Buchbesprechung

Hier ausnahmsweise einmal eine völlig subjektive!

Risikofaktor Mensch
Kevin Mitnick
mit einem Vorwort von Steve Wozniak

Neu !

2003, Hardcover
400 Seiten, Format 17,0 x 24,0 cm
ISBN 3-8266-0999-9

€ 19,95

Kevin Mitnick, einst der meist gesuchte Verbrecher der USA, saß fünf Jahre lang im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Dabei bediente er sich häufig nicht nur seiner umfassenden technischen Hacker-Kenntnisse, sondern überlistete praktisch jedes Sicherheitssystem, indem er sich Passwörter erschlich, in Mülltonnen nach sicherheitsrelevanten Informationen suchte und falsche Identitäten vorgaukelte. Mitnick führt den Leser in die Denk- und Handlungsweise von Hackern ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die folgenschweren Konsequenzen, die sich aus diesen Einbrüchen ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers wie auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso jeder Angriff so erfolgreich war - und wie man sich effektiv dagegen schützen kann. Kevin D. Mitnick arbeitet nach seiner Freilassung aus dem Gefängnis als IT-Sicherheitsberater. Ein ihm auferlegtes Computernutzungsverbot wurde mittlerweile aufgehoben. Sein Co-Autor William L. Simon ist Bestseller-Autor von mehr als einem Dutzend Büchern und prämierten Film- und Fernsehdrehbüchern.

http://www.mitp.de/vmi/mitp/index.php?pTyp=detail&pWert=0999&PHPSESSID=c41aed778a46e516e1ec2d9c985f6654

Daher der Rat: Nicht kaufen!
Wie das?
Ganz einfach. Möchten Sie sich als Verantwortlicher eines Unternehmens, das Server, PC, Inter- und Intranet nutzt, einen ruhigen Schlaf bewahren, folgen Sie einfach meinem Rat und kaufen dieses Buch nicht. Sie werden es mir danken!
Im Grunde genommen, wissen und kennen Sie schon alles das, was darin geschrieben steht. Warum sich dann nochmals seine Unterlassungen vorhalten lassen?

Social Engeneering ist ein Anglizismus für Uralttechniken zur Überlistung von Personen. Ein bekanntes Beispiel ist die Geschichte des Hauptmanns von Köpenick. Eine weniger bekanntes handelt von einem Trick der Engländer, die verzweifelt die geänderte Anordnung der Verschlüsselungswalzen der deutschen Verschlüsselungsmaschine „Enigma“ zu erlangen suchten.
Sie ließen drei Tage hintereinander an der bretonischen Küste immer zur selben Zeit die selbe Boje von einem Kampfflugzeug bombardieren. Natürlich wurde dies auch immer brav verschlüsselt und an die vorgesetzten Stellen gemeldet.
Drei Tage derselbe Text, lediglich das Datum war jeweils neu. Alles klar?
Warum die Boje bombardiert wurde? Interessierte niemand. Hauptsache: Korrekte Meldung, wehrmachtsgerecht ohne einen einzigen Tippfehler. Und gerade ein oder mehrere Tippfehler hätten den Angreifer völlig durcheinander gebracht. Nur, vertippen war in Wehrmachtskreisen verpönt, auf jeden Fall in Meldungen an die vorgesetzten Stellen. Man kann sich gut vor-

stellen, wieviel Liegestützen der arme „Vertipper“ hätte machen müssen. Das wußten die Briten sehr genau. Social Engeneering der ersten Klasse!

Was aber nicht heißt, dass die Deutschen Stellen nicht auch „Social Engeneering“ betrieben haben. Das Beispiel soll nur zeigen, dass selbst Fachleute ersten Ranges nicht dagegen gefeit sind! Die kampferprobten Trojaner haben sich ja auch über den Tisch ziehen lassen.

Also: Doch kaufen?
Ich sage: Ja!
Haben Sie wenig Zeit zum Lesen? Kein Problem, darunter leiden auch die „Sozial-Ingenieure“. Daher hat Kevin Mitnick das Wichtige in schnell lesbaren „MitnickSpots“ zusammengefaßt.
Das dauert Ihnen immer noch zu lange? Auch gut, dann lesen Sie Kapitel 17 ab Seite 375. Es ist ein echtes 7-seitiges Management-Papier. Nur, danach können Sie nicht mehr sagen, Sie hätten es nicht gewußt! Also: Vorsicht! Vielleicht doch nicht kaufen?

Aber Mitnick kennt als „Sozial-Ingenieur“ auch sehr gut die Tücken des Sicherheitsgeschäftes. Eine davon ist die Bequemlichkeit. Das Kapitel 16 enthält daher ein komplettes 75-Seiten-Programm, mit dem Sie Ihre Mitarbeiter sensibilisieren und schulen können. Also: Doch kaufen, preiswerter erhält man keine Schulungsunterlagen zu diesem Thema.
Machen Sie es ALLEN Ihren Mitarbeitern, vom Portier über den Azubi im ersten Lehrjahr bis hin zum Vizepräsidenten, zum Geschenk –dann können Sie ruhiger schlafen.
Und der Rückfluß der Investitionen? Vielleicht schon nach einem Tag oder nach einem Monat. Wo gibt es das noch?

