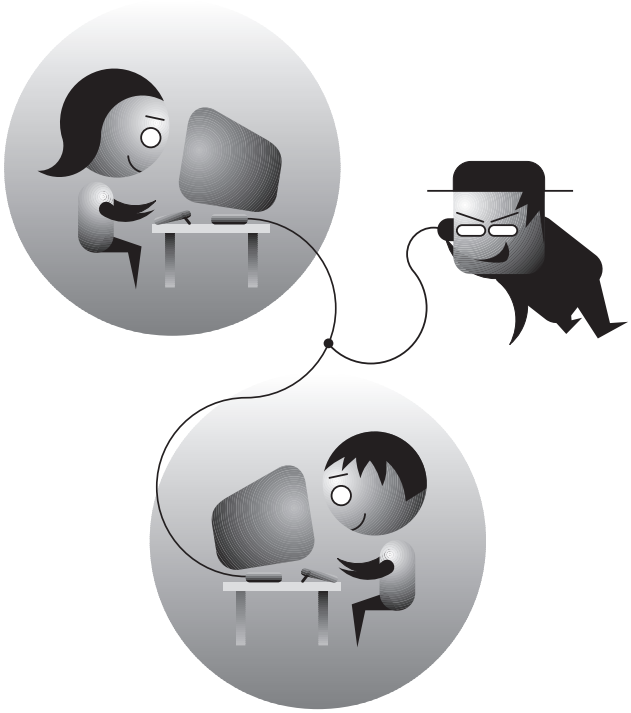


Risiko Internet?

Sicherheitsaspekte bei der Internet-Benutzung

Michael Näf
Patrick Streule
Werner Hartmann

Urheberschaft: Michael Näf, Patrick Streule, Werner Hartmann

Illustrationen: François Chalet

Das vorliegende Dokument ist die kostenfreie Version im Format PDF des 2000 im Orell Füssli Verlag Zürich unter demselben Titel erschienenen Buches.

Wichtig: Obwohl das Buch 2000 erschienen ist, sind die meisten Informationen darin nach wie vor gültig. Verschiedene neuere Risiken sind aber nicht abgedeckt , zum Beispiel Phishing. Den Leserinnen und Lesern wird deshalb die ergänzende Lektüre einschlägiger Websites empfohlen, zum Beispiel `http://www.bsi-fuer-buerger.de/`.

Inhalt

Einleitung

Internet – Netz der Netze, Datenozean, Information Superhighway. Das Internet kennt viele Bezeichnungen und ebenso viele Anwendungen. Wir kommunizieren per E-Mail, verschicken elektronische Bücher und Musikdateien, beziehen neue Software aus dem Internet und profitieren vom Netz als schier unerschöpflicher Informationsquelle. Auch der Zahlungsverkehr erfolgt immer häufiger über die elektronischen Medien. Selbst amtliche Stellen nutzen zunehmend die neuen Möglichkeiten. Die Durchführung von Abstimmungen via Internet ist nur noch eine Frage der Zeit.

Das Internet wurde im Hinblick auf einen einfachen, schnellen und robusten Datenaustausch konzipiert. Sicherheitsaspekte standen nicht im Vordergrund. Unterdessen aber haben die Dienste des Internets im Alltag Einzug gehalten, und Fragen rund um die Sicherheit im Internet sind zu einem relevanten Thema geworden.

Internet-Benutzer sind besorgt um die Wahrung ihrer Privatsphäre. Online-Firmen möchten möglichst gute Profile ihrer Kunden erstellen. Beim elektronischen Briefverkehr sollte die Identität des Absenders überprüft werden können. Und Online-Zahlungsverkehr wird sich nur durchsetzen, wenn ausreichende Sicherheitsvorkehrungen getroffen werden. Eine Vielzahl von Gefahren lauert im Internet: Unabsichtliches Fehlverhalten von Anwendern und Anwenderinnen kann zu Datenverlusten führen oder Unberechtigten Einsicht in vertrauliche Daten eröffnen. Computerviren und fehlerhafte Programme können ganze Systeme zum Absturz bringen. Immer wieder gelingt es Hackern, in vertrauliche Datenbestände einzudringen oder Online-Dienste lahm zu legen.

Die besten technischen Vorsichtsmassnahmen nützen wenig, wenn beispielsweise die Belegschaft einer Firma die Notwendigkeit und den Sinn von Sicherheitsvorkehrungen nicht erkennt oder versteht. Ausgeklügelte Mechanismen zur Verschlüsselung von E-Mails oder sichere Internet-Verbindungen beim Online-Banking erübrigen sich, wenn die Anwender diese Möglichkeiten falsch nutzen.

Hier setzt das vorliegende Buch an. Es vermittelt langlebiges Wissen rund um Sicherheitsfragen in der kurzlebigen Zeit des Internets. Wichtige Gefahrenquellen und mögliche Schutzmassnahmen werden aufgezeigt. Der Schwerpunkt liegt auf den grundlegenden Problemen der Informationsübertragung und Kommunikation im Internet. Es wird darauf verzichtet, Bedienungsanleitungen für spezifische Virenschutzprogramme oder Sicherheitseinstellungen für alle erdenklichen Browsermodelle aufzuführen. Bezüglich der im Internet lauernden Gefahren wird weder Schwarzmalerei noch leichtfertige Verharmlosung betrieben. Wichtiger ist es, den Anwenderinnen die Gefahren bewusst zu machen und grundlegende Verhaltensstrategien zu vermitteln, die auch noch in einigen Jahren ihre Gültigkeit haben.

Zielpublikum

Das Buch richtet sich an einen breiten Personenkreis von Internet-Anwendern und -Anwenderinnen, die über grundlegende Fertigkeiten und Erfahrungen mit dem Internet verfügen und sich im Hinblick auf eine sichere Nutzung der Internet-Dienste weiterbilden wollen. Das Buch richtet sich somit an alle, die im Berufsleben oder privat das Internet verantwortungsbewusst als Werkzeug einsetzen möchten.

