In diesem Kapitel:

- Verschlüsselte Übertragung mit HTTPS
- E-Commerce
- Online-Banking
- Verschlüsselungsverfahren
- Virtuelle Bankräuber

KAPITEL 7

E-Commerce und Online-Banking

E-Commerce und Online-Banking haben sich erst innerhalb der letzten fünf Jahre durch den Ausbau der Infrastruktur, die zunehmende gesellschaftliche Akzeptanz und die Weiterentwicklung von Skript- und Programmiersprachen zu einem ernst zu nehmenden Angebot im Internet entwickeln können. Steht beim gewöhnlichen Surfen oder bei E-Mail der Schutz der Privatsphäre im Vordergrund, kommt beim Einkauf im Internet und der Abwicklung von Online-Banking-Geschäften ein weiterer Faktor hinzu: Es geht schlicht um Geld, und das Mitlesen von Daten wie Kreditkarteninformationen ist nicht nur aus Sicht des Datenschutzes ärgerlich, sondern kann für den Nutzer sehr teuer werden. Identitätsdiebstahl ist kein Schreckgespenst aus dem Nachmittagsprogramm im Fernsehen, sondern zunehmend ein ernstes Problem, das derzeit aus den USA nach Europa schwappt. Verbindungen, über die sensible Informationen übertragen werden, sollten also nicht auf HTTP und der damit verbundenen Übertragung in Klartext basieren, sondern erfordern ein erhöhtes Maß an Sicherheit.

In diesem Zusammenhang sind die bereits erwähnten Ideale der *Authentizität* und *Vertraulichkeit* von Kommunikation im Internet zentral. Um eine sichere Verbindung zu gewährleisten, müssen sich erstens erstens die beiden Kommunikationspartner gegenseitig kennen und ausweisen (Authentizität) und dass zweitens muss der Weg zwischen ihnen als vertrauenswürdig gelten (Vertraulichkeit). Letzteres ist aber im Internet nicht möglich, und genau an dieser Stelle setzt das Konzept der Verschlüsselung an. Selbst wenn eine der Zwischenstationen den Datenverkehr belauscht, kann sie wenigstens den Sinn der Nachricht nicht erkennen.

Verschlüsselte Übertragung mit HTTPS

Für eine Verschlüsselung kommen grundsätzlich drei Verfahren in Frage: eine feste Kodiervorschrift, ein symmetrisches oder ein asymmetrisches Verschlüsselungsverfahren. Bei Ersterem handelt es sich um die einfachste Form der Kryptographie, bei

der die Daten nach einem festen Muster chiffriert werden. Ein typisches Beispiel hierfür ist *ROT13*, das gelegentlich immer noch im Usenet benutzt wird, um Nachrichten zu kodieren. Dabei wird jeder Buchstabe einfach um 13 Stellen im Alphabet verschoben, so dass beispielsweise aus einem A ein N wird usw. Natürlich sind solche Verfahren blitzschnell entschlüsselt und eignen sich daher lediglich dafür, um Informationen nicht direkt im Klartext zu präsentieren. Nützlich ist das vor allem bei so genannten *Spoilern*, also Mails oder Postings (z.B. in Foren) in denen z.B. das Ende eines Films verraten wird oder Tipps zu Spielen stehen. Der Nutzer kann also die Filmkritik in Ruhe lesen und an den entsprechenden und chiffrierten Stellen selbst entscheiden, ob er diese lesen möchte.Wenn Sie mögen, können Sie sich an folgender Zeile aus der Hackerszene versuchen:[1]

```
Bayl gur cnenabvq jvyy fheivir!
```

Beim symmetrischen und asymmetrischen Verschlüsselungsverfahren hingegen bedient man sich nicht mehr nur einer festen Kodierungsvorschrift, sondern chiffriert die Daten abhängig von einem so genannten *Schlüssel*. Dieser Schlüssel bestimmt, wie die Nachricht kodiert wird. Beim symmetrischen Verfahren wird derselbe Schlüssel zum Lesen und zum Schreiben benutzt, beim asymmetrischen hingegen gibt es immer ein Schlüsselpaar: einen öffentlichen, mit dem *ver*schlüsselt, und einen privaten, mit dem *ent*schlüsselt wird.

Das Problem der symmetrischen Verschlüsselung liegt vor allem darin, dass ein und derselbe Schlüssel für das Chiffrieren und Dechiffrieren benutzt wird und dieser daher beiden Partnern bekannt sein muss. Gelingt es einem Angreifer, in den Besitz des Schlüssels zu kommen, kann er die gesamte Kommunikation mitlesen. Da sich die beiden Partner aber zunächst auf einen gemeinsamen Schlüssel einigen müssen, wird dieser trotz der Sicherheitsbedenken meist über das Internet übertragen und ist daher für Abhörmaßnahmen anfällig. Zwar ist dieses Verschlüsselungsverfahren um den Faktor 100 bis 1000 schneller als das asymmetrische Pendant, wir können aber nicht mehr von einer sicheren Verbindung sprechen, da nicht auszuschließen ist, dass der Schlüssel abgehört wurde. Aus diesem Grund bedient man sich in der Praxis einer Kombination aus beiden Verfahren.

Der Standard für eine sichere Kommunikation ist derzeit HTTPS. Diese Abkürzung steht für *Hypertext Transfer Protocol SSL* (*Secure Sockets Layer*). Wenn eine sichere Verbindung mittels HTTPS zwischen Client und Server aufgebaut werden soll, überträgt der Server seinen öffentlichen Schlüssel an den Partner (asymmetrischer Teil des Verfahrens). Dank dieser Information kann der Client nun eine Nachricht verschlüsseln, die nur vom Server gelesen werden kann und in der der symmetrische Schlüssel mitgeteilt wird. Dieser Schlüssel wird von den Partnern fortan für die wesentlich schnellere symmetrische Verbindung benutzt.

1 Oder Sie geben die Zeichenkette einfach hier ein: *http://www.rot13.de/*.

Nachdem wir nun davon ausgehen können, dass die Verbindung abhörsicher und somit vertrauenswürdig ist, bleibt noch zu klären, wie es um die gegenseitige Authentifizierung der Kommunikationspartner bestellt ist. Dieser Punkt ist deshalb so zentral, weil auch die beste Verschlüsselung kein Garant dafür ist, dass die Daten überhaupt an ihrem Ziel ankommen. Schließlich könnte sich jedermann als der von uns gesuchte Server ausgeben und wir würden fleißig alle sensiblen Daten zu ihm schicken. Dies ist im Übrigen keineswegs nur eine theoretische Gefahr, sondern wurde bereits bei zahlreichen Angriffen beobachtet. Dabei überflutet der Angreifer entweder den Originalserver so stark mit Daten, dass dieser den Dienst einstellt (*Denial-of-Service-Attacke*), oder er verändert die Route zum Server hin. In beiden Fällen ist der Zielcomputer dann nicht mehr erreichbar, und der Angreifer gibt seinen PC als den eigentlichen Server aus. Ein ahnungsloser Benutzer wird nicht bemerken, dass er nicht wirklich auf dem Originalserver, sondern auf einer Kopie arbeitet, und ohne Bedenken seine Zugangsdaten eingeben. Hat der Angreifer nur die Route geändert, kann er die Daten an den wirklichen Server weiterschicken und somit unbemerkt als Relaisstation dienen. Zu einer ähnlichen Situation kann es unter Umständen auch in Firmennetzen kommen, wenn die Kommunikation über einen HTTPS-Proxy läuft. Da der Proxy als Stellvertreter agiert, kann er die Pakete ebenfalls mitlesen. Solche Proxies sind gelegentlich Teil der firmeninternen IT-Sicherheitsstrategie und dienen folglich dem Schutz des Netzwerks. Dennoch kann dies zu Missbrauch führen. Generell sollten Sie deshalb Online-Banking nicht aus dem Firmennetz heraus betreiben.[2]

Um Angriffe mittels einer gefälschten Identität zu vermeiden, hat man sich auf so genannte *Zertifikate* geeinigt. Diese werden von einer als seriös geltenden Zertifizierungsstelle (*Certificate Authority* – CA) ausgestellt und bescheinigen dem jeweiligen Computer, dass er tatsächlich der ist, der er vorgibt zu sein. Bevor nun also die verschlüsselte Kommunikation beginnt, schickt der Server dem Client sein Zertifikat zu, so dass der Benutzer die Echtheit überprüfen kann. Wenn Sie das erste Mal eine Website mittels HTTPS besuchen, kennt Ihr Browser das Zertifikat des entsprechenden Servers noch nicht und fragt daher nach, ob Sie diesem Zertifikat und somit auch der CA, die es ausgestellt hat, vertrauen wollen (siehe Abbildung 7-1). Wenn Sie der CA und dem Zertifikat trauen und es annehmen, gilt die Identität des Servers als bewiesen. Da der Browser das Zertifikat herunterlädt und speichert, fragt er in Zukunft nicht mehr bei Ihnen nach, sondern gleicht das Zertifikat in der jeweiligen Sitzung mit dem von ihm gespeicherten ab. Alternativ können Sie sich auch entscheiden, dem Zertifikat nur dieses eine Mal zu trauen. In diesem Fall fragt der Browser bei jedem anschließenden Besuch wieder nach.