Kevin Mitnick macht eindeutig klar, das die beste und ausgefeilteste Technik überhaupt nicht hilft wenn der Mensch die schwächste Stelle ist. Und er wird sie immer bleiben, sorry. Es ist an Ihnen, diese Schwachstelle zu minimieren –aber bitte nie vergessen: Eine 100 %-Sicherheit gibt´s nicht! Sicherheit ist kein Status, es ist ein ununterbrochener Prozeß. Ein immerwährendes gegenseitiges Aufschaukeln von Angriff und Abwehr. Von Angreifer und Verteidiger – nur das die Verteidiger meistens nicht die kriminelle Energie der Angreifer besitzen und sich diese oft überhaupt nicht einmal vorstellen können!
Der Kenner der Zen-Philosophie wird hier sagen: Der Weg ist das Ziel.

Als Erfinder und Spezialist für dynamische biometrische Erkennungsverfahren gingen mir die Erläuterungen zu den Paßwörtern und deren operationellen Schwächen natürlich ´runter wie Öl. Obwohl immer wieder abgestritten, werden die PIN und die Paßwörter in Massen an den Bildschirmen geklebt –Post-It´s sei Dank. Oder wie oft werden die armen Unterseiten Tastaturen zum Notieren mißbraucht?

Aber selbst Mitnick vergißt in seiner Aufzählung der Gruppen von Paßwörtern (Familie, Freundin, Sport, Arbeit, KFZ, Haustiere und Ähnliches) sogar eine wichtige Gruppe: die der Fäkalwörter. Da glaubt jedermann, die wären so fies, das versucht keiner –aber Hacker beginnen gerade damit!
Also, man sieht, entweder die Gruppe ist Mitnick auch zu fies oder er hat sie vergessen. Hacker und Social Engineers vergessen so etwas nicht! Denen ist überhaupt nichts zu fies.

Aber Kevin Mitnick kannte auch nicht die Smart Defense-Antwort auf einen Brut Force-Angriff: das eigenhändig geschriebene Passwort. Nur so als Tip für Sie.
Hat nämlich ein bekanntes Unternehmen mit, sagen wir ´mal 10.000 PC-Arbeitsplätzen, nur EIN Passwort für ALLE und für Alles, hat der Hacker es wohl vermeintlich sehr einfach. Das

Passwort ist sogar bekannt. Tja, da liegt er aber nicht so ganz richtig. Er kann, wo auch immer versuchen in einen PC oder Server ein zu dringen, immer erfolgt die Meldung: „Bitte schreiben Sie „Wolfsburg“. Nun muss er die unbekannte und unfälschbare Schreibdynamik so exakt in Schreibdruck, Schreibzeit und Schreibpausen niederschreiben, dass er wiedererkannt wird. Und je sensibler der Bereich, um so strenger wird die Schreibdynamik geprüft! Dann kann es vielleicht sein, dass sogar der Berechtigte drei mal unterschreiben muss!
Ist das Passwort dann noch unbekannt, nun, da hat er doppeltes Pech. Es gibt ja eine unendliche Zahl davon, man beginne nur einmal mit dem Atlas bei „Aalen“ und zähle bis „Zwickau“ durch. Wird das eigenhändig geschriebene Passwort noch mit einer tippdynamische erfaßten PIN (jeder Mensch hat seine individuelle Tippdynamik) kombiniert, gibt’s für den Angreifer wirklich ernsthafte Probleme.
Es ist auch an zu nehmen, dass Kevin Mitnick noch nicht über sichere mobile Signaturkomponenten (Mobiltelefon mit „Analoger Tastatur“ zur Eingabe von Zahlen und Schriftzeichen) informiert wurde.
Aber das war an sich ein unerlaubter Ausflug in die fortschreitende Technik. Wobei ich manchmal glaube, dass derlei sichere Verfahren nicht aller Orten und nicht bei allen Organisationen beliebt sind.

Kevin Mitnick zählt im Index 27 mal den Begriff „Sicherheit“, von Sicherheit bis Sicherheitszertifikat. Danach folgt sofort „Passwort“ mit 18 Erwähnungen. Scheint etwas daran zu sein, an den operationellen Schwächen der Passwörter!
Auf Seite 364 meint Mitnick zur Auswahl der Paßwörter folgendes: Das Passwort muss ...
... für Standard-Nutzerkonten wenigstens acht Zeichen und für privilegierte mindestens zwölf Zeichen lang sein,
... mindestens eine Nummer und ein Symbol und einen Groß- und einen Kleinbuchstaben enthalten,
... es folgen noch weitere Kriterien, die aber alle an sich bekannt sein sollten. Sollten!

Sind sie offensichtlich aber nicht. In der gerade wieder angefachten Diskussion zur flächendeckenden Einführung sogenannter „digitale Signaturen“ (besser: digitale Siegel) wird vorsichtshalber das Problem der Passwörter Aussen vor gelassen. Nach der Verordnung zur „Digitalen Signatur“ sollen diese Paßwörter lediglich sechs Stellen besitzen –von einer Änderung nach vier oder sechs Wochen ist da keine Rede. Wie auch, wenn schon Personen, die beruflich mit Paßwörtern zu tun haben, die operationellen Schwächen nicht beachten, wie dann der unbedarfte digitale „Have-Not“?
Daher: Mitnicks Buch ist die ideale „Bibel“, vulgo „Belehrungsunterlage“, für zukünftige Aspiranten digitaler Siegel oder, das „schönere“ Wort soll auch zur Anwendung kommen, digitale „Signaturen“.

Also, lieber Leser, Sie sehen, Sie stehen nicht alleine da, was ja auch tröstlich sein kann. Aber, ein starker Trost ist das gerade nicht.
Daher: Doch kaufen, einige schlaflose Nächte hinter sich bringen, Mitnicks Ratschläge befolgen, dann klappt´s!
Immerhin ist er Insider und weiß wovon er schreibt! Viele könnten, dürfen aber nicht schreiben.