Abgrenzung

Der im Buch behandelte Stoff konzentriert sich ausschliesslich auf Sicherheitsaspekte, mit denen Anwenderinnen und Anwender im Alltag konfrontiert werden. Die Erklärungen sind deshalb bewusst einfach gehalten, auf unnötige technische oder mathematische Details wird verzichtet. Systemadministratoren und Sicherheitsfachleute werden auf die entsprechende Fachliteratur verwiesen.

Aufbau

Das Buch ist in erster Linie als Lehrbuch aufgebaut. Die einzelnen Kapitel liefern jeweils die nötigen Voraussetzungen für die folgenden Kapitel. Dank dem ausführlichen Stichwortverzeichnis dient das Buch aber auch als hilfreiches Nachschlagewerk nach der ersten Lektüre. Alle Kapitel, mit Ausnahme des ersten und letzten, sind gleich aufgebaut. Ausgangspunkt sind jeweils typische Anwenderfragen, mit denen – konsequent aus der Perspektive der Anwenderin oder des Anwenders – in die Problematik eingeführt wird. Darauf folgen grundlegende Prinzipien und das theoretische Hintergrundwissen zum betreffenden Themengebiet. Ein praxisorientierter Teil vermittelt das für die Umsetzung der Theorie in die Praxis notwendige Wissen und liefert oft wertvolle Zusatzinformationen. Als Kapitelabschluss wird das erarbeitete Wissen auf die einführenden, beispielhaften Anwenderprobleme angewendet.

Keine Links

Wir verzichten in diesem Buch gänzlich auf die Angabe von Internet-Adressen, denn viele dieser Adressen wären schon kurz nach der Veröffentlichung nicht mehr gültig. Die wenigen konkreten Internet-Adressen dienen lediglich der Illustration und erheben keinen Anspruch auf Gültigkeit. Mit einer Ausnahme:

```
http://www.internet-kompetenz.ch/
```

Auf den Web-Seiten unter dieser Adresse werden weiterführende Informationen zum Buch und Linksammlungen zu den verschiedenen Themen angeboten.

Internet contra Alltag

Längst ist das Internet zu einem Teil des Alltags geworden. Wir verschicken E-Mails, benutzen Informationsdienste im WWW und

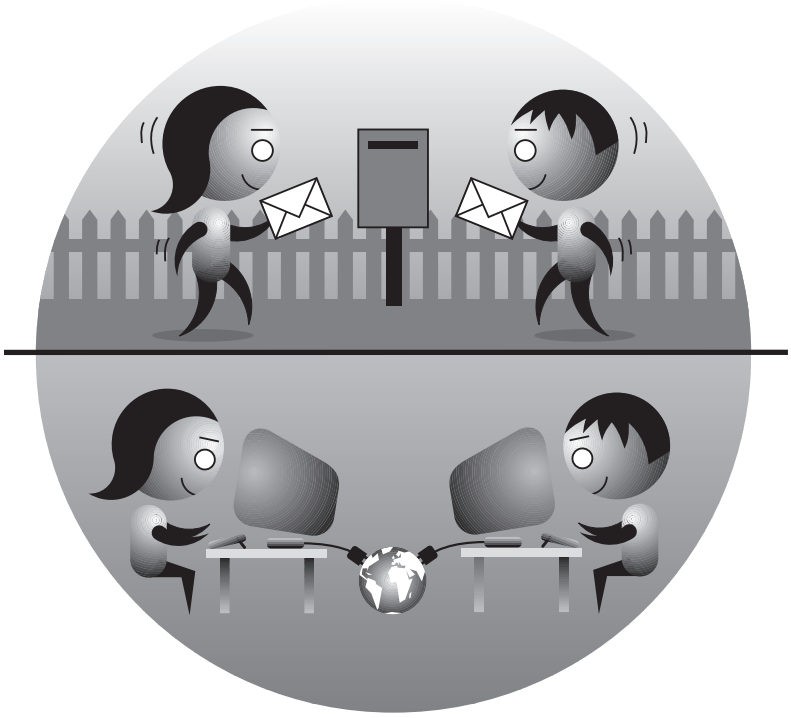
kaufen via Internet ein. Viele dieser Aktivitäten haben wir vor dem digitalen Zeitalter in analoger Weise ohne das Internet erledigt. In diesem Buch knüpfen wir immer wieder an diese «herkömmlichen» Tätigkeiten ohne Benutzung des Internets an. Wenn wir der Einfachheit halber von «Sicherheit im Alltag» und «Sicherheit im Internet» reden, so umfasst «Alltag» diese herkömmlichen Aktivitäten ohne Internet.

Danke schön!

Ein grosses «Dankeschön!» geht an Raimond Reichert und Daniel Frei für die kritischen und wertvollen Kommentare zu diesem Buch.

Kapitel 1

Sicherheit im Alltag – Sicherheit im Internet

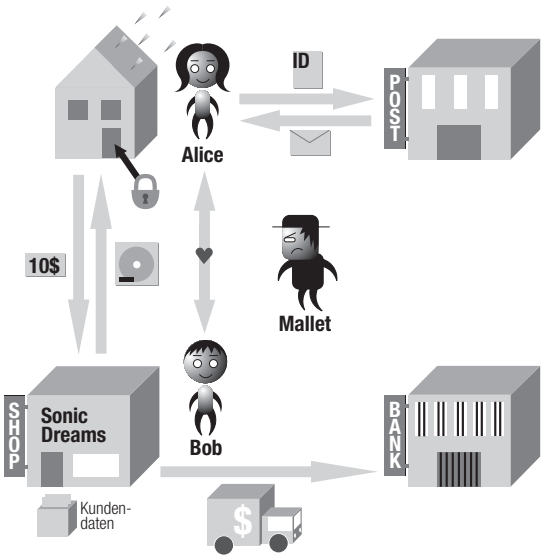


Welche Risiken bestehen bei der Benutzung des Internets? Welche Gefahren lauern in der grossen weiten Welt der Datenströme? Welche Möglichkeiten hat man als Benutzerin, sich zu schützen? Fragen dieser Art beschäftigen uns im Zusammenhang mit Sicherheitsaspekten bei der Internet-Benutzung.