Da die Kriterien der Authentizität und Vertraulichkeit nun erfüllt sind, können wir davon ausgehen, dass die Kommunikation erstens sicher ist und dass zweitens auch

2 Wir werden uns im Kapitel 9, *Anonymität*, ausführlicher mit Proxies beschäftigen.

Abbildung 7-1: Opera fragt beim Zertifikat des ccc nach: vertrauenswürdig oder nicht?

nur mit dem gewünschten System kommuniziert wird. Ob eine solche sichere Verbindung besteht, erkennen Sie an dem geschlossenen Vorhängeschloss bzw. Schlüsselsymbol in der Statuszeile Ihres Browsers. Darüber hinaus erscheint anstelle von *http://...* nun *https://...* in der Browser-Adressleiste. HTTPS gilt als sehr sicher und wird vor allem beim E-Commerce und Online-Banking eingesetzt. Theoretisch spricht jedoch nichts dagegen, auch alle anderen, weniger sensiblen Daten mittels HTTPS zu übertragen. Ob ein Server eine verschlüsselte Übertragung über HTTPS anbietet, können Sie herausfinden, indem Sie in der entsprechenden Adresse einfach *http://...* durch *https://...* ersetzen. Wenn der Server HTTPS nicht unterstützt, erhalten Sie eine Fehlermeldung.

Warum es sinnvoll ist, möglichst viel Kommunikation zu verschlüsseln, erläutert der Chaos Computer Club e.V. wie folgt:

> »Unser WWW-Programm ist öffentlich – wir haben hier nichts zu verbergen. Aber genau deswegen möchten wir durch die vollständige Verschlüsselung der Daten von und zu unserem Webserver Einblicke in die Kommunikation erschweren. Wenn möglichst viele Internetnutzer möglichst viel Kommunikation verschlüsseln – egal ob es öffentliche oder private ist –, wird es für die Bedarfsträger und Schlapphüte ganz schön schwierig, private Daten von öffentlichen zu unterscheiden. Also, geben wir ihnen mal ordentlich zu tun.«[3]

Die Datenverschlüsselung ist insbesondere in Zusammenhang mit dem Schutz der Privatsphäre wichtig, denn nur wenn Kommunikation in großem Stil verschlüsselt wird, erweckt die einzelne Verschlüsselung keine Aufmerksamkeit mehr. Wenn hingegen nur von wenigen und nur zu besonderen Ereignissen (z.B. Online-Banking)

3 Siehe *http://www.ccc.de/https/alt*.

verschlüsselt wird, lassen sich daraus bereits umfangreiche Profile ableiten, da die Kommunikationspartner trotz Chiffrierung bekannt bleiben. Verschlüsselt werden nur die Inhalte der Übertragung, nicht jedoch die Informationen über Ausgangs- und Zielpunkt.

Zuletzt müssen wir noch auf einige Besonderheiten beim Einsatz von HTTPS zu sprechen kommen. Die Sicherheit der Daten wird durch die Länge des Schlüssels bestimmt. Dieser sollte bei asymmetrischer Verschlüsselung 1.024 Bit, bei symmetrischer Verschlüsselung unbedingt 128 Bit lang sein. Kürzere Schlüssel können heute nicht mehr als sicher gelten. Zwar wird manchmal die Länge mit 128 Bit angegeben, tatsächlich verschlüsselt wird aber lediglich mit 40 Bit. Dies gilt vor allem für amerikanische Verschlüsselungssoftware, da dort die Gesetzeslage den Export von sicheren Schlüsseln verbietet. Achten Sie also darauf, europäische Varianten der Software zu benutzen oder ein erweiterndes Patch (z.B. für den Internet Explorer) zu installieren.

Ein weiteres Problem liegt in den CAs begründet. Theoretisch kann jede Person oder jede Firma Zertifikate verteilen. Wer seriös ist, bleibt Ermessenssache des Benutzers, der sich auf den Webseiten der jeweiligen CAs über deren Lizenzbedingungen informieren muss. Der Sinn dieses Zertifizierungsverfahrens ist allerdings insofern fragwürdig, als es vom Benutzer verlangt, sich das Zertifikat selbstständig anzuschauen, die Zertifizierungsstelle auf Seriösität zu überprüfen und dann zu entscheiden, ob er der Sache trauen will oder nicht. Den meisten Internetnutzern fehlt hierzu vermutlich das Know-how, so dass die Zertifizierungsmethode letztlich doch wieder reine Vertrauenssache ist. Zudem haben Online-Shops die Möglichkeit, (fragwürdige) Zertifikate für teures Geld zu erwerben, die zum Beispiel vom Internet Explorer per Default akzeptiert werden, ohne dass der Surfer etwas davon mitbekommt. Dies soll angeblich den Benutzerkomfort verbessern, hebelt aber das ganze SSL-Gerüst wieder aus.

E-Commerce

Während sich das Einkaufen im Internet früher nur auf Technologieprodukte wie Software oder eventuell Hardware beschränkte, kann man heutzutage nahezu alle Produkte – vom Haus über Autos bis hin zur Versicherung – online kaufen. Zwar zählen derzeit Bücher, CDs und Software nach wie vor zu den umsatzträchtigsten Artikeln im Internet, doch wird sich dieses Verhältnis zugunsten einer weiter gefassten Produktpalette zunehmend ändern.[4] Zudem werden technisches Know-how und Informationen immer mehr zu einer wichtigen Ware in unserer Gesellschaft und damit auch im WWW. So kann man im Internet beispielsweise digitales Kar-

4 Ein gutes Beispiel dafür ist sicherlich eBay. Dort gab es sogar einen Golf zu ersteigern, mit dem Benedikt XVI. vor seiner Ernennung zum Papst gefahren ist. Ein anderes Beispiel wären die zahlreichen Reiseanbieter im Internet oder Fluggesellschaften, die immer mehr Umsatz über Online-Buchungen erzielen.

tenmaterial oder den Zugang zu wichtigen Nachrichtenstellen und Online-Recherchen kaufen.

Unabhängig vom Produkt steht dabei die Frage nach der Seriosität des Anbieters im Vordergrund. In Kapitel 3, *Sicherheitsbewusstsein*, haben wir bereits die nötigen Schritte kennen gelernt, um mehr über einen Shop-Betreiber in Erfahrung zu bringen. In diesem Abschnitt wollen wir uns eher mit den grundsätzlichen Gefahren beim Online-Shopping vertraut machen.

Inzwischen gibt es mehr als ein Dutzend verschiedener Protokolle, Empfehlungen oder Standards, die für mehr Sicherheit im E-Commerce sorgen sollen. Ihnen allen ist aber gemeinsam, dass sie das Problem aus der Sicht des Betreibers und nicht aus der des Besuchers angehen, d.h., der Weg zwischen dem Shop und dem PC des Users bleibt eine Schwachstelle. Für den Surfer ist es darüber hinaus nicht ohne weiteres möglich, einzusehen, welchen Sicherheitsempfehlungen ein Online-Shop folgt. Zudem sieht es in der Praxis natürlich ganz anders aus als in der Theorie, und so werden Sie vor allem bei kleineren oder mittelgroßen Anbietern häufig ältere und damit anfällige Standards vorfinden. Um den Rahmen nicht zu sprengen, wollen wir uns auf vier Aspekte beschränken: Kundendaten und Identitätsdiebstahl, Accounts, Produktdaten und Shopzertifizierung.

Kundendaten

Die Frage nach dem Umgang mit Ihren persönlichen Daten steht für Sie als Kunde an erster Stelle. Dabei muss man zunächst die Übermittlung der Daten und dann deren Archivierung betrachten. In der Praxis kommen bei der Übermittlung mehrere Varianten zum Einsatz.

Die einfachste Lösung ist das Abschicken der Bestellung per E-Mail. Wegen des fehlenden Bedienungskomforts ist diese Lösung aber mittlerweile praktisch ausgestorben und wird nur noch von sehr kleinen Anbietern benutzt. Dass hierbei von Sicherheit keine Rede sein kann, erschließt sich in Kapitel 6, *E-Mail – wer liest mit?*, sowie dem Wissen über das Routing im Internet. Es würde beispielsweise schon ausreichen, wenn ein auf den Shop aufmerksam gewordener Cracker einen Host, über den die Route zwischen Mail-Server und Betreiber läuft, kompromittiert und sämtliche darauf gespeicherten Nachrichten ungestört mitliest. Prinzipiell sollten Sie nie Passwörter, Kreditkartendaten oder sonstige sensible Informationen per E-Mail verschicken! Die Tatsache, dass zahlreiche Online-Shops dem Kunden nach der Bestellung eine Bestätigungsmail samt persönlicher Angaben und der verwendeten Kreditkartendaten zukommen lassen, lässt jedem Sicherheitsexperten die Haare zu Berge stehen. Unabhängig davon, welche Sicherheitsmaßnamen (z.B. HTTPS) zuvor beim Einkaufen für vermeintliche Sicherheit sorgten, diese eine E-Mail macht sie alle zunichte.

