Buch Hacking für Manager

Was Manager über IT-Sicherheit wissen müssen. Die Tricks der Hacker.

Tobias Schrödel
Gabler, 2011
Listen now

- play
- pause

00:00
00:00

Rezension

Tobias Schrödel ist sozusagen Hacker von Beruf. Sicherheitslücken bei alltäglichen Produkten wie Kreditkarten und Smartphones zu finden, macht dem IT-Berater augenscheinlich Spaß. So berichtet er z. B., wie er das Handy eines Freundes unbemerkt via Bluetooth umprogrammiert hat, um diesen auf seinen laxen Umgang mit persönlichen Daten aufmerksam zu machen. Leser, die den Namen ihres Partners oder Haustiers als Passwort verwenden, dürften sich bei solchen Beispielen durchaus ertappt fühlen. Schrödels besonderes Talent liegt darin, nicht mit erhobenem Zeigefinger zu schreiben, sondern humorvoll und hilfreich Möglichkeiten für einen besseren Datenschutz aufzuzeigen. Diese sind meist nicht mal sonderlich aufwändig, erhöhen die Sicherheit aber deutlich. *BooksInShort* empfiehlt das Buch allen, die mit Computern arbeiten – also so ziemlich jedermann.

Take-aways

- Ein sicheres Passwort besteht aus einer Kombination von mindestens acht Buchstaben, Ziffern und Sonderzeichen.
- Es lässt sich etwa aus den Anfangsbuchstaben der Wörter eines Satzes und der Hinzufügung von Sonderzeichen erstellen.
- Speichern Sie Ihre Passwörter weder im Browser noch in Passwort-Safes.
- Werden Sie skeptisch und geben Sie keine Auskunft, wenn man Sie am Telefon nach Ihrem Benutzernamen und Passwort fragt.
- Das mTAN-Verfahren (Tranksaktionsnummer per SMS) beim privaten Onlinebanking bietet hohe Sicherheit.
- Das derzeit sicherste Verfahren für geschäftliches Onlinebanking ist HBCI, mit einer Karte und einem externen Lesegerät zur Autorisierung.
- Aktivieren Sie Bluetooth nur, wenn Sie tatsächlich Daten übertragen möchten.
- Verschlüsseln Sie Ihr WLAN zumindest mit WEP, am besten mit WPA2.
- Verwenden Sie keinen USB-Stick, den Sie zufällig gefunden haben. Er könnte absichtlich ausgelegt worden sein und ein schädliches Programm enthalten.
- Den Papierkorb zu leeren, nützt nichts: Damit entfernen Sie lediglich Informationen über den Speicherort, aber nicht die Daten selbst.

Zusammenfassung

Gelöscht ist nicht gleich gelöscht

Wer sicher am Computer arbeiten will, muss umdenken. Denn in der digitalen Welt ist vieles ganz anders als im Alltag. Beispiel Datenvernichtung: Wird eine Datei nicht mehr benötigt, landet sie im Papierkorb, der wiederum mehr oder weniger regelmäßig geleert wird. Doch damit sind Ihre Daten nicht von der Festplatte gelöscht, wie man eigentlich denken sollte. Durch das Leeren des Papierkorbs wird lediglich die Information darüber gelöscht, wo die Datei gespeichert war, nicht aber deren Inhalt. Erst wenn der Bedarf an Speicherplatz besteht, überschreibt das System die alte Information mit einer neuen. Spezielle Programme können deshalb Daten, bei denen lediglich die Angabe zum Speicherort fehlt, relativ einfach rekonstruieren. Nur Dateien, die vor dem Löschen möglichst sieben Mal überschrieben wurden, sind unwiderruflich vom Speichermedium entfernt.

Schnell vergessen: Passwörter

Das Dumme an Passwörtern ist, dass man sie sich merken muss. Deshalb neigen Anwender dazu, unsichere Passwörter zu benutzen: 5 % aller Passwörter sind Vornamen, mit Vorliebe der des Partners. Doch Passwörter, die nur aus Buchstaben bestehen, sind binnen weniger Stunden entschlüsselt. Um die Internetkindersicherung zu knacken, probieren schon Sprösslinge einfach ein paar Namen aus dem eigenen Umfeld aus – mit großem Erfolg. Ein strukturiertes Ausprobieren aller möglichen Buchstabenkombinationen heißt Brute-Force-Attacke. Besteht das Passwort nur aus Klein- und Großbuchstaben sowie Ziffern, sind 68 Zeichen zu kombinieren. Werden Sonderzeichen verwendet, müssen schon Kombinationen aus 94 Zeichen ausgetestet werden, was exponentiell länger dauert. Schon wenn Sie in Ihr Passwort ein einziges Sonderzeichen einbauen, steigern Sie die Laufzeit einer Attacke um ein Vielfaches.