Zuerst überlegen wir uns aber, mit welchen Problemen und Risiken wir im Alltag konfrontiert werden. Oft besteht nämlich kein grosser Unterschied zwischen der Offline- und der Online-Welt.

Sicherheit im Alltag

Im Alltag gibt es verschiedene Anbieter von Dienstleistungen: zum Beispiel eine Bank, einen Plattenladen oder die Post. Alice arbeitet als Journalistin bei der renommierten Zeitung *The Backstreet Journal* und nimmt je nach Bedarf die gewünschten Dienstleistungen in Anspruch.



Am liebsten geht Alice in den Plattenladen *SonicDreams*, denn dort arbeitet Bob. Bob ist der Inhaber dieses Plattenladens.

Alice und Bob sind ineinander verliebt. Aber die Beziehung ist alles andere als einfach. Der Grund heisst Mallet. Mallet ist ein finsterer Geselle, der auf Bob eifersüchtig ist. Er setzt alles daran, unserem Liebespaar das Leben schwer zu machen. Was er unternimmt und wie sich Alice und Bob dagegen schützen können, werden wir in den nächsten Kapiteln sehen.

Zugriffsschutz und Zutrittskontrolle

Alice wohnt in einem Haus, das einerseits Schutz gegen Kälte oder Nässe bietet. Andererseits soll das Haus den teuren Fernseher und die wertvollen Gemälde vor Dieben schützen. Insofern erfüllt das Haus mit seinen Mauern die Funktion *Zugriffsschutz*.

Trotz Zugriffsschutz muss Alice das Haus betreten können. Deshalb gibt es eine Eingangstüre. Das Türschloss übernimmt die *Zutrittskontrolle* zum Haus. Nur wer den Schlüssel besitzt, kann Alices Haus betreten. Alice darf ihren Schlüssel nicht verlieren, sonst erhalten Unbefugte wie Mallet Zugang zum Haus. Sollte Alice ihren Schlüssel dennoch verlieren, lässt sie vorzugsweise die Schlösser auswechseln. Alle Vorsichtsmassnahmen nützen allerdings wenig, wenn ein Brand das Haus zerstört. Von besonders wichtigen Dokumenten bewahrt Alice deshalb immer eine Kopie in ihrem Büro beim *Backstreet Journal* auf.

Auch die Anbieter von Dienstleistungen kümmern sich um Zugriffsschutz und Zutrittskontrolle. In einer Bank zum Beispiel wird die Schalterhalle mit Panzerglas von den Büroräumlichkeiten abgetrennt. Noch besser geschützt ist der Tresorraum. Bei so viel Schutz geht nichts ohne gute Zutrittskontrollen. Berechtigte Personen werden anhand der Kenntnis von Zahlenkombinationen oder anhand des Besitzes der richtigen Schlüssel oder Badges (Personalausweise) identifiziert.

Zahlungsverkehr

Für Alice ist vor allem wichtig, dass die Bank ihr Geld sicher aufbewahrt. Geld dient als allgemein akzeptiertes *Zahlungsmittel*. Alice kann damit zum Beispiel den Plattenladen besuchen und das neus-

te Album ihrer Lieblingsband erstehen. Die Bezahlung funktioniert, weil gesetzlich vorgeschrieben ist, dass der Plattenladen Alices Bargeld akzeptieren muss. Ausserdem gibt es mit der Nationalbank eine dritte, unabhängige Stelle, die für das Geld bürgt und der man allgemein Vertrauen schenkt. Eine Voraussetzung für das Vertrauen ist, dass die Geldnoten nicht leicht fälschbar sind. Das wird durch verschiedene Techniken erreicht: spezielles Papier, Wasserzeichen, Hologramme, besondere Drucktechniken usw. Trotzdem verbleiben zwei Hauptgefahren im Zusammenhang mit Bargeld: Es kann gestohlen und es kann gefälscht werden.

Alice kann ihre Einkäufe auch bargeldlos bezahlen. Dazu benutzt sie eine Kreditkarte. Wiederum bürgt eine dritte Stelle dafür, dass hinter der Kreditkarte ein gültiges Konto steckt. Alice muss aber auf ihre Kreditkarte ähnlich gut aufpassen wie auf Bargeld. Die Kartennummer, der Name der Besitzerin und das Ablaufdatum genügen, um die Kreditkarte zu belasten.

Datenschutz und die Privatsphäre

Als Inhaber des Plattenladens hat Bob ein Interesse daran, möglichst genau herauszufinden, welche Musik bei seinen Kunden am beliebtesten ist. So kann er das Musikangebot oder die Werbung gezielt auf die Bedürfnisse der Kunden auslegen.

Noch besser wäre es, wenn Bob von jedem Kunden einzeln die Vorlieben kennen würde. Das lässt sich mit Hilfe einer Rabattkarte realisieren. Der Kunde erhält ein Kärtchen, mit dessen Hilfe jeder Kauf inklusive Artikelbezeichnung registriert wird. Dadurch entstehen eine komplette Liste mit allen Einkäufen und ein detailliertes Profil der Vorlieben und Interessen des jeweiligen Kunden. Als Gegenleistung wird dem Kunden ein gewisser Rabatt auf seine Einkäufe angeboten. Jeder Kunde muss selber entscheiden, ob ihm die Wahrung seiner Privatsphäre oder der Rabatt wichtiger ist.