Die zweite Möglichkeit der Übermittlung von Daten besteht darin, dass Sie sowohl Ihren Produktwunsch als auch Ihre Kundendaten in ein Formular eingeben und diese Daten dann per HTTP an den Anbieter übertragen werden. Auch hier stellt sich wieder die Frage nach den Gefahren des Übertragungswegs. Da bei HTTP die Kommunikationsinhalte nicht verschlüsselt werden, eignet sich diese Methode auch nicht für eine wirklich sichere Verbindung. Zwar spricht nichts dagegen, die reinen Artikeldaten des Warenkorbs unverschlüsselt zu übertragen, die Kunden- und insbesondere die Zahlungsdaten sollten aber auf keinen Fall mit HTTP übertragen werden.

Die dritte und bislang beste Lösung ist eine komplett in HTTPS abgewickelte Kommunikation. Für einen Außenstehenden werden so weder die bestellten Artikel noch die Kundendaten sichtbar. Hierbei müssen Sie darauf achten, dass der Online-Shop auf jeden Fall eine volle 128-Bit-Verschlüsselung benutzt.

Ihre Aufgabe als Kunde besteht also im Wesentlichen darin, abschätzen zu können, wie sorgsam der Anbieter mit Ihren Daten umgeht. Dabei spielt die Verschlüsselung samt Bewertung des Zertifikats eine ebenso große Rolle wie die Frage nach den persönlichen Ansprechpartnern des Shops. Eine seriöse Seite kann man in vielen Fällen bereits am äußeren Erscheinungsbild erkennen. Die meisten seriösen Betreiber werden selbst ein Interesse daran haben, ihre Kunden auf Sicherheitsrisiken aufmerksam zu machen. Wenn aus dem Angebot deutlich ersichtlich wird, welche Firma sich hinter dem Shop verbirgt und wie es um die Zahlungsmodi und die Sicherheitsrisiken steht, kann man zumindest annehmen, dass das Angebot seriös ist. Dies ist zwar noch keine Garantie für sicheres Einkaufen, aber ein erster Hinweis, wie ernst der Anbieter es mit der Sicherheit meint.[5] Kritischer ist da schon die Frage, wie sicher die Daten beim Shop-Betreiber gelagert werden. Da sich die Archivierungsproblematik dem Einfluss des Kunden entzieht und dieser somit keine Druckmittel in der Hand hat, liegen besonders viele ernsthafte Sicherheitslücken in diesem Bereich. Wir wollen uns diese Problematik anhand eines Beispiels anschauen.

Angenommen, der Shop-Betreiber bietet dem Kunden eine vermeintlich sichere HTTPS-Übertragung an, mittels derer die Zahlungsdaten auf dem Server landen. Nun müssen diese Daten ja auch irgendwie einen Mitarbeiter des Online-Shops erreichen. In den meisten kleineren und mittelgroßen Shops steht der Webserver aber nicht in der Firma selbst, sondern bei einem Webhoster. Um die Bestellung zu erhalten, schicken daher zahlreiche Shops die Kundendaten per E-Mail an ihre Mitarbeiter, die diese dann auswerten und die Auslieferung der Ware in die Wege leiten. Unter Sicherheitsaspekten ist ein solches Vorgehen völlig indiskutabel, da die bei der Eingabe verschlüsselten Daten im Nachhinein doch im Klartext per E-Mail

5 Inzwischen ist jeder deutsche Anbieter verpflichtet, ein Impressum auf seiner Webseite zu veröffentlichen. Machen Sie davon Gebauch und informieren sie sich so unbedingt vor dem Einkauf! Bei einem vermeintlichen Einzelunternehmen mit Postfach und ohne weitere Kontaktdaten sollte man, wenn man sich überhaupt für einen Kauf entscheidet, zumindest von einer Zahlung per Vorkasse absehen.

übertragen werden. Für einen Cracker ist es dann meistens ein Leichtes, an sämtliche Kunden- und vor allem Zahlungsdaten zu gelangen, und einem Missbrauch steht nichts mehr im Weg. Der einzige Vorteil dieser Lösung ist wohl darin zu sehen, dass die Daten anschließend nicht mehr auf dem Server liegen, sondern sich im (hoffentlich) sicheren Netz des Anbieters befinden. Erstaunlicherweise sind sich die Anbieter solcher Lösungen anscheinend nicht bewusst, dass sie erstens ihre eigene, teuer erstandene HTTPS-Lösung aushebeln und zweitens ihre sicherheitsbewussten Kunden hinters Licht führen.

Noch kritischer wird es hingegen, wenn der Betreiber die Daten im Klartext in einer Textdatei auf dem Server lagert. Dies mag zwar für Kundendaten noch in Ordnung sein, Kreditkarteninformationen und Ähnliches sind so aber sicherlich falsch aufgehoben. Kaum zu glauben ist vor allem, dass es tatsächlich immer wieder vorkommt, dass sich solche Dateien unterhalb des Webserver-Rootverzeichnisses befinden und somit für jeden einsehbar sind. Aber auch das Auslesen der Benutzerdaten aus einer Datenbank oder per FTP ist nicht wirklich sicher, solange diese Übertragung nicht verschlüsselt abläuft. Selbst wenn die Daten nun sicher vom Käufer zum Server gelangen, dort sicher in einer Datenbank gelagert werden und die Mitarbeiter des Shoppingsystems nur per verschlüsselten Verbindungen auf den Server zugreifen, besteht die Möglichkeit, dass einer der vielen Dienste auf dem Server eine Sicherheitslücke aufweist und diese vom Administrator nicht rechtzeitig geschlossen wird. Virtuellen Einbrechern reicht meist schon ein kleiner Fehler in einer scheinbar zweitrangigen Komponente, um den gesamten Server zu kompromittieren und an die Datenbankinhalte zu gelangen. Die Seriosität des Anbieters und Ihr persönliches Vertrauen zu diesem sind daher die zentralen Sicherheitsaspekte beim elektronischen Einkaufen. Im Nachhinein haben Sie keine Chance, auf Sicherheitslücken beim Betreiber Einfluss zu nehmen, geschweige denn, dass Sie jemals davon erfahren. Unter *http://www.datenschutz.de* finden Sie viele Hinweise und Informationen, welche personenbezogenen Daten gelagert werden dürfen und wie Sie gegebenenfalls gegen unseriöse Praktiken vorgehen können.

Identitätsdiebstahl

Kommen wir nun auf die wirklich kritischen Punkte zu sprechen. Ein Servereinbruch an sich braucht Ihnen keine Kopfschmerzen zu bereiten, interessant wird das Ganze erst, wenn man sich fragt, was denn mit den erbeuteten Kundendaten passiert.

Eine Möglichkeit wäre es natürlich, die erbeuteten Daten beispielsweise an Spammer zu verkaufen. In der Praxis passiert dies sicherlich, ist aber eher ein Nebenschauplatz. Spammer sind eigentlich nur an zwei Arten von Ware interessiert: Listen über aktive E-Mail-Accounts sowie geknackte Rechner, über die man in kurzer Zeit und anonym möglichst große Mengen an E-Mails verschicken kann. Beides ist zurzeit im Überfluss vorhanden, und der rege Markt, der damit betrieben wird,

ist zwar illegal, birgt aber längst nicht die Gefahren eines Einbruchs in ein großes Shopsystem oder gar das Online-Portal einer Bank. Das Gleiche gilt für die Rückführung solcher personenbezogenen Daten in den mehr oder weniger legalen Bereich des Handels mit Kundenprofilen. Sicherlich mag es einige dubiose Firmen geben, die solche Daten kaufen und anschließend selber benutzen oder weiterverkaufen, denn Kundenprofile sind schließlich eine sehr begehrte Ware. Ergaunerte Sozialversicherungsnummern und Kreditkartendaten sind dagegen ein wirklich heißes Eisen. Was passiert also mit den gestohlenen Daten?

Allem Anschein nach hat sich rund um die einst verspielte Crackergemeinschaft eine wahre Internetmafia entwickelt. Identitätsdiebstahl scheint dort derzeit besonders hoch im Kurs zu stehen, und die Welle, die in den USA begann, scheint auch nach Europa herüberzuschwappen. Beim Identitätsdiebstahl werden die erbeuteten Angaben dazu benutzt, unter falschem Namen Geschäfte zu tätigen. Im harmlosesten Fall nimmt ein Angreifer die Identität eines Opfers an, um so an weitere Informationen zu gelangen oder sich bei Online-Angeboten zu registrieren, ohne seine eigentliche Identität preiszugeben. Oft genug geben sich Angreifer damit zufrieden, sich auf Kosten anderer bei Pornoseiten oder anderen dubiosen Angeboten anzumelden. Der Geschädigte bemerkt so etwas meist nach der ersten Kreditkartenabrechnung, was sehr ärgerlich, jedoch finanziell zu verschmerzen ist. Ganz anders sieht es hingegen aus, wenn der Angreifer die Daten benutzt, um auf illegale Angebote zuzugreifen oder in großem Stil auf Kosten des Opfers einzukaufen. Als Geschädigter stehen Sie in der Pflicht nachzuweisen, dass Ihr Account ohne eigenes Verschulden gecrackt wurde, ansonsten sehen Sie Ihr Geld nie wieder. Abgesehen vom finanziellen Verlust kann es Sie zudem in massive Schwierigkeiten bringen zu erklären, warum Sie beispielsweise in Deutschland nicht zugelassene Medikamente oder Bücher in großen Mengen bestellt[6] oder eine ganze Reihe von Konten mit dubiosen Geldeingängen eröffnet haben.