> „Wir wissen schon aus dem sonntäglichen Tatort, dass selbst ausradierte Schriften wieder sichtbar gemacht werden können."

Leider stellen verschiedene Anwendungen recht unterschiedliche Anforderungen an die Länge von Passwörtern und die erlaubten Zeichen. Viele Benutzer variieren ihr Standardpasswort durch Hochzählen am Ende (z. B. „schlüssel01", „schlüssel02" usw.). Das trägt kaum zur Sicherheit bei. Dabei ist es gar nicht schwer, ein wirklich sicheres Passwort zu finden und sich dieses zu merken. Der Trick: Wählen Sie einen Satz mit acht Wörtern und verwenden Sie deren Anfangsbuchstaben. So wird aus „Schlaf Kindlein schlaf, deine Mutter ist ein Schaf" das Passwort „SKsdMieS". Nun haben Sie schon Groß- und Kleinbuchstaben kombiniert. Möchten Sie Hacker über Jahre beschäftigen, ergänzen Sie am Ende Ziffern und Sonderzeichen („SKsdMieS7%") oder ersetzen Sie Buchstaben durch ähnliche Ziffern und Sonderzeichen („$KsdMie$"). Achtung: Im Internet gibt es unendlich viele Seiten, die zwar ein Log-in erfordern, aber dem Anwender keinen Nutzen bieten. Hier geht es nur ums Sammeln von Passwörtern in so genannten Honeypots. Verwenden Sie deshalb nicht überall dasselbe Passwort, sondern tauschen Sie je nach Anwendung einfach ein Zeichen, z. B. das letzte.

> „Die Betreiber von Honeypots, also Webseiten, die Menschen anlocken und eine Registrierung erfordern, wissen, dass wir immer wieder dasselbe Passwort verwenden."

Browser bieten die absurde Funktion, Passwörter zu speichern. Ganz praktisch, denken viele Anwender daheim, wer interessiert sich schon für meine privaten Dateien? Doch aufgepasst: Wer so denkt, vergisst, dass sich berufliche und private Passwörter bei vielen Nutzern stark ähneln oder sogar identisch sind – und sei es nur in ihrer Struktur. So ist es für einen Eindringling ein leichtes, die am privaten PC geklauten Passwörter auszutesten und sich Zugang zum beruflich genutzten PC zu schaffen. Auch so genannte Passwort-Safes, die nach Eingabe eines sicheren Passworts Zugang zu allen Passwörtern gewähren, sind nicht unbedingt sicher. Denn woher wissen Sie, ob der Hersteller des Safes ein vertrauenswürdiger Anbieter ist und wie er Ihre Passwörter verschlüsselt? Relativ sicher sind Passwort-Safes, die Hersteller von Antivirenprogrammen oder wissenschaftliche Einrichtungen entwickeln.

Internet: anonym oder personalisiert

Wer im Internet surft, weiß meist nicht, was alles über ihn gespeichert wird. Eine Spur, die man zwingend hinterlässt, ist die eindeutige, öffentliche IP-Adresse des Routers, über den man online geht. Dieser Router vergibt jedem Surfer eine weitere, private IP-Adresse. Doch weil diese nur innerhalb des eigenen Netzwerks einmalig ist, speichert jede Website, die man ansteuert, jeweils nur die öffentliche IP-Adresse. Rechtlich gesehen haftet bei einem Vergehen deshalb nicht unbedingt der eigentliche Täter (z. B. ein Hotelgast), sondern der Inhaber des Anschlusses (hier: das Hotel). Wer völlig anonym im Internet surfen will, muss auf Institutionen ausweichen, die ein ganzes Netzwerk von länderübergreifend verstreuten Routern betreiben, z. B. Universitäten. Mithilfe so genannter Tor-Server verhindern sie das Speichern der IP-Adresse. Der Nachteil ist, dass die Surfgeschwindigkeit markant sinkt.

> „Das Speichern von Passwörtern im Browser ist vergleichbar mit dem Einbau einer Sicherheitstüre, die Sie zwar absperren – aber den Schlüssel stecken lassen."