Auch für Alice spielt die Privatsphäre eine grosse Rolle. Zum Beispiel wünscht sie nicht, dass alle Welt beobachten kann, was sie in ihren eigenen vier Wänden treibt. Deshalb hat sie Vorhänge vor den Fenstern in ihrem Haus angebracht.

Problematische Inhalte

Alice hat eine 12-jährige Tochter mit dem Namen Virginia. Manchmal macht sich Alice Sorgen, mit welchen Themen ihre Tochter beim Fernsehen, in Zeitschriften oder bei Kinobesuchen konfrontiert wird. Es gibt einige Inhalte, die gemeinhin und unbhängig vom Medium als problematisch eingestuft werden. Häufig geht es um den Schutz von Kindern oder Jugendlichen vor übermässigen Gewaltdarstellungen, Pornografie oder politisch extremen Ansichten.

Problematische Inhalte werden oft entsprechend deklariert. Zum Beispiel kennt man die Altersbegrenzungen von Kinofilmen. Im Plattenladen wird auf den heiklen Alben ein Hinweis wie «Parental Advisory – Explicit Content» angebracht. Und am Kiosk werden die Magazine mit pornografischen Inhalten typischerweise in den obersten Regalen – ausserhalb der Reichweite von Kindern – untergebracht.

Identifikation von Personen

Ab und zu erhält Alice eine eingeschriebene Sendung, deren Empfang sie quittieren muss. Die Post möchte sicherstellen, dass die richtige Person und nicht etwa eine Hochstaplerin den Empfang bestätigt. Das heisst, Alice muss ihre Identität beweisen, indem sie dem Postbeamten ihren Pass oder einen anderen Identitätsausweis zeigt.

Wieso funktioniert ein Pass? Bei einem Pass handelt es sich um ein offizielles Dokument, für das ein Staat bürgt. Der Staat garantiert, dass die Angaben im Pass zutreffen. Ausserdem ist ein Pass relativ fälschungssicher. Die Identität einer Person kann aufgrund von drei Punkten überprüft werden: Erstens, die Person ist im Besitz des Passes. Zweitens, das Foto im Pass stimmt mit dem Aussehen der Person überein. Drittens, die Unterschrift der Person stimmt mit derjenigen im Pass überein.

Ein Pass bietet jedoch keine hundertprozentige Sicherheit. Vielleicht gelingt es jemandem, Alices Pass zu entwenden. Dann muss die Person «lediglich» ihr Aussehen anpassen und die Unterschrift üben, um in Alices Rolle zu schlüpfen.

Identifikation von Firmen und Organisationen

Alice benutzt einen Pass oder einen anderen Ausweis, um ihre Identität zu beweisen. Wie aber identifiziert sich eine Firma? Wie kann Alice sichergehen, dass sie tatsächlich mit der offiziellen Post Geschäfte treibt und nicht mit einer Hochstaplerfirma?

Alice vertraut zum Beispiel auf den Standort des Postbüros. Bei einer allfälligen Reklamation geht sie zum selben Ort zurück und bringt ihre Beschwerde an. Ausserdem ist das Logo der Post so gut bekannt, dass sich Alice auch daran orientieren kann.

Schliesslich zählt Alice auf einen weiteren Punkt: Es wäre schlicht zu aufwendig, eine Hochstaplerfirma aus dem Boden zu stampfen und einige Tage später wieder aufzulösen, nur um einige nichts ahnende Zeitgenossen hintergehen zu können.

Trotz allem – folgendes Szenario könnte funktionieren: Der Bösewicht Mallet bastelt einen Briefkasten im selben Format und in derselben Farbe wie die offiziellen Briefkästen der Post. Er stellt den gefälschten Briefkasten an einem geeigneten Ort auf und wartet ab. Vielleicht bringt er sogar eine Notiz an, die auf die vorbildliche Service-Erweiterung der Post hinweist. Zweifellos könnte er auf diese Weise an einige Briefe gelangen, bevor der Betrug auffliegt.

Geschützte Übermittlung

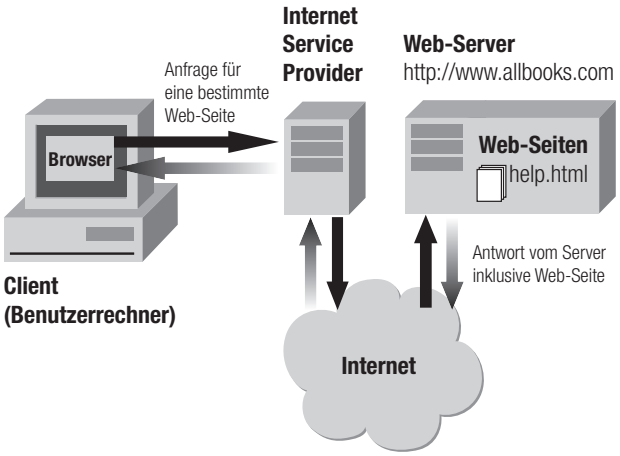
Zurück zu Bob und seinem Plattenladen. Der Feierabend naht, die Tageseinnahmen werden abgerechnet. Das Geld soll zur Bank transportiert werden. Dazu werden die Geldkassetten von Sicherheitsleuten abgeholt und in einem Panzerwagen zur Bank verfrachtet. Der Panzerwagen soll den Schutz des Geldes unterwegs gewährleisten.

Alice möchte manche Briefe an Bob am liebsten ebenfalls per Panzerwagen übermitteln. Alice und Bob verwenden deshalb eine Geheimsprache. Ein Fax an Bob mit zwei Kreisen in der linken oberen Ecke bedeutet: «O.K., ich gehe heute eine Stunde früher aus dem Büro.» Ein einziger Kreis bedeutet: «Sorry, zu viel Arbeit. Wir können uns nicht treffen.» Diese Korrespondenz soll Alices Chef beim *Backstreet Journal* schliesslich nicht mitverfolgen können, ebenso wenig der eifersüchtige Mallet.