Um die Dimension dieses Problems zu verdeutlichen, schauen wir uns zwei spektakuläre Fälle aus dem Jahr 2005 an. Um es gleich vorweg zu nehmen, die folgenden Zahlen sind leider keine Tippfehler.

Die Firma CardSystems Solutions wickelt die Transaktionen zahlreicher Kreditkartenanbieter, darunter auch MasterCard und Visa, ab. Anscheinend ist es Angreifern bereits im Mai 2005 gelungen in das Computersystem einzubrechen und Zugriff auf 40 Millionen Kreditkarten- und Kundendaten zu erhalten. Es ist sehr wahrscheinlich, dass die Einbrecher dabei nicht in den Besitz aller Datensätze gelangt sind, sondern nur bestimmte Daten heruntergeladen haben. Die unglaubliche Zahl von 40 Millionen vollständigen Datensätzen wäre sonst wohl kaum zu bewältigen gewesen

6 Oftmals lassen sich die Täter die Ware an eine leerstehende Wohnung liefern und fangen den Postboten »zufällig« an der Tür ab. Dies geht weit über die Sicherheitsprobleme des Internets hinaus und soll daher an dieser Stelle nicht vertieft werden.

und hätte einen massiven und auffälligen Datenverkehr verursacht. Letztlich ist wohl eher davon auszugehen, dass einige zehntausend oder hunderttausend Datensätze gestohlen wurden. Offensichtlich (Genauere Angaben zu machen wäre pure Spekulation) hatte CardSystems Solutions den Vorfall dem FBI gemeldet und man hatte sich gemeinsam geeinigt, die ganze Angelegenheit unter Verschluss zu halten. Zwar wurden die betroffenen Kredikarteninstitute und eventuell einige Großhändler informiert, die Presse erfuhr jedoch nichts von dem Angriff. Mitte Juni, also etwa einen Monat später, trat dann jedoch MasterCard an die Presse heran und machte den Einbruch öffentlich. Alleine bei MasterCard waren schätzungsweise 14 Millionen Kreditkarten betroffen, und es hatte erste Fälle von Unterschlagung gegeben. Daher war es wohl ratsamer, sich der Problematik zu stellen, anstatt darauf zu warten, dass ein findiger Journalist die ganze Angelegenheit publik machen würde und das Vertrauen in die Anbieter noch stärker geschädigt worden wäre. Offiziell heißt es, die Anzahl der Fälle, in denen es zu Missbrauch gekommen sei, sei »verhältnismäßig gering«. Was dies jedoch im Bezug auf zigtausend Datensätze heißen mag, bleibt unklar, lässt aber Böses erahnen. Für die betroffenen Kunden hat dieses Publikwerden einen entscheidenden Vorteil: Sollte das eigene Konto betroffen sein, wird der Anbieter sehr großzügig und ohne Komplikationen zurückerstatten.

Der zweite Vorfall fand ebenfalls im Mai 2005 statt. Hier war es Angreifern gelungen, knapp vier Millionen Kundendatensätze der Citigroup zu entwenden. Die Daten sollten eigentlich per UPS verschickt werden, erreichten jedoch nie den Bestimmungsort. Dieser Datenverlust war besonders heikel, da bereits in den Wochen zuvor immer wieder Sicherungsbänder großer Unternehmen verschwunden waren, so dass eine solide Vorbereitung auf solch einen Vorfall zu erwarten gewesen wäre. Die Daten wurden in diesem Fall also nicht im Internet, sondern auf physischem Wege gestohlen. Interessant ist dies jedoch, weil die Daten offensichtlich unverschlüsselt auf den Sicherungsbändern lagen und somit für Cracker leichte Beute sind.

Sie brauchen trotz dieser beunruhigenden Meldungen nicht den Kopf zu verlieren. Zwar können Sie keinen Einfluss auf die Sicherheitsmängel bei Dritten nehmen, Sie können das Risiko jedoch durch umsichtiges Verhalten verringern und anhand der eigenen Rechnersicherheit aufzeigen, dass Sie sich im Rahmen Ihrer Möglichkeiten korrekt verhalten haben. Surfen Sie hingegen ohne Virenscanner, haben Sie später sehr schlechte Karten zu argumentieren, Sie hätten den Missbrauch nicht fahrlässig in Kauf genommen.

Accounts

Bei zahlreichen, vor allem größeren Online-Angeboten ist es möglich oder sogar nötig, einen Account anzulegen, bevor man dort einkaufen kann. Dieser Account wird mittels einer Benutzerkennung und eines Passworts geschützt und enthält neben den Kundendaten auch Zahlungsinformationen und die Bestellhistorie. Beim

ersten Betreten eines Shops richtet man sich so ein Profil ein, mit dem man in Zukunft bequem ohne ständiges Neueingeben der Daten einkaufen kann. Leider führen die meisten Betreiber keinen Sicherheitscheck der von den Kunden gewählten Passwörter durch und riskieren somit mögliche Cracker-Angriffe.

Genauso gefährlich ist auch die Variante, bei der der Anbieter dem Kunden das Passwort mittels einer unverschlüsselten E-Mail zukommen lässt. In beiden Fällen hätte ein Angreifer leichtes Spiel, an die Account-Daten zu gelangen und somit auch die Zahlungsmodalitäten zu verändern oder sonstigen Mißbrauch zu betreiben. Achten Sie daher darauf, ein sicheres Passwort zu wählen und es in regelmäßigen Abständen zu ändern. Sollten Sie Ihr Kennwort per E-Mail erhalten haben, ist es ebenfalls angebracht, zügig ein neues zu wählen. Leider gibt es immer noch Shops, die einen Wechsel der Login-Daten nicht zulassen; in diesen Fällen sollten Sie den Anbieter entweder per E-Mail auf diese Sicherheitslücke hinweisen oder zukünftig auf Geschäfte mit ihm verzichten.

Grundsätzlich sollten Sie niemals das gleiche Passwort bei verschiendenen Online-Shops wählen – wohin das führen kann, haben wir bereits in Kapitel 3, *Sicherheitsbewusstsein*, ausführlich besprochen.

Produktdaten

Vor allem bei kleineren Online-Shops oder bei Anbietern, die den Webauftritt nur als zusätzliche Einnahmequelle sehen, gibt es oft Defizite bei den Produktdaten. Das reicht von veralteten Preisangaben bis hin zu ungenauen oder völlig falschen Beschreibungen der angebotenen Produkte. In einigen Produktbereichen, in denen sich die Preise häufig ändern (z.B. bei Hardware), ist es deshalb wichtig zu wissen, von wann die Preisangaben im Web stammen.

Daher zeigen viele Online-Shops das Datum der letzten Preisänderung auf der Internetseite an. Achten Sie deshalb darauf, dass die Preis- und Produktangaben nicht zu alt sind und vor allem regelmäßig aktualisiert werden. Shops, die nur selten ein Update ihrer Preise durchführen, bergen immer eine gewisse Gefahr in sich. Im Gegensatz zur »realen Welt« können Sie die Produkte ja nicht in Augenschein nehmen und sind daher darauf angewiesen, dass die Bezeichnungen im Web auch tatsächlich mit dem Produkt übereinstimmen. Immer wieder wird über Lieferungen berichtet, die nicht dem gewünschten Artikel entsprechen. Oft reicht z.B. bei Hardware schon ein Buchstabe in der Produktspezifikation, um zwei verschiedene Versionen eines Artikels zu kennzeichnen; daher ist hier besonders darauf zu achten, dass die Produktangaben vollständig sind.[7]

7 Nutzen Sie im Notfall Ihr Recht, die Ware innerhalb von 14 Tagen an den Händler zurückzuschicken. Eine Begründung ist dafür nicht nötig und es fallen (wenn der Kaufpreis über 40 € liegt) auch keine Versandkosten an.

Shop-Zertifizierung

Aus dem bisher Gesagten wird vor allem deutlich, dass Qualität und Vertrauenswürdigkeit eines Online-Shops für den Kunden selten wirklich einzuschätzen sind. Umso wichtiger ist es, sich auf seriöse Tests oder auch auf Zertifizierungsstellen verlassen zu können.