Die Suchmaschine Google speichert die Daten jeder Suchanfrage. Ziel ist es, Anwenderprofile zu erstellen, um ein möglichst optimales Suchergebnis zu erzielen. Diesen Zweck erkaufen sich die Surfer mit der Preisgabe ihrer privaten Daten. So kennt Google beispielsweise über die IP-Adresse die geografische Lage des Suchers. Die Uhrzeit der Anfrage ist ein weiterer Mosaikstein, der über persönliches Verhalten informiert. Auch Suchmuster und Suchinhalte tragen dazu bei, einen Personenkreis zu bestimmen. Und wenn Sie mal den eigenen Namen googeln, liefern Sie Ihre Identität quasi auf dem goldenen Tablett! Schätzungen zufolge sollen 70 % der regelmäßigen Googler bereits der passenden Person zugeordnet sein.

Onlinebanking, aber sicher!

Wie sicher Sie Überweisungen von zu Hause aus tätigen, hängt von dem gewählten Verfahren ab. Um sich online mit seiner Bank zu verbinden, genügt eine vier- oder fünfstellige PIN (persönliche Identifikationsnummer). Das Schlüsselsymbol im Browser zeigt, dass die Verbindung über HTTPS verschlüsselt wird. Dabei wird aus der PIN ein sicheres, 16-stelliges Passwort, das selbst ein Brute-Force-Angriff nicht sprengt. Relativ machtlos ist die sichere Verbindung jedoch gegen so genannte Man-in-the-Middle-Angriffe, die Schlüssel abfangen und kopieren. Dagegen können Sie sich nur mit einer HBCI-Karte und einem externen Kartenlesegerät schützen. Beides erhalten Sie von Ihrer Bank gegen Vorlage eines amtlichen Ausweises und ca. 100 €. Dieses Verfahren wird in vielen Unternehmen eingesetzt.

„Es gibt wenige Tricks, die derart gut funktionieren wie Fachchinesisch von vertrauenswürdigen Stellen."

Mit der PIN sind Sie nun auf Ihrem Onlinebanking-System angemeldet und können Salden und Umsätze einsehen. Richtig riskant wird es erst, wenn Sie Überweisungen tätigen. Wie verhindert die Bank, dass das Geld auf dem falschen Konto landet? Beim TAN-Verfahren bestätigen Sie jede Überweisung mit einer TAN (Transaktionsnummer). Weil diese jedoch für jede Transaktion gültig ist (und sich leicht ergaunern lässt), wurde die iTAN eingeführt: Hier müssen Sie für eine Transaktion exakt die angeforderte TAN eintippen. Doch auch dieses Verfahren wurde bald geknackt, indem findige Webdesigner ganze Bankportale nachprogrammierten und mit der vom Anwender eingegebenen, passenden TAN Geld auf eigene Konten überwiesen. Eine Weiterentwicklung stellt die mTAN dar, wobei der Anwender die zur Überweisung passende TAN per SMS auf sein Handy erhält. Wie beim HBCI erhöht diese Zwei-Faktor-Authentisierung Ihre Sicherheit deutlich.

WLAN – Wer funkt mir dazwischen?

WLAN sei Dank können wir heute fast überall drahtlos surfen. Doch Verschlüsselung muss sein – oder möchten Sie, dass jemand über Ihren DSL-Anschluss illegale Raubkopien verbreitet? Die zwei wichtigsten Verschlüsselungsmethoden derzeit sind WEP und WPA2. Während erstere sich relativ einfach knacken lässt (jedoch immer noch besser ist als gar keine Verschlüsselung), ist letztere nach heutigem Stand nicht zu entschlüsseln und damit sicher. Tragen Sie den WPA2-Schlüssel unbedingt in Ihren Router und alle damit verbundenen, mobilen Geräte ein.

Bluetooth – ganz schön blauäugig

Adressen und besonders Telefonnummern sind wertvolle, vertrauliche Daten. Weil die Dateneingabe zeitintensiv und mühsam ist, lassen sich digitale Telefonbücher inzwischen komfortabel kopieren. Eine tolle Funktion – mit der Einschränkung, dass sich genauso leicht auch fremde Telefonbücher kopieren lassen. Die Ursache sind lückenhafte Bluetooth-Programmierungen der Hersteller Nokia und Sony Ericsson. Ein Hacker kann angreifbare Handys leicht anhand ihrer Herstellernummer identifizieren. Von der Aktivität des Datendiebs bemerkt der Angegriffene leider gar nichts. So ist es binnen Sekunden möglich, ein ganzes Adressbuch zu kopieren und sogar Mitteilungen von fremden Handys zu schicken – sehr zur Verwunderung des Absenders. Und über eine gehackte Bluetooth-Verbindung vom Handy zum Headset kann jedes Gespräch abgehört werden. Weil Bluetooth bidirektional funktioniert, kann der Hacker theoretisch sogar mitreden! Zwar erfordert der Verbindungsaufbau eine PIN, doch die Standard-PINs sind allseits bekannt und lassen sich nur schwer ändern. Überlegen Sie deshalb genau, ob und wann Sie eine blaue Wanze am Körper tragen möchten!