Sicherheit im Internet

Die verschiedenen Aspekte bezüglich Sicherheit im Alltagsleben sind hinlänglich bekannt. Im Internet existieren die meisten Probleme ebenfalls und in ähnlicher Weise. Allerdings verschiebt sich die Gewichtung etwas. Manche Probleme sind im Umfeld des Internets relevanter und akuter als andere. Um die Gemeinsamkeiten und Unterschiede zwischen Alltag und Internet besser zu verstehen, fassen wir kurz die wichtigsten Eigenschaften des Internets zusammen:

Das Internet ist ein Zusammenschluss einer unüberschaubaren Menge von Computern. Jeder Rechner im Netz verfügt über eine eindeutige Adresse. Mit Hilfe der Adresse kann ein Rechner mit einem anderen Rechner Kontakt aufnehmen und anschliessend mit ihm kommunizieren.



Man teilt die Computer im Internet üblicherweise in zwei Klassen ein: Die *Server* stellen ein bestimmtes Angebot zur Verfügung. Server sind typischerweise rund um die Uhr am Netz angeschlossen und beantworten Anfragen von Benutzerinnen. Beispiele für Server sind Web-Server, Suchdienste oder News-Server. Die *Clients* (oder *Benutzerrechner*) dagegen bieten in der Regel nichts an, sondern nutzen die Angebote der Server. Insbesondere die privaten Benutzerrechner sind

häufig nicht permanent am Netz angeschlossen, sondern wählen sich nach Bedarf über einen *Internet Service Provider* (kurz: *Internet-Provider*) ein.

Der wohl wichtigste Internet-Dienst neben E-Mail ist das *World Wide Web* oder kurz *WWW*. Für den Zugriff auf das WWW verwendet ein Benutzer einen *Web-Browser*. Der Browser ist ein Werkzeug zur Ansicht von Daten im Internet und speziell im WWW und hat unter anderem die Aufgabe, *Web-Seiten* auf dem Bildschirm darzustellen. Eine Web-Seite besteht aus einem Inhalt (Text, Bilder usw.) sowie Layoutbefehlen. Die Layoutbefehle werden durch eine spezielle Sprache namens *Hypertext Markup Language* oder kurz *HTML* festgelegt.

Web-Seiten liegen bei einem *Web-Server* bereit und werden über eine eindeutige Adresse namens *URL* oder *Uniform Resource Locator* identifiziert. Der URL `http://www.allbooks.com/help.html` beispielsweise verweist auf die Hilfeseite namens `help.html` beim Server `www.allbooks.com`. Der erste Teil des URL bestimmt den Internet-Dienst. Im Beispiel steht `http` für *HTTP* oder *Hypertext Transfer Protocol* und bezeichnet den Dienst zum Bezug von Web-Seiten. Alle zusammengehörenden Web-Seiten auf einem Web-Server bezeichnen wir als eine *Web-Site*. Zum Beispiel besteht die Web-Site von AllBooks aus allen Seiten, die auf dem Server `www.allbooks.com` liegen.

Eigenschaften des Internets

Die folgende Auflistung bietet eine Übersicht über die wichtigsten Aspekte, die ein Computernetzwerk wie das Internet vom übrigen Alltagsleben unterscheiden:

- Eine Eigenheit der Computerwelt ist die Tatsache, dass Information und Informationsträger klar voneinander getrennt sind. Im Alltagsleben ist das unvorstellbar. Beispiel: Ein klassisches Gemälde ist untrennbar mit der Leinwand verbunden, auf der es gemalt ist. Es ist nicht möglich, eine perfekte Kopie eines Ölgemäldes zu erstellen. Ganz anders sieht es in der digitalen Welt aus. Bei einem digitalen Bild steht die Information unabhängig vom Informationsträger zur Verfügung. Es macht keinen Un-

terschied, ob sich die Bilddatei auf einer Floppy-Disk, auf einer Festplatte oder auf einer CD-ROM befindet. Die Information lässt sich beliebig kopieren, wobei ein perfektes Duplikat entsteht, ohne dass irgendwelche Spuren hinterlassen werden.

- Ein Computer im Internet befindet sich in einer sehr exponierten Situation. Grundsätzlich kann jeder Rechner im Internet auf jeden anderen Rechner zugreifen. Alle physischen Barrieren verschwinden. Wenn Mallet beispielsweise von Zürich aus physisch in eine Bank an der Wallstreet in New York City einbrechen möchte, muss er immerhin zuerst in die USA fliegen. Im Internet hingegen genügt es, wenn er sich mit seinem Rechner in Zürich ins Internet einwählt und anschliessend in die Server der Bank einzubrechen versucht.

- Ein grosses Problem im Internet ist das Vertrauen. Wenn wir im Alltag eine Person zum ersten Mal treffen, bilden wir uns ein Urteil, indem wir verschiedene Aspekte berücksichtigen: Aussehen, Kleidung, Hygiene, Wortwahl, Gestik, Mimik usw. Jede Beurteilung aufgrund dieser Eigenschaften ist von Vorurteilen geprägt. Trotzdem handelt es sich um nützliche Anhaltspunkte. Im Internet dagegen fallen diese begleitenden Anhaltspunkte weg. Man kennt oft nur eine E-Mail-Adresse, der direkte Kontakt mit der Person entfällt. Zudem vergrössert sich im Internet der Personenkreis, mit dem man konfrontiert wird.

- Computer sind schnell und geduldig – derselbe Arbeitsschritt kann problemlos millionenfach ausgeführt werden. Von der Automatisierbarkeit von Arbeitsschritten kann ein Hacker profitieren, um per Internet in einen Computer einzubrechen. Zum Beispiel können mittels geeigneter Programme ganze Wörterbücher ausprobiert werden, um ein Passwort zu knacken. Schlimmer noch: Der Hacker kann sein Programm veröffentlichen. In der Folge sind auch weniger versierte Anwender in der Lage, das Hacker-Programm herunterzuladen, auszuführen und unter Umständen grossen Schaden anzurichten.