Das Unternehmen Trusted Shops GmbH führt genau solche Shop-Zertifizierungen durch (*http://www.trustedshops.de*, siehe Abbildung 7-2). Dabei muss ein Anbieter eine Reihe von Kriterien erfüllen, um Mitglied bei Trusted Shops zu werden und seine Website mit dem entsprechenden Gütesiegel schmücken zu dürfen. Wir wollen diese Anforderungen kurz betrachten, um die Vor- und Nachteile der Zertifizierung besser einschätzen zu können. Behalten Sie dabei jedoch unbedingt im Hinterkopf, dass Trusted Shops, wie auch zahlreiche andere Zertifizierungsstellen, vom Zertifizieren lebt.

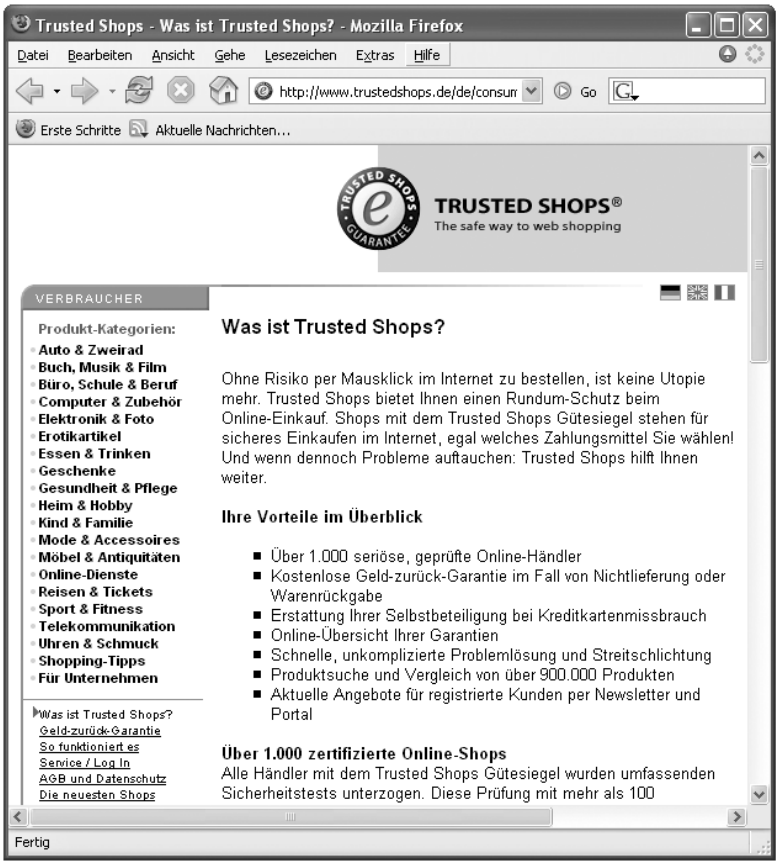

Abbildung 7-2: Die Startseite von Trusted Shops

Anbieterkennzeichnung

Der Betreiber verpflichtet sich dazu, eine vollständige Anbieterkennzeichnung leicht auffindbar auf seiner Internetseite zu positionieren.

Allgemeine Geschäftsbedingungen und Vertragsabschluss

Auf der Ausgangsseite muss ein gut sichtbarer Verweis sowohl auf die AGB als auch auf alle ähnlichen Informationen und Bedingungen enthalten sein. Der Inhalt sollte leicht verständlich formuliert und gut lesbar sein (z.B. Schriftgröße). Zudem wird verlangt, dass die Produktdaten vollständig sind und dem Kunden samt der AGB vor der Bestellung zur Verfügung gestellt werden.

Jugendschutz und E-Mail-Werbung

Die angebotenen Artikel müssen den gesetzlichen Bestimmungen, insbesondere im Hinblick auf den Jugendschutz, genügen. Die Leichtgläubigkeit und Unerfahrenheit von Kindern darf nicht ausgenutzt werden. Die gesammelten Kundendaten dürfen nicht für E-Mail-Werbung (Spam) missbraucht werden, wenn dies nicht ausdrücklich vom Kunden erwünscht ist.

Preistransparenz und Zahlungsbedingungen

Sämtliche Preise inklusive Steuern und Zusatzkosten (z.B. Porto) müssen leicht auffindbar bei den Produkten aufgeführt werden. Bereits vor der endgültigen Bestellung muss der Gesamtpreis samt allen Zahlungsbedingungen für den Kunden ersichtlich sein.

Bestellbestätigung

Der Kunde erhält unverzüglich nach der Bestellung eine Bestätigung, die mindestens das Bestelldatum, das voraussichtliche Lieferdatum, alle bestellten Artikel mit Einzelpreis und den gesamten Endpreis der Bestellung enthält.

Leistungserbringung und Kundenservice

Alle Kundenanfragen müssen »innerhalb angemessener Zeit« beantwortet werden. Der Anbieter ist verpflichtet, den Kunden darüber zu informieren, wenn sich der Liefertermin verzögert oder die bestellte Ware kurzzeitig vergriffen ist und der genannte Liefertermin daher nicht eingehalten werden kann.

Widerrufs- oder Rückgaberecht und Kaufpreiserstattung

Die von Trusted Shops gestellten Anforderungen bezüglich dieser Punkte beziehen sich vor allem auf die Informationspflicht und das zweiwöchige Rückgaberecht und sind inzwischen durch deutsches Recht ausreichend abgesichert. Zusätzlich wird ein Rückgabeformular verlangt, das den Kunden über seine Rechte informiert und ihm die Möglichkeit gibt, sich zu der Rückgabe zu äußern.

Datenschutz

Der Online-Shop muss die Gesetze zum Datenschutz einhalten und dem Kunden alle dazu verfügbaren Informationen offen legen. Personenbezogene Daten dürfen nur mit Erlaubnis des Kunden an Dritte weitergegeben werden. Zudem verpflichten sich die Betreiber allgemein, so wenig personenbezogene Daten

wie möglich zu sammeln, und speziell, den Kunden verständlich über den Einsatz von Cookies zu informieren. Der Kunde hat jederzeit das Recht, seine Daten löschen zu lassen.

Daten- und Systemsicherheit
: Der Online-Shop verpflichtet sich, die Daten nur verschlüsselt zu übertragen und einen sicheren Server zu benutzen. Die Art der Verschlüsselung wird dem Kunden verständlich mitgeteilt. Es ist erlaubt alternativ auch unverschlüsselte Verbindungen zuzulassen wenn der Benutzer dies ausdrücklich wünscht und über potenzielle Gefahren informiert wurde.

Der vollständige Anforderungskatalog findet sich unter *http://www.trustedshops.de/de/shops/obligations_de.html*.

Wie Sie sehen, spielt die technische Systemsicherheit in diesen Anforderungen nur eine untergeordnete Rolle. Vielmehr werden hier Kriterien genannt, die eine Art Standard für seriöses Online-Shopping darstellen sollen. Da bei Trusted Shops bereits viele hundert Anbieter aus den verschiedensten Bereichen zu finden sind, scheint sich diese Art der Zertifizierung durchsetzen zu können. Bedenken Sie jedoch, dass der Online-Shop dadurch nicht unbedingt auch technisch sicherer wird, da die Forderung nach einer verschlüsselten Übertragung und einem sicheren Server relativ allgemein gehalten sind. Es gibt zahlreiche andere Zertifizierungsstellen, die sich ausschließlich auf diese Aspekte konzentrieren.

Ein weiteres interessantes Feature von Trusted Shops ist die Geld-Zurück-Garantie. Nach dem Einkauf bei einem zertifizierten Anbieter können Sie sich bei Trusted Shops anmelden und erhalten dann eine Geld-Zurück-Garantie, wenn es bei (nach) dem Einkauf zu Schwierigkeiten kommen sollte. Näheres dazu finden Sie auf den Seiten des jeweiligen Anbieters oder unter *http://www.trustedshops.de/de/consumers/guarantee_de.html*.

In einem Buch über Internetsicherheit läuft man Gefahr, nur die Problemfälle zu thematisieren, ohne zu zeigen, dass es auch anders geht. Daher sei an dieser Stelle auch ein positives Beispiel vorgestellt. Der Online-Shop der *computeruniverse.net GmbH* lässt in den Punkten Kundenaufklärung und Sicherheitsbewusstsein eigentlich keine Wünsche offen. Wie man in Abbildung 7-3 erkennen kann, befinden sich auf der Homepage gut erkennbare Hinweise auf gleich fünf verschiedene (unabhängige) Zertifikate.[8] Per Mausklick gelangt man auf eine Infoseite, auf der die einzelnen Zertifikate genauer und vor allen Dingen verständlich erklärt werden. Von dort aus kommt man auch auf die Seite des Zertifizierungsdienstes. Dies ist besonders wichtig, da jeder beliebige Online-Shop einfach das Zertifikatlogo auf seiner Internetseite einbinden könnte – es handelt sich dabei schließlich nur um eine simple Computergrafik. Im Zweifel ist es daher immer angebracht, das Zertifikat zu über-

8 Wobei es natürlich auf die Qualität und nicht die Menge der Zertifikate ankommt, lassen Sie sich also nicht blenden.

prüfen. Rechts unten am Rand jeder computeruniverse.net-Webseite finden Sie einen Link zum Impressum (Anbieterkennzeichnung) sowie eine Erklärung zum Datenschutz. Von dort aus führen wiederum Links zu zahlreichen Informationen über die Sicherheitsmaßnamen des Anbieters, den Sinn und die Funktion von Cookies, den Umgang mit den Kundendaten und vielem mehr. Diese und weitere Informationen sind auch über den Menüpunkt INFO&SERVICE zu erreichen. Tippen Sie einmal zum Spaß »Sicherheit im Internet« in die Suchmaske. Sie erhalten anschließend nicht nur einen Überblick über relevante Produkte (z.B. Bücher), sondern auch entsprechende Hilfsthemen wie etwa eine Warnung über Computerviren, die unter Missbrauch der computeruniverse.net-Mailadressen verschickt wurden.