Der Mensch, ein schwaches Glied in der Sicherheitskette

Oft genug öffnen die Mitarbeiter eines Unternehmens dem Datendieb persönlich die Tür – meist im Glauben, ihm damit einen harmlosen Gefallen zu tun. Manch ein mutiger Unternehmer hat Sicherheitsexperten beauftragt, in seine Firma einzudringen, um bestehende Kontrollen zu testen. Die legalen Einbrecher durften lügen und sich verkleiden, nicht aber erpressen oder entführen. Die Ergebnisse erschrecken, denn meist waren Einstieg und Diebstahl kinderleicht. Als Türöffner genügt ein nachgedruckter Firmenausweis mit dem eigenen Foto. Alternativ findet sich irgendwo eine Raucherecke, wo der Notausgang geöffnet ist. Einmal drinnen im Gebäude, liegen in leicht zugänglichen Räumen höchst vertrauliche Dokumente zur Selbstbedienung bereit (z. B. im Abfalleimer neben dem Kopierer). In leeren Meeting-Räumen können zurückgelassene Informationen einfach vom Flipchart abgenommen oder in aller Ruhe vom Whiteboard kopiert werden. Und nicht zuletzt schließt die hilfsbereite Putzfrau schon mal das Chefbüro auf, wenn der nette Mann im Anzug angeblich seine Unterlagen vergessen hat ...

Achtung, Schauspieler!

Um an Nutzernamen und Passwörter zu kommen, genügt schauspielerisches Talent. Denn nichts beeindruckt unbedarfte Anwender so sehr wie Fachchinesisch aus vertrauter Umgebung! Ein vorgetäuschter Anruf aus der IT-Abteilung kann wahre Wunder wirken, wenn es darum geht, Zugangsdaten auszuschnüffeln. Ein beliebter Trick: Zu Vertrauenszwecken programmiert der Angreifer sein Telefon auf eine interne Nummer um, ruft beim Opfer an und gibt vor, eine dringende Fernwartung auf dessen PC vornehmen zu müssen. Nach einem kurzen Verwirrspiel mit fehlgeschlagenen Log-ins wird der Angerufene genervt aufgeben und sein Passwort preisgeben – schließlich kann er ohne einsatzfähigen PC nicht arbeiten. Kommt Ihnen ein Anruf verdächtig vor, notieren Sie die Nummer und rufen Sie zurück oder lassen Sie sich intern verbinden. So finden Sie heraus, ob der Anrufer tatsächlich ein Kollege oder aber ein Datendieb ist.

Verdächtige Fundstücke

Eine weitere Gefahr besteht in der menschlichen Neugierde. Wer kann schon einem USB-Stick widerstehen, der herrenlos in der Tiefgarage herumliegt? Was für Bilder, Briefe oder Bekenntnisse mögen darauf gespeichert sein? Schwupps, eingesteckt und gleich am Computer angeschaut. Microsoft hat zwar die Autostart-Funktion für externe Laufwerke abgeschaltet, das ist aber leider noch nicht an jedem PC angekommen. Noch dümmer, wenn jemand den USB-Stick nicht verloren, sondern aktiv gestreut hat, um Trojaner in Firmennetze einzuschleusen. Dass Viren ausführbare „*.exe"-Dateien sind, ist für den Eindringling nur scheinbar ein Problem. Denn wer mag nicht die animierten Spielchen und Powerpoints, die z. B. zur Weihnachtszeit herumkreisen? Sie sind ideal, um im Hintergrund ein feindliches Programm zu starten, mit dem sich Daten ausspionieren lassen. Deshalb: Bringen Sie verdächtige Fundstücke besser zu Ihrer IT-Abteilung.

Über den Autor

Tobias Schrödel ist selbstständiger Berater in Sachen IT-Sicherheit, sein Steckenpferd ist die Kryptografie. Als Autor, Redner und Komiker teilt Schrödel sein Wissen über Datensicherheit in Publikationen, TV-Shows und Vorträgen.