- Die Internet-Infrastruktur wurde ursprünglich nicht auf Sicherheit ausgelegt, sondern auf möglichst hohe Robustheit und Ausfallsicherheit. Deshalb bietet das Internet viele Angriffspunkte und sicherheitsrelevante Schwachstellen. Diese Schwachstellen werden zwar allmählich ausgebessert, doch der Übergang zu sichereren Technologien ist langwierig.

Alice, Bob und Mallet im Internet

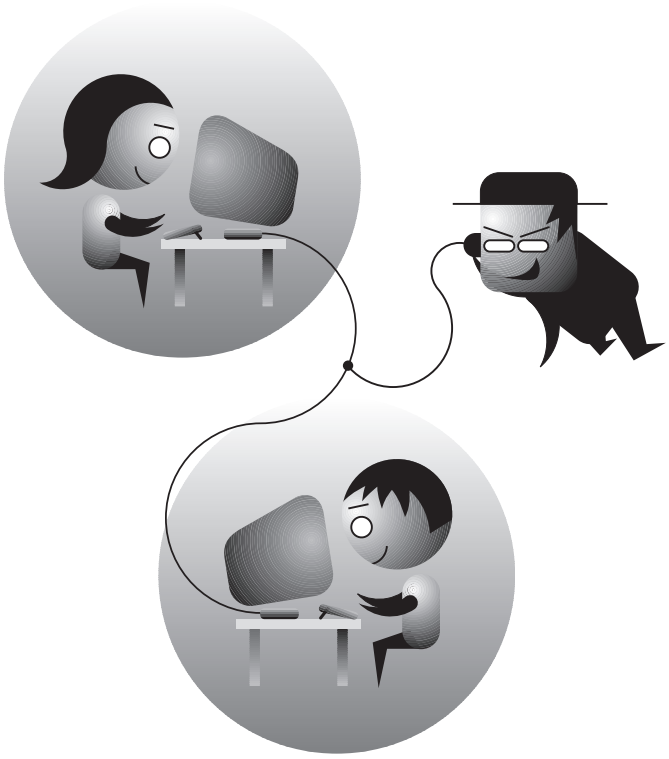
In der Redaktion des *Backstreet Journals* wird regelmässig im Internet recherchiert. Alle Journalistinnen verfügen über einen eigenen Rechner inklusive Internet-Zugang. Alice kann aber auch von zu Hause über ihren privaten Internet-Provider *WonderSurf* das Internet benützen. E-Mail empfängt sie unter der Adresse `alice@wondersurf.com`. Alices Tochter Virginia weiss das Internet als Informationslieferanten für die Hausaufgaben und als Unterhaltungsmedium für die Freizeit zu nutzen.

Bob hat für seinen Plattenladen eine eigene Web-Site unter der Adresse `www.sonicdreams.com` aufgesetzt. Bobs E-Mail-Adresse lautet `bob@sonicdreams.com`. Er bietet seine CDs auch online an. Bestellungen können direkt über die Web-Site von SonicDreams getätigt und per Kreditkarte bezahlt werden.

Was Alice und Bob können, kann Mallet schon lange. Er kennt sich im Internet bestens aus und schreckt nicht davor zurück, die neuen Technologien für seine düsteren Machenschaften auszunützen. Die folgenden Kapitel zeigen, welche konkreten Möglichkeiten Mallet hat und wie sich Alice und Bob gegen die potenziellen Gefahren schützen können.

Kapitel 2

Sicher kommunizieren via Internet



Alice und Bob schreiben sich häufig E-Mails, auch während der Arbeitszeit. Für Bob ist das kein Problem; er ist sein eigener Herr und Meister. Alice hingegen ist es nicht immer wohl bei der Sache. Nicht alles, was sie Bob schreibt, ist für andere Augen gedacht. Wie kann Alice sicherstellen, dass ihr E-Mail-Verkehr nicht vom *Backstreet Journal* oder gar von Mallet «abgehört» wird? Gerade diese Woche hat Alice zudem eine brisante Mail erhalten. Das Konkurrenzblatt *Evening Moon* hat angefragt, ob Alice nicht die Stelle wechseln wolle. Davon soll das *Backstreet Journal* vorderhand natürlich nichts erfahren.

Alice ist eine Vielleserin. Regelmässig bestellt sie Bücher bei `www.allbooks.com` und bezahlt die Bücher mit ihrer Kreditkarte. Das ist einfach, sie muss lediglich die Kreditkartenangaben im entsprechenden Feld des Online-Bestellformulars eintragen. Doch wer garantiert Alice, dass Mallet die Informationen nicht abfängt und missbraucht? Gibt es Vorsichtsmassnahmen, die Alice treffen kann?

Bei ihrer täglichen Arbeit greift Alice via WWW oft auf kostenpflichtige Datenbanken zu. Dazu benötigt Alice ein Passwort, das sie auf den Einstiegsseiten der betreffenden Datenbanken eingibt. Damit Alice sich nicht Dutzende von Passwörtern merken muss, verwendet sie immer das gleiche: `iLoveBob`. Dasselbe Passwort benutzt Alice auch für den Zugang zu ihrem eigenen Rechner. Kann Mallet ihr Passwort wohl im Internet abfangen? Was kann Alice dagegen unternehmen?

Verschlüsseln von Informationen

Alice möchte Bob eine wichtige und geheime Nachricht zustellen. Alice kann die Nachricht auf verschiedene Arten verschicken; zum Beispiel ganz altertümlich per Pferdekurier oder ganz modern via E-Mail. Meistens stellt sich dasselbe Problem: Die Nachricht kann unterwegs durch Unberechtigte abgefangen und gelesen werden. In unserem Beispiel übernimmt Mallet die Rolle des «bösen Spions».