Abbildung 7-3: Unterschiedliche Shop-Zertifikate bei computeruniverse.net

All diese Informationen und Zertifikate sagen noch nichts darüber aus, ob der Online-Shop nicht doch erfolgreich angegriffen werden könnte, aber sie zeigen deutlich das Bewusstsein des Anbieters für diese Problematik und den Willen, den Kunden über die gegebene Situation zu informieren und für Transparenz zu sorgen. Leider nehmen es zahlreiche (auch große) Anbieter mit ausreichenden und verständlichen Informationen nicht so genau.

Online-Banking

Beim Online-Banking muss man zunächst zwischen dem eigentlichen Home-Banking z.B. mittels T-Online und dem Banking über das Internet differenzieren. Der Hauptunterschied liegt im verwendeten Netz, wobei es sich beim Home-Banking um ein geschlossenes und beim Internet-Banking um ein offenes Netzwerk handelt.

Beim Home-Banking kommunizieren Sie mit der Bank nur über den Umweg über den Provider und dessen Netz. Im Gegensatz dazu sind im Internetmodell noch zahlreiche weitere Zwischenstationen (z.B. Router) an der Kommunikation beteiligt. Zwischen Ihnen und der Bank liegt also ein offenes, nicht vertrauenswürdiges Netz. Obwohl das Home-Banking aufgrund des geschlossenen Netzes seine Daseinsberechtigung hat, wird sich auf kurz oder lang dennoch Internet-Banking durchsetzen, das bereits jetzt von der überwältigenden Mehrheit der Banken und Kreditinstitute unterstützt wird. Wir wollen uns zunächst mit den technischen Aspekten des Internet-Banking befassen und uns anschließend die Sicherheitsproblematik anhand vier berühmter »virtueller Banküberfälle« vor Augen führen.

Verschlüsselungsverfahren

Um die Kommunikation zwischen Bank und Kunden so sicher wie möglich zu gestalten, wird diese zwar verschlüsselt, es muss jedoch zudem sichergestellt werden, dass nur autorisierte Personen Zugriff erhalten. Dazu verwendet man, grob gesagt, zwei Ansätze: zum einen das PIN/TAN-Verfahren und zum anderen HBCI.

PIN/TAN

Derzeit verwenden über 90% der Banken das PIN/TAN-Verfahren, bei dem es einerseits eine *PIN (Personal Identification Number)* zur Autorisierung des Kunden und andererseits die *TAN (Transaction Number)* zur Autorisierung der einzelnen Transaktionen gibt.[9] Nachdem Sie bei Ihrer Bank als Online-Kunde freigeschaltet worden sind, werden Ihnen sowohl PIN als auch mehrere TANs jeweils in einem gesonderten Brief zugeschickt. Einige Banken setzen die PIN standardmäßig auf »12345«, so dass sich der Surfer beim ersten Betreten des Online-Angebots eine neue PIN ausdenken muss. Nachdem Sie sich per Kontonummer und PIN bei Ihrer Bank angemeldet haben, können Sie Ihren Kontostand einsehen oder Überweisungen tätigen. Bevor diese Überweisung jedoch wirksam wird, muss sie durch eine Nummer aus Ihrem TAN-Bestand autorisiert werden. Jede dieser TANs verliert nach einmaliger Benutzung ihre Gültigkeit und wird aus dem Bestand gestrichen.

9 In der ersten Auflage dieses Buches war hier von 80% die Rede, und ich war eigentlich sicher, in einer späteren Auflage nichts mehr über PIN/TAN schreiben zu müssen. Erstaunlicherweise muss man die Zahl sogar nach oben korrigieren. Anscheinend dringt das Wissen um die Gefahr durch Phishing (welches nur beim PIN/TAN-Verfahren möglich ist) nur sehr langsam bis zu den Verantwortlichen vor.

Wenn alle TANs verbraucht worden sind, sendet Ihnen die Bank automatisch einen neuen Block zu. Der Sicherheitsmechanismus greift also auch dann, wenn Sie die PIN einmal verlieren, da der Angreifer dann zwar an Ihre Kontoauszüge gelangt, aber keine Überweisungen oder Ähnliches tätigen kann. Auf keinen Fall aber sollten Sie die TANs auf Ihrer Festplatte speichern oder auf eine andere elektronische Art zugänglich machen.

Eigentlich galt das PIN/TAN-Verfahren in den letzten Jahren als recht sicher, es ist aber besonders gegen Trojaner anfällig. Ein Trojaner fängt dabei eine eingegebene TAN ab, bevor sie zur Bank gesendet wird, und fordert den Benutzer auf, eine weitere einzugeben, da die gerade verwendete angeblich ungültig sei. Dies wirkt insofern plausibel, als TANs meist verdeckt eingegeben werden, der Benutzer also nicht sieht, wenn er sich vertippt. Die zweite TAN wird dann verwendet, um die Transaktion zur Zufriedenheit des Nutzers auszuführen, während der Angreifer mit der erbeuteten ersten TAN eigene Transaktionen durchführen kann. Eine Variante dieses Tricks besteht darin, den Computer des Bankkunden zum Abstürzen zu bringen, nachdem der Angreifer die TAN mit Hilfe seines Trojaners erbeutet hat. Auf diese Weise hindert er den Kunden für einige Minuten am Absenden der Überweisung und kann in dieser Zeit selbst tätig werden.

Inzwischen braucht es aber keine Trojaner mehr, um das PIN/TAN-Verfahren auszuhebeln, denn dies ist mittels einer einfachen Social Engineering-Attacke (Phishing) ebenfalls leicht möglich. Daher muss man deutlich darauf hinweisen, dass aus Sicherheitsgründen das PIN/TAN-Verfahren nicht mehr genutzt werden sollte. Als Kunde sollten Sie Ihre Bank also unbedingt dazu bewegen, Ihnen Home-Banking per HBCI zur Verfügung zu stellen. Wie schnell man ansonsten unter Umständen sein Geld los ist, werden wir uns in den nächsten Abschnitten und im Kapitel 11, *Angriffsszenarien*, genauer anschauen.

HBCI und FinTS

Das *Home-Banking Computer Interface* (HBCI) und die *Financial Transaction Services (FinTS)* liegen derzeit in der Version 4.0 vor und scheinen sich als offizieller Standard für Internet-Banking durchzusetzen. Angestrebt wird bei diesem Verfahren eine Kombination aus asymmetrischer Verschlüsselung und Chipkarten oder das PIN/TAN-Verfahren. Um zu verstehen, warum wir in diesem Buch dennoch zwischen HBCI und FinTS[10] auf der einen und PIN/TAN auf der anderen Seite unterscheiden, müssen wir etwas weiter ausholen.

HBCI wurde Mitte der 90er des letzten Jahrtausends als Alternative zum unsicheren PIN/TAN-Verfahren vorgeschlagen. Eine Zeit lang schien es dann so, als würde sich

10 Eigentlich ist HBCI inzwischen Teil des FinTS-Standards, wir werden der Übersichtlichkeit halber aber HBCI schreiben, wenn das Chipkartenverfahren gemeint ist. Dies entspricht auch der Regelung im FinTS Standard.

HBCI auf Grund immer neuer, erfolgreicher Angriffe auf PIN/TAN (siehe unten) durchsetzen. Letztendlich ist dies jedoch (aus Kostengründen) nicht der Fall gewesen. Stattdessen wurde 2002 FinTS der Nachfolgestandard von HBCI und kurz darauf um PIN/TAN erweitert. Im Moment gibt es also in diesem Bereich ein FinTS-Verfahren mit HBCI und FinTS mit PIN/TAN. Letzteres wurde als großer Erfolg gefeiert, ist in Wirklichkeit aber ein schlechtes Tauschgeschäft, in dem Sicherheit gegen Bequemlichkeit und eine geringfügige Kostenersparnis seitens der Geldinstitute getauscht wurde.

