Tobias Schrödel

Ich glaube, es hackt!

Ein Blick auf die irrwitzige Realität der IT-Sicherheit

3. Auflage

SACHBUCH

Springer Spektrum

Ich glaube, es hackt!

Tobias Schrödel

Ich glaube, es hackt!

Ein Blick auf die irrwitzige Realität der IT-Sicherheit

3., aktualisierte und erweiterte Auflage

Springer Spektrum

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 978-3-658-04245-5 ISBN 978-3-658-04246-2 (eBook)
DOI 10.1007/978-3-658-04246-2

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

Springer Spektrum

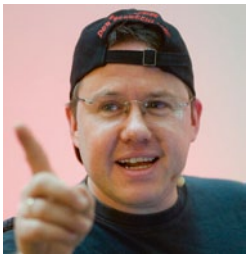
Lektorat: Stefanie Brich, Carolin Wolfram
Cover-Foto: Tobias Schrödel/Peter Gross

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Spektrum ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-spektrum.de

Inhalt

Über den Autor



Tobias Schrödel, Jahrgang 1971, ist „Deutschlands erster Comedyhacker®“. Der Münchner 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 drei Jahren 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 Münchner 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.comedyhacker.de/blog/

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.

T. Schrödel, *Ich glaube, es hackt!,* DOI 10.1007/978-3-658-04246-2_1,

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

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

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.

Diese aktualisierte Auflage mit neuem Titel wurde um 50 Kapitel erweitert und deckt somit viel mehr Themen rund um den privaten Einsatz von Computer und Smartphone ab (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, der 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.

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 vier Millionen 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 Virenscanner 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 verschiedensten 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 angeschossenes Tier hin und her und müht sich im Schneckentempo in den Automaten zu kommen.

T. Schrödel, *Ich glaube, es hackt!,* DOI 10.1007/978-3-658-04246-2_2,

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 gewählt[1] 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,

aber es ist nie exakt gleich. Obwohl sie wissen, *welche* Farben rein müssen, müssten Sie auf den tausendstel Milliliter genau wissen, *wie viel* von jeder Farbe rein muss – von Problemen beim Eingießen solch kleiner Mengen mal abgesehen.

Die Geldautomaten und Ihre Geldkarte vergleichen quasi ebenfalls Farben. Das Orange ist auf dem Magnetstreifen gespeichert. Es wurde vorher von der Bank gemischt und die Menge **einer** der hinzugefügten Grundfarben wurde Ihnen mitgeteilt – in Form einer PIN. Die Menge der anderen Grundfarbe steht zusammen mit dem Ergebnis – dem gemischten Orange – auf dem Magnetstreifen.

Tippen Sie nun die Menge Ihrer Farbe – Verzeihung – Ihre PIN am Automaten ein, dann kann die Bank die auf dem Magnetstreifen gespeicherte Menge der anderen Farbe hinzumischen. Das entstandene Orange wird nun mit der Farbe auf Ihrem Magnetstreifen verglichen. Ist es identisch (und nicht nur ähnlich), dann geht der Automat davon aus, dass Ihre PIN die richtige war und Sie bekommen Ihr Geld. Deshalb ist es auch völlig egal, wenn jemand die Farbe auf Ihrer Geldkarte kennt, weil die exakte Mengenangaben (Ihre PIN) fehlt.

Nun könnten Sie ja auf die Idee kommen, einfach alle möglichen Mengen durchzuprobieren, bis das Orange exakt identisch ist. Leider scheitert das an der immens großen Zahl an Möglichkeiten. Selbst wenn Sie mehrere tausend Versuche pro Stunde haben, würden Sie Jahrtausende benötigen, um die richtige Lösung zu finden.

Vielleicht werfen Sie mir jetzt vor, ich kann nicht rechnen. Die PIN ist vierstellig von 1000 bis 9999. Es gibt also maximal 8 999 Möglichkeiten. Sie haben Recht. Tatsächlich ist das Verfahren etwas komplizierter. Es kommen noch Institutsschlüssel und Poolschlüssel ins Spiel.

Lediglich um es ein wenig einfacher zu machen, hatte ich Ihnen erklärt, die PIN *entspricht* Ihrer Farb-Mengenangabe. Tatsächlich wird mit weiteren Einbahnstraßenformeln gerechnet.

Aber: Sie haben genau drei Versuche am Automaten, bevor die Karte gesperrt wird. Das entspricht einer Chance von weniger als 0,03 % – nicht wirklich so attraktiv wie ein hübsches Orange.

2.3 Demenzkranker Käse – Wie man sich PINs merken und sogar aufschreiben kann

Manchmal ist der Unterschied zwischen einem Luftballon und dem was wir im Kopf haben nur die Gummihaut des Ballons. Wir stehen vor einem Geldautomaten oder möchten das Handy einschalten und uns will und will die PIN einfach nicht mehr einfallen. Dabei haben wir diese bestimmt schon mehrere hundert Male eingetippt.

Das ist der Moment, in dem mir meine grauen Haare wieder einfallen. Die, die sich nächtens heimtückisch, aber konstant und mit rasender Geschwindigkeit vermehren. Und fällt das Aufstehen nicht auch täglich immer schwerer? Ist es so weit? Bekomme ich Löcher im Kopf? Ist das der Beginn von Demenz und Kreutzfeld-Jakob?

Beim berühmten Schweizer Käse ist das marketingtechnisch ganz gut gelöst. Die Löcher entstehen in ihm durch Gasbildung beim Reifeprozess. *Reifeprozess* – klingt doch gleich viel besser als Demenz, oder?

Nun hilft dieses Schönreden nicht gegen den partiellen Gedächtnisverlust. Die PIN muss her, schließlich soll Geld aus dem Automaten kommen oder das wichtige Telefonat muss geführt werden. Was also tun? Aufschreiben darf man die PIN ja nicht, sonst wird uns bei einem Kontomissbrauch gleich grobe Fahrlässigkeit unterstellt.

Oder etwa doch? Gibt es eine Möglichkeit die PIN aufzuschreiben und sogar im Geldbeutel neben der Geldkarte mitzuführen,