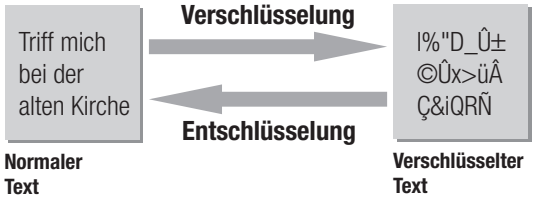
Durch das Verschlüsseln der Nachricht soll Mallet ein Schnippchen geschlagen werden. Mit *Verschlüsselung* (Englisch: *Encryption*) bezeichnen wir die Übersetzung von Text (oder anderen Daten) in einen geheimen Code. Der Text wird für Dritte unleserlich und damit unbrauchbar gemacht. Zum Beispiel würde Alice anstelle der lesbaren Botschaft *(Klartext)*

```
Triff mich bei der alten Kirche
```

den Buchstabensalat *(Schlüsseltext)*

```
|%"D_Û±©Û÷x>üÂ‘ÃÇ&iQRÑ;δr¬βÏFHü©&øègWéÕè}çgê?~
```

an Bob schicken. Für Mallet ist nicht ersichtlich, was der ursprüngliche Text war. Bob hingegen muss in der Lage sein, den Buchstabensalat wieder in die ursprüngliche Form zu bringen. Er muss also den Vorgang der Verschlüsselung rückgängig machen können. Dieser Umkehrvorgang wird *Entschlüsselung* (Englisch: *Decryption*) genannt. Für die Ver- und Entschlüsselung von Daten wird eine Zusatzinformation benötigt. Diese Zusatzinformation nennen wir einen *Schlüssel*.



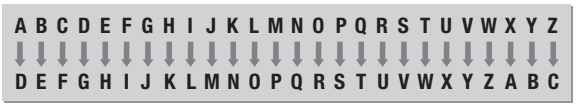
Es gibt verschiedene Arten von Verschlüsselungsverfahren. Wir werden im Folgenden zwei Klassen von Verfahren betrachten.

Symmetrische Verschlüsselungsverfahren

Eine sehr alte Verschlüsselungsmethode ist CAESAR. Man sagt, der berühmte römische Feldherr habe dieses Verfahren angewendet. Es handelt sich um eine sehr simple Verschlüsselung.

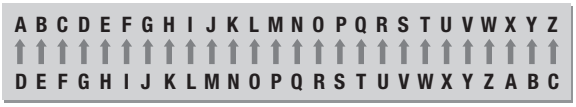
Bei CAESAR wird jeder Buchstabe des Alphabets durch einen anderen ersetzt. Den neuen Buchstaben erhält man, indem man vom alten Buchstaben um eine bestimmte Anzahl Schritte im Alphabet weiterrückt. Am Ende des Alphabets wird zyklisch wieder beim Anfang begonnen. Das CAESAR-Verfahren wird folglich durch eine einzige Grösse festgelegt: Die Anzahl der Schritte, welche die Buchstaben voneinander trennt. Diese Schrittzahl ist der *geheime Schlüssel* beim CAESAR-Verfahren.

Man kann sich je nach Schrittzahl eine «Umrechnungsschablone» zusammenstellen. Das folgende Beispiel verschiebt um drei Positionen:



Die obere Zeile zeigt das alte, normale Alphabet. Die untere Zeile stellt das neue, verschobene Alphabet dar. Die Schablone wird zur Verschlüsselung von Texten verwendet. Zum Beispiel wird die kurze Nachricht `Triff mich bei der alten Kirche` verschlüsselt zu `Wulii plfk ehl ghu dowhq Nlufkh`. Den auf diese Weise verschlüsselten Text schickt Alice an Bob.

Bob entschlüsselt den Text nach derselben Methode – nur eben umgekehrt. Jeder Buchstabe wird durch den um drei Positionen weiter vorne liegenden ersetzt. Die Schablone zur Entschlüsselung sieht gleich aus wie oben. Lediglich die Richtung der Pfeile ändert:

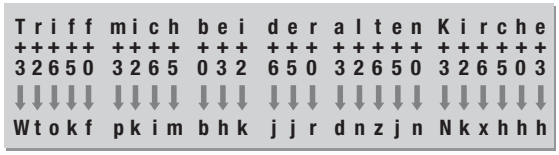


Bei CAESAR wird zum Ver- und Entschlüsseln derselbe Schlüssel benutzt. Im Beispiel ist der Schlüssel die Schrittzahl 3. Alle Verschlüsselungsverfahren mit dieser Eigenschaft – gleicher Schlüssel für die Ver- und Entschlüsselung – gehören zu den so genannten *symmetrischen Verschlüsselungsverfahren.*

Wichtig ist die Schlüssellänge

Alice schickt eine CAESAR-verschlüsselte E-Mail an Bob. Was muss Mallet tun, damit er die Nachricht entschlüsseln kann? (1) Er muss die Nachricht abfangen können. (2) Er muss herausfinden, dass Alice das CAESAR-Verfahren zur Verschlüsselung benutzt. (3) Nun versucht er, die verschlüsselte Nachricht mit den 26 möglichen Schlüsseln – den Schrittzahlen von 1 bis 26 – zu entschlüsseln. Mallet hat ein Programm geschrieben, das die Schlüssel automatisch durchprobiert. Mit Hilfe eines Computers ist es eine Sache von Sekundenbruchteilen, den richtigen Schlüssel bei CAESAR herauszufinden.

