-Senders sind. Sie vergessen Oma Kasupke, die vielleicht einen Computerkurs für Senioren bei der Volkshochschule besucht hat und gerade mal weiß, wie man ein Setup-Programm von einer CD startet. Sie macht einen Großteil der Zuseher aus und ist definitiv keine Zuschauerattrappe. Oma Kasupke lebt – millionenfach in diesem Land und unter verschiedenen Namen. Und sie alle haben es verdient, dass einer ihnen in für sie verständlichen Worten erklärt, was Sache ist. Deshalb guckt Oma Kasupke Akte, stern TV oder Planetopia: wegen den Expertenattrappen.

Haben Sie sich eigentlich geärgert, dass der Siedewasser-Reaktor in den Nachrichten gar nicht so funktioniert, wie gezeigt? Ich nicht, denn bei dem Thema Atomkraftwerke bin ich Oma Kasupke und ich danke den Experten, dass sie sich vor Millionen Zuschauern dazu durchringen, ihren wissenschaftlichen Background zu verstecken und mir Informationen auf meinem Niveau servieren.

2

Geldkarten & -automaten

2.1 Epileptische Karten – Warum Geldkarten im Automaten so ruckeln

Auch mehr als ein Jahrzehnt nach Einführung des Euro sind mehr als 100 Mio. D-Mark nicht umgetauscht. Sie gammeln in alten Sparstrümpfen, Kaffeedosen und unter Kopfkissen vor sich hin. Eigentlich verwunderlich, dass einem nicht hier und da noch der ein oder andere DM-Schein untergejubelt wird.

Warum gibt es Bargeld eigentlich überhaupt noch, frage ich mich oft? Mittlerweile können wir ja praktisch überall mit Geldkarte bezahlen. Im Supermarkt, im Taxi, beim Pizzadienst, ja selbst Parkuhren akzeptieren mittlerweile dank der Geldkarten-Funktion lieber Plastik als Münzen und kunstvoll mit spezieller Farbe bedrucktes, noch spezielleres Papier. Das Ende des Bargeldes ist nah, ja sogar die Geldautomaten sind nur noch Auslaufmodelle. Sie veralten und wie bei einem Oldtimer quietscht und knackt es schon an den meisten Automaten.

Bei manchen ist es gar ein Wunder, dass die uns so wichtige Geldkarte in den Automaten gelangt und – oh Wunder – es auch wieder hinaus schafft. Da ruckelt die Karte wie ein angeschosenes Tier hin und her und müht sich im Schneckentempo in den Automaten zu kommen.

Erwarten wir zu viel Service? Schafft es die Bank nicht, uns „König-Kunde“ einen Automaten zu präsentieren, bei dem unser wichtigstes Zahlungsmittel mit Samthandschuhen behandelt und geschmeidig eingezogen wird? Sie könnte. Es ist schlimmer: die Bank macht das mit Absicht nicht!

Wenn dreiste Verbrecher mit kleinen Kameras die PIN abfilmen, müssen sie auch den Inhalt des Magnetstreifens irgendwie zu Gesicht bekommen. Das einfachste ist, diesen zu kopieren – doch dazu muss man die Karte in die kriminellen Finger kriegen. Einfacher ist es, wenn der eigentliche Besitzer die Kopie gleich selbst anfertigt. Die Übeltäter kleben dazu einfach einen zweiten Kartenleser direkt vor den der Bank. Das Geldinstitut bebt vor Wut und lässt den Geldautomaten daher vibrieren.

Zitternde Karteneinzüge an EC-Automaten verhindern nämlich, dass Betrüger durch das Anbringen eines zweiten Kartenlesers vor dem eigentlichen Einzugsschlitz eine Kopie unserer Karte anfertigen.

Die frei erhältlichen und kleinen Aufsätze der Betrüger können die Daten des Magnetstreifens nur dann erfassen, wenn die Karte gleichmäßig durchgezogen wird. Das ewige hin und her erzeugt Datenmüll und die Kopie ist wertlos. Ein epileptischer Anfall unserer Geldkarte sorgt quasi dafür, dass unser Kontostand gesund bleibt.

2.2 Rot – Gelb – Geld – Wieso die PIN nicht auf der Geldkarte gespeichert ist

Ist die Geldkarte endlich im Automaten, kommt das nächste Problem – die PIN. Vierstellig, zufällig von der Bank gewählt¹ und dummerweise niemals das eigene Geburtsdatum. Wer soll sich

¹ Einige Banken erlauben selbst gewählte PIN.

das merken können? Zum Glück kennt sie der Automat auch und gibt uns Bescheid, wenn wir sie nicht mehr wissen. Einmal, zweimal und weg.

Räumen wir erst einmal mit Irrglaube Nr. 1 auf. Die PIN ist **nicht** auf dem Magnetstreifen gespeichert. Wer nur die Karte besitzt kann die PIN nicht auslesen oder errechnen. Das ging mal, aber diese Zeiten sind seit längerem vorbei.

Irrglaube Nr. 2 lautet: Geldautomaten können die PIN nur überprüfen, wenn sie mit unserer Hausbank online verbunden sind. Wären sie das, dann müssten die Banken alle PINs ihrer Kunden zu jedem Wald-und-Wiesen-Automaten im hintersten Ausland übertragen. Das wäre viel zu gefährlich. Wenn es jemandem gelänge, in diesem Netzwerk eine Stunde mitzulesen – nicht auszudenken.

Der Automat weiß, ob die PIN die Richtige ist – obwohl sie nicht auf der Karte steht und auch nicht von der Hausbank überprüft wird. Wie geht das? Es gibt mathematische Einbahnstraßen. Formeln, die – wenn man sie mit zwei Werten füllt – ein Ergebnis liefern. Niemand – und ich meine tatsächlich niemand – kann anhand des Ergebnisses die zwei ursprünglichen Werte herausfinden – obwohl er die Formel und das Ergebnis kennt!

Das Prinzip dieser Formeln entspricht in etwa einer Farben-Misch-Maschine im Baumarkt. Sobald Sie sich ein neues frisches Orange für das Schlafzimmer ausgesucht haben, tippt die freundliche Verkäuferin die Nummer von der Farbtafel in eine Tastatur und Sie erhalten die Wunschfarbe der Dame des Hauses (*oder hat bei Ihnen der Mann schon einmal die Farbe des Schlafzimmers ausgesucht?*)

Der Automat mischt Ihnen aus den Grundfarben Rot und Gelb exakt Ihr gewünschtes Orange zusammen – immer und immer wieder, so viele Eimer Sie wollen. Aber wenn Sie selbst versuchen, aus eben den gleichen Eimern mit Rot und Gelb das Wunsch-Orange *exakt* nachzumischen, werden Sie dies niemals schaffen. Ihr Orange mag dem aus dem Baumarkt ähnlich sehen,