HBCI-Verfahren haben im Vergleich zu PIN/TAN-Verfahren den Vorzug, dass eine verschlüsselte Verbindung zusammen mit einer persönlichen Chipkarte benutzt wird. Diese Chipkarte ist zusätzlich durch eine PIN geschützt, so dass bei Verlust die Gefahr des Missbrauchs deutlich verringert wird. Was HBCI zudem besonders sicher macht, ist die Möglichkeit, die Karte nach erfolgtem Online-Banking einfach aus dem Chipleser zu ziehen und damit Angriffe auszuschließen.

Um diese Chipkarte benutzen zu können, brauchen Sie ein zusätzliches Lesegerät für Ihren Computer. Grob gesagt gibt es drei Klassen von Chipkartenlesern. Die kleinste Version (Sicherheitsklasse 1) ist ein einfaches Lesegerät, das Sie per USB oder PCMCIA an Ihren Computer anschließen können. Geräte der Klasse 1 besitzen weder ein eigenes Display noch eine Tastatur. Die Eingabe der PIN erfolgt daher über die Computertastatur. Der Preis liegt üblicherweise unter 20 Euro. Lesegeräte der Klasse 2 und 3 besitzen hingegen eine eigene Tastatur und lassen sich per USB an den Computer anschließen. Die Eingabe der PIN findet daher direkt auf dem Gerät statt, der Computer bleibt dabei völlig außen vor. Im Unterschied zu Klasse-2-Geräten besitzen Klasse-3-Geräte ein zusätzliches Display und sind darüber hinaus multifunktional. In Zukunft wird man beispielsweise seine Geldkarte auf diesem Weg online von zu Hause aus aufladen können. Zudem lassen sich diese Geräte updaten, so dass der Hersteller sie um neue Funktionen erweitern oder bestehende Sicherheitsmerkmale verbessern kann. Leser der Klasse 2 kosten zwischen 40 und 60 Euro, für einen der Klasse 3 sind es dann noch einmal 10 bis 20 Euro mehr. Die HBCI-Chipkarte erhalten Sie bei Ihrer Bank für eine einmalige Gebühr, die in der Regel unter 10 Euro liegt.

Ob Sie sich für ein Gerät der Klasse 2 oder 3 entscheiden, liegt in Ihrem eigenen Ermessen. Wir würden zu einem Gerät der Klasse 3 raten, da diese völlig unabhängig vom Computer arbeiten. Sie können die einzelnen Schritte der Überweisung auf dem eingebauten Display verfolgen und schließen somit aus, dass das, was Sie am PC sehen, vielleicht nur vorgegaukelt ist. Geräte der Klasse 1 sollten Sie besser nicht verwenden. In dem Moment, in dem Sie Ihre PIN über die Computertastatur eingeben, werden Sie für Angriffe mit Trojanern und Keyloggern anfällig, da diese die eingegebene PIN quasi mitlesen können. Dies muss zwar noch nicht für einen erfolgreichen Angriff ausreichen, hebelt aber bereits einen der wichtigsten Sicherheitsmechanismen aus.

Viele Banken unterstützen HBCI, bieten dem Kunden aber lieber ein PIN/TAN-Verfahren an. Banken befürchten anscheinend, den Kunden zu verschrecken, wenn sie sie mit der einmaligen Investition von ca. 80 Euro konfrontieren, und legen ihnen eher das kostenlose PIN/TAN-Online-Banking nahe. Wie kurzsichtig diese Einstellung ist, zeigt sich gerade jetzt in den Zeiten von Phishing sehr deutlich. Statt die Schuld bei der eigenen Informationspolitik und Sicherheitsstrategie zu suchen, ist man in Einzelfällen sogar dazu übergegangen, die eigene Kundschaft (die noch dazu Opfer von Phishing geworden ist) zu verklagen. Fragen Sie daher unbedingt bei Ihrer Bank nach HBCI, die Einstiegskosten lohnen sich gerade bei den flexiblen Geräten allemal, und man läuft nicht Gefahr, plötzlich vor einem leeren Konto zu stehen.[11]

Früher wurde bei der Einrichtung eines Online-Banking-Accounts eine Grenze festgesetzt, wie viel Geld maximal pro Tag bewegt werden darf. Diesen durchaus sinnvollen Schutz gibt es inzwischen nicht mehr, oder nur noch auf Nachfrage. Daher ist es tatsächlich möglich, mit einer einzigen erbeuteten TAN mehrere Tausend Euro zu stehlen.

Nähere Informationen zum HBCI- und FinTS-Standard finden Sie auf der Seite *http://www.hbci-zka.de/*. Dort können Sie sich auch darüber informieren, ob Ihre Bank HBCI unterstützt. Chiplesegeräte bekommen Sie entweder im Online-Shop Ihrer Bank oder im (Online-)Fachhandel.

Virtuelle Bankräuber

Dass geschlossene Netze nicht zwangsläufig sicherer sind als offene, zeigt der Einbruch zweier Jugendlicher in das Home-Banking-System von T-Online. Mittels eines Trojaners war es ihnen 1998 gelungen, an über 600 Zugangskennungen und damit auch an die Konten der Kunden zu gelangen. Zwar wurde dabei kein Schaden angerichtet, da die Hacker keine bösartigen Motive verfolgten, der Einbruch machte jedoch die Schwachpunkte dieser Systeme deutlich. In den folgenden Beispielen wollen wir uns mit einigen prominenten Bankeinbrüchen im Zusammenhang mit Internet-Banking beschäftigen.

Vladimir Levin

Der spektakulärste und wohl meistdiskutierte virtuelle Bankraub fand 1994/95 in Russland statt. Damals ist es Vladimir Levin aus St. Petersburg gelungen, in die amerikanischen Rechner der Citibank einzubrechen und Passwörter für zahlreiche Konten zu stehlen. Anschließend transferierte er über 10 Millionen US-Dollar auf

11 Dies bedeutet natürlich nicht, dass jedes PIN/TAN-Konto gleich virtuellen Bankräubern zum Opfer fällt. Die Gefahr ist jedoch um ein Vielfaches größer und die Anzahl der Vorfälle hat sich 2005 stark erhöht. Dies ist ein Hinweis dafür, dass PIN/TAN einfach nicht mehr zeitgemäß ist.

verschiedene Depots in zahlreichen Ländern. Im März 1995 wurde er jedoch verhaftet, da die Spuren der Überweisungen zu ihm zurückführten. Trotz dieses nur kurzfristigen Erfolgs gilt er noch heute als eine der Hacker-/Cracker-Größen und ist in zahlreichen »Halls of Fame« verewigt.

Dieses Beispiel zeigt zwar die Gefahren im Online-Banking, aber auch den Vorteil des Buchgeldes. Selbst wenn ein virtueller Bankraub gelingt, verbleiben im Gegensatz zum Bargeld Transaktionsspuren, die zum Täter führen können. Das macht einen erfolgreichen Einbruch in einer solchen Größenordnung zwar nicht unmöglich, jedoch zumindest unwahrscheinlich. Inzwischen setzen organisierte Kriminelle jedoch Strohmänner ein, um dieses Problem zu umgehen. Daher sind virtuelle Bankraube derzeit sehr wohl möglich und finden auch tatsächlich statt. Große Summen lassen sich so jedoch nur sehr schlecht oder nur über längere Zeiträume hinweg erbeuten.

Der ActiveX-Hack (CCC 1997)

Anfang 1997 kam es im Rahmen einer Veranstaltung des CCC (Chaos Computer Club) zu einer Diskussion über so genannte »Attacken nullter Ordnung« auf Internet-Banking-Systeme. Ziel war es, experimentell zu testen, ob es innerhalb kürzester Zeit möglich sein würde, das System des Anwenders (also den Start- bzw. Endpunkt der Kommunikation, daher »nullte Ordnung«) so zu kompromittieren, dass ein Zugriff auf dessen Online-Konto möglich würde. Da der Angriff eine große Streubreite haben sollte, entschloss man sich dazu, einerseits den Internet Explorer und andererseits Quicken, das am häufigsten genutzte Programm für Kontenverwaltung und Online-Banking, zu benutzen. Als Köder diente eine simple Internetseite mit einem ActiveX-Control.

Wenn der ahnungslose Surfer die Seite betrat, wurde im Hintergrund ohne sein Wissen *Quicken* gestartet und durch das Control ferngesteuert. Anschließend konnten beispielsweise Überweisungen oder Ähnliches getätigt werden, während der Benutzer noch auf das Laden der Webseite wartete. Damit das im Hintergrund laufende *Quicken* nicht sichtbar wurde, manipulierte das ActiveX-Control mittels eines Befehls auf Betriebssystemebene den Client so, dass der Internet Explorer immer im Vordergrund blieb. Das Problem bei dieser Art Attacke nullter Ordnung liegt vor allem darin, dass der Server der Bank korrekterweise den Kunden als Kommunikationspartner annimmt, weil er nicht weiß, dass dieser durch ein ActiveX-Control ferngesteuert handelt. Der »Fehler« liegt also nicht auf Seiten der Bank, sondern beim User.