Folglich müssen längere Schlüssel verwendet werden. Beispielsweise könnten Alice und Bob die fünfstellige Zahl 32650 als Schlüssel verwenden. Die erste Ziffer 3 bedeutet, dass in der Nachricht der erste, sechste, elfte usw. Buchstabe jeweils um 3 Buchstaben verschoben wird. Die zweite Ziffer 2 verschiebt analog den zweiten, siebten, zwölften usw. Buchstaben der Nachricht um 2 Buchstaben. Die Nachricht `Triff mich bei der alten Kirche` wird verschlüsselt zu `Wtokf pkim bhk jjr dnzjn Nkxhhh`:



Der fünfstellige Schlüssel macht die Sache für Mallet um einiges schwieriger. Um eine abgefangene Nachricht zu entschlüsseln, muss er alle Schlüsselzahlen von 00001 bis 99999 durchprobieren.

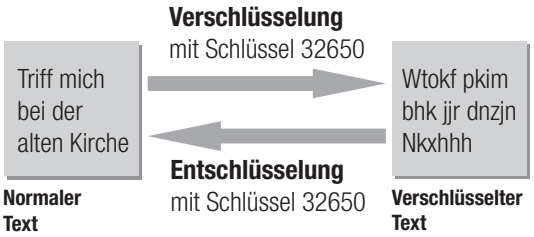
Alice und Bob können die Schlüssellänge grundsätzlich beliebig vergrössern. Sie haben eine 100-stellige Zahl als Schlüssel vereinbart:

7945626724672. . . 11311005151016398. Unter diesen Voraussetzungen dauert es selbst Mallet zu lange, alle Möglichkeiten durchzuspielen.

Die in der Praxis eingesetzten Verschlüsselungsverfahren arbeiten komplexer als CAESAR. Die grundlegenden Eigenschaften jedoch sind identisch. Beispiele bekannter Verschlüsselungsverfahren sind der *Data Encryption Standard (DES)*, der *International Data Encryption Algorithm (IDEA)* sowie die Verfahren *RC2*, *RC4* und *RC5*. Diese Methoden arbeiten zum Beispiel mit Schlüssellängen von 40 oder 128 Bit. Das entspricht 1 099 511 627 776 beziehungsweise 340 282 366 920 938 463 463 374 607 431 768 211 456 unterschiedlichen Schlüsseln.

Schwachstelle symmetrischer Verschlüsselungsmethoden

Alle symmetrischen Verschlüsselungsverfahren weisen einen wichtigen Nachteil auf: Zum Verschlüsseln und Entschlüsseln muss derselbe Schlüssel verwendet werden. Daher stammt die Bezeichnung *symmetrische Verschlüsselungsverfahren*. Ein anderer passender Name ist *Private-Key-Verfahren*, weil der Schlüssel unbedingt geheim gehalten werden muss.



Bevor Alice und Bob verschlüsselte Nachrichten austauschen können, müssen sie sich auf einen gemeinsamen geheimen Schlüssel einigen. Das machen sie bei einem persönlichen Treffen, damit Mallet den Schlüssel nicht erfährt.

Ein wesentlicher Aspekt des Internets ist aber die globale Kommunikation über grosse Distanzen. Ein persönliches Treffen ist häufig undenkbar. Der geheime Schlüssel für ein symmetrisches Verschlüsselungsverfahren darf auch nicht via E-Mail ausgetauscht werden, weil

die Gefahr des «Abhörens» besteht. Es ist ein Verfahren gefragt, mit dem ein Schlüssel gefahrlos bekannt gegeben werden kann. Bob hat sich etwas Raffiniertes ausgedacht ...

Public-Key-Verschlüsselungsverfahren

In seinem Plattenladen bietet Bob über 350 000 verschiedene Platten an. Die Platten sind in einer Datenbank auf Bobs Computer mit Titel, Interpret, Erscheinungsjahr und einer eigenen, achtstelligen Artikelnummer erfasst.

Titel	Interpret	Jahr	Nummer
Tales from the Punchbowl	Primus	1995	177.34.222
An Ordinary Life	Anne Clark	1986	873.12.003
Tubercul'House	Apparatus	1998	112.75.775
Incidental Seductions	Percy Howard	1999	050.11.933
Still	Tanith	1999	350.38.445
Recycling	Suchas	1993	112.13.622
The Edges of Twilight	The Tea Party	1995	543.99.814
...	...	...	...

Verschlüsseln mittels Public Key

Per Mausklick lässt Bob das Plattenverzeichnis nach Titeln alphabetisch ordnen. Ausserdem entfernt er alle Angaben ausser Titel und Artikelnummer. Ein Ausschnitt aus der neu entstandenen Tabelle sieht wie folgt aus:

Titel	Nummer
An Ordinary Life	873.12.003
Incidental Seductions	050.11.933
Recycling	112.13.622
Still	350.38.445
Tales from the Punchbowl	177.34.222
The Edges of Twilight	543.99.814
Tubercul'House	112.75.775

Bob druckt das neue Verzeichnis aus und schickt es an Alice. Er könnte sogar eine Kopie an Mallet schicken oder im *Backstreet Journal* veröffentlichen. Die Liste ist nämlich sein *öffentlicher Schlüssel*, der so genannte *Public Key*.

Alice benutzt den Public Key zur Verschlüsselung von Nachrichten an Bob. Für jeden Buchstaben wählt sie einen Titel mit passendem Anfangsbuchstaben aus dem Verzeichnis und ersetzt den Buchstaben durch die entsprechende Artikelnummer. Aus der Nachricht `Triff mich bei der alten Kirche` entsteht so die Zahlenfolge 17734222/11213622/05011933/... Dabei ist 17734222 die Artikelnummer der Platte namens «Tales from the Punchbowl» von Primus, 11213622 die Nummer von «Recycling» usw.

Die verschlüsselte Botschaft schickt Alice an Bob. Mallet weiss genau, wie der Text verschlüsselt wurde. Er kennt sogar den Schlüssel, die alphabetisch nach Titeln geordnete Liste. Trotzdem kann Mallet die Botschaft nicht innert nützlