Tobias Schrödel

Hacking für Manager

IT-Sicherheit für alle,
die wenig Ahnung
von Computern haben.

2. Auflage

GABLER

Tobias Schrödel

Hacking für Manager

Tobias Schrödel

Hacking für Manager

IT-Sicherheit für alle, die wenig Ahnung von Computern haben.

2., erweiterte Auflage

GABLER

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

Tobias Schrödel ist freiberuflicher Berater für IT Security & Awareness und arbeitet Teilzeit bei T-Systems. „Deutschlands erster Comedy Hacker“ (CHIP 05.2010) erklärt die Systemlücken des Alltags auch immer wieder im Fernsehen für jeden verständlich.

1. Auflage 2011
2., erweiterte Auflage 2012

Lektorat: Peter Pagel

Gabler Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.gabler.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: Stürtz GmbH, Würzburg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8349-3342-3

Inhaltsverzeichnis

1 Vorspiel

1.1 Von Hackern und Datenschnüfflern

Worum es geht und wie die Spielregeln sind

Erinnern Sie sich, wie Sie als Kind den Kaugummiautomaten mit einer spanischen Münze aus dem Urlaub überlistet haben? Zugegeben, seit der Euro-Einführung wurde diese Sicherheitslücke gestopft, aber Sie verstehen was ich meine.

Schon als Kind war es eine spannende Aufgabe, den Automaten zu überlisten. Von schlechtem Gewissen natürlich keine Spur.

Es funktioniert, wie sollte es anders sein, nach dem Prinzip der Belohnung. Löse ein Problem und du bekommst Futter. Das Prinzip klappt nicht nur beim Menschen, auch Ratten, Meerschweinchen und Affen sind darin ziemlich gut.

Der Trick mit der spanischen Münze wurde nur unter der Hand weitergereicht, von Kumpel zu Kumpel. Ich verrate Ihnen hier, wie das mit den Kaugummis in der virtuellen Welt – im so genannten Cyberspace – funktioniert. Es lauern weitaus mehr Möglichkeiten 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. Und keine Sorge, es geht hier nicht nur um den Computer und Bits und Bytes. Sie müssen weder Computerfachmann noch IT Profi sein.

Manche Lücken stecken im Detail, manche 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

T. Schrödel, *Hacking für Manager,* DOI 10.1007/978-3-8349-7128-9_1,

mit der PIN bei der EC-Karte funktioniert oder warum gelöschte Daten gar nicht gelöscht sind? Dieses Buch erklärt Ihnen verständlich, wie all das geht und funktioniert.

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. Manche Geräte sind absichtlich komplizierter als es sein müsste. Aber oft ist die unverständliche Umständlichkeit ganz bewusst implementiert, um die Sicherheit des Systems zu erhöhen.

IT Menschen sind eben nicht in allen Fällen diejenigen, die uns nur deshalb unsinnige Vorgaben machen, weil sie niemals Mitarbeiter des Monats werden möchten. Nein, sie machen durchaus sinnvolle Vorgaben, zum Beispiel im Umgang mit Passwörtern. Leider sind sie nicht in der Lage, die Gründe ihres Tuns verbal zu äußern.

All dies ist nicht viel komplizierter zu verstehen als der Kaugummi-Trick mit der spanischen Münze. Wahrscheinlich sind Sie selbst schon länger tagtäglich Opfer von Hackern und Datenschnüfflern. Sie wissen es nur noch nicht.

Drehen wir den Spieß einfach um. Ich erkläre Ihnen, wie das alles funktioniert und mache Sie selbst zum Hacker. Dadurch sind Sie in der Lage, zu erkennen, wie Sie sich schützen können, welchen Risiken Sie und Ihr Unternehmen ausgesetzt sind.

Außerdem zeige ich, wie Sie den einen oder anderen Trick zu Ihrem persönlichen Vorteil nutzen können. »*Hacking für Manager*« eben, um das erste Klischee gleich mal zu bedienen.

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 richtig ist. 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 Fernseh-Zuschauer. 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 Groß 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 Experten-Attrappe.

Nun ja, 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 Zuschauer-Attrappe. 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, SternTV 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 und -automaten

2.1 Epileptische EC-Karten

Warum EC-Karten im Automaten so ruckeln

Auch mehr als ein Jahrzehnt nach Einführung des EURO sind mehr als 100 Millionen 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 EC-Karte 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 EC-Karte 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.

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 es, diesen zu kopieren – doch dazu muss man die Karte in die kriminellen Finger kriegen. Einfacher ist es, wenn der eigentliche Besitzer die

T. Schrödel, *Hacking für Manager,* DOI 10.1007/978-3-8349-7128-9_2,

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 EC-Karte sorgt quasi dafür, dass unser Kontostand gesund bleibt.