Da die Einzelheiten dieses faszinierenden Hacks komplett im Internet veröffentlicht wurden, möchten wir uns eher mit den Folgen dieses Angriffs als mit den technischen Gegebenheiten beschäftigen. Ein Blick auf den entsprechenden *iX*-Artikel unter *http://www.heise.de/ix/artikel/1997/03/090/* lohnt aber mit Sicherheit und demonstriert zudem sehr anschaulich, wie Hacks funktionieren und welche Motive sich dahinter verbergen (in diesem Fall eben keine kriminellen!).

Die Konsequenzen, die aus diesem Angriff gezogen werden können, sind recht eindeutig. Angriffe auf Kommunikationsendpunkte umgehen leicht alle Sicherheitssysteme wie Verschlüsselungen und PINs und werden in Zukunft stark an Bedeutung gewinnen. Desweiteren bestätigt sich unsere Vermutung aus Kapitel 5, *Browser – einer für alles*, dass der Einsatz ein und derselben Programmiersprache für Web, Anwendungen (*Quicken*) und Betriebssystem fatale Folgen haben kann. Allein der Besuch einer Internetseite kann bei Microsoft-Produkten schon ausreichen, um das gesamte System zu kompromittieren.

Der Dresdner Bank-Hack von Jordan Hrycaj (CCC Frankfurt)

Um die Unzulänglichkeiten in der damaligen Implementierung des HBCI-Standards aufzuzeigen, hackte der CCC Frankfurt Online-Konten bei der Dresdner Bank. Der Angriff fand live beim Hessischen Rundfunk statt und erwies sich im Nachhinein als weit einfacher als erwartet.

Auch hier wurde der Client-PC des Kunden als Angriffsziel ausgewählt. Per E-Mail (oder Download) verschickten die Hacker einen Trojaner auf die Computer und brachten diese so unter ihre Kontrolle. Mittels des Trojaners konnten sie nicht nur den PC fernsteuern, sondern auch alle Tastatureingaben protokollieren. Nachdem Hrycaj so an das Kennwort des Kunden gelangt war, meldete er sich einfach mittels der noch im Lesegerät befindlichen Chipkarte des Users bei der Bank an und konnte so beliebige Transaktionen auf dem Konto ausführen.

Um HBCI auf diese Weise auszuhebeln, muss lediglich die Voraussetzung gegeben sein, dass die Chipkarte eingelegt ist, ohne dass bereits eine Verbindung zur Bank besteht. Zwei Zugänge desselben Accounts sind zur gleichen Zeit eigentlich nicht möglich; doch laut Jordan Hrycaj ist aber auch das kein Problem, da man den Kunden mittels eines Fensters im Design der Dresdner Bank einfach auffordern könnte, die Chipkarte wieder einzulegen, während man gleichzeitig die aktive Sitzung zur Bank unterbricht, um eine eigene aufzubauen. Beides ist problemlos möglich, da der Trojaner vollen Zugriff auf den PC zulässt.

Da HBCI ein Standard ist, tritt diese Sicherheitslücke nicht nur bei der Dresdner, sondern bei allen Banken auf, die HBCI unterstützen. Der Hack zeigt wiederum, dass es mit der Absicherung der Endpunkte mit Chipkarten allein nicht getan ist, sondern dass es vor allem um eine eindeutige Identifizierung der Absicht des Kunden geht. Für den Bankserver sieht ja alles völlig korrekt aus, da sich der Trojaner wie ein Kunde verhält. Den einzig effektiven Schutz vor diesem Angriff bietet ein Klasse-2- oder Klasse-3-Lesegerät, bei dem die Eingabe des Kennworts nicht über die Tastatur des Computers, sondern direkt über den Chipkartenleser erfolgt, und der zudem immer eine Bestätigung des Kunden per Knopfdruck anfordert.

Weitere Informationen zu diesem HBCI-Hack finden Sie im Netz *beispielsweise* unter *http://www.tecchannel.de/news/themen/business/405181/*. Von dort aus können Sie sich zu Details und technischen Grundlagen durchklicken.

Der »Ratgeber Technik«-Hack von Thomas Vosseberg

Nach der Lektüre der beiden CCC-Hacks ist man gewillt zu glauben, die Sicherheitsstandards wären nun so ausgefeilt, dass ein einfacher Angriff keinen Erfolg mehr haben könnte. Doch Mitte September 2001 strahlte die ARD in ihrer Sendung »Ratgeber Technik« einen besonders spektakulären Hack aus. Dabei gelang es dem Hacker Thomas Vosseberg unter anderem, von den gehackten Bankkunden sowohl die PIN als auch eine gültige TAN zu erbeuten und damit eine Testüberweisung von 50 Euro durchzuführen. Da wir solch einen Angriff nullter Ordnung in einer anderen Form bereits kennen gelernt haben, möchten wir diesen hier nicht mehr weiter besprechen, sondern die Ergebnisse eines anderen Teils des Angriffs näher beleuchten.

Dabei sollte untersucht werden, wie gut die Server der Banken gesichert sind, und ob es möglich wäre, von dort aus an die benötigten Informationen zu gelangen. Bisher war man eigentlich davon ausgegangen, dass ein direkter Angriff auf den Zentralcomputer einer Bank nicht erfolgreich sein könnte. Die Überraschung war umso größer, als sich herausstellte, dass zahlreiche Server nur mangelhaft gesichert waren. Besonders schwer traf es dabei den Server der HypoVereinsbank. Durch einen völlig falsch konfigurierten Webserver (Microsoft IIS 4.0) gelang es dem Hacker mittels einiger Tricks, Zugriff auf das System zu erlangen und innerhalb weniger Tage 1,5 Millionen Online-Buchungen durchzuführen und jede Menge Geheimnummern (PINs) zu erbeuten, ohne dass man bei der Bank Verdacht geschöpft hätte. Gegen solch fahrlässige Fehler von Seiten der Banken sind Sie als Benutzer leider völlig schutzlos, zumindest bleibt aber zu hoffen, dass dieser Hack zu Konsequenzen auf der Betreiberseite führt.

Phishing

Phishing ist eine Spielart des Trickbetrugs, die gerade im Zusammenhang mit Online-Banking immer häufiger auftritt. Dabei handelt es sich um eine Kombination aus Social Enginnering, Identitätsdiebstahl und einer Art Man-in-the-Middle-Attacke. Der Angreifer verschickt massenhaft E-Mails[12] an alle ihm bekannten (von ihm gesammelten) Adressen. Als Absender gibt er dabei den Namen einer Bank an und und wählt eine sinnvolle und glaubwürdige Absenderadresse wie etwa *administrator@deutsche-bank.de*. In der Mail, die möglichst den Eindruck einer offiziellen

12 Phishing an sich ist aber nicht auf E-Mail beschränkt, genauso könnte es eine Nachricht im einem Instant Messenger sein.

Mail des Geldinstituts erwecken soll, wird der Kunde unter verschiedenen Vorwänden (wie oben beschrieben neuerdings ironischerweise sogar als Schutz vor Phishing) aufgefordert, seine Kontodaten sowie PIN und eine TAN einzugeben. Dazu soll man einem Link in der Mail folgen, der scheinbar auf die Seite der Bank führt. In Wirklichkeit handelt es sich aber um eine gefälschte Seite, die dem Original verblüffend gut nachempfunden ist.

Haben Sie sorglos Ihre Daten eingegeben, werden Sie anschließend auf die Originalseite der Bank weitergeleitet und bemerken den Betrug nicht. Einige Tage später befindet sich aber womöglich viel weniger Geld auf Ihrem Konto als zuvor. Bemerken Sie den Betrug, sollten Sie sich unverzüglich mit der Bank und der Polizei in Verbindung setzen. Das gilt übrigens auch für den Fall, dass Sie plötzlich Geld auf Ihrem Konto haben, das Sie keinem Ihnen bekannten Auftraggeber zuordnen können. Ansonsten müssen Sie mit juristischen Konsequenzen seitens des Geldinstituts wegen des Verdachts auf Geldwäsche rechnen.

Zum Schutz vor Phishing haben einige Banken ihr TAN-System auf das so genannte iTAN-System (indizierte Transaktionsnummern) umgestellt. Dabei ist es nicht mehr möglich, eine beliebige TAN aus dem TAN-Block einzugeben. Stattdessen entscheidet der Bankserver per Zufallsprinzip, welche TAN Sie eingeben müssen. Alle anderen TANs werden nicht akzeptiert. Daher kann der Angreifer mit einer erbeuteten TAN nur wenig anfangen, es sei denn, er hätte das große Glück, ausgerechnet diejenige zu erwischen, die im weiteren Verlauf auch vom Banksystem abgefragt wird. Leider arbeiten viele Banken dennoch mit dem alten TAN-System weiter.

Dennoch hilft die iTAN-Sicherung nicht, wenn der Angriff über einen Phishing-Trojaner stattfindet. Mit solchen Trojanern werden wir uns in Kapitel 11, *Angriffsszenarien*, noch genauer befassen. Zudem ist es nur eine Frage der Zeit, bis die ersten erfolgreichen Angriffe gegen iTAN bekannt werden. Nur HBCI bietet ausreichend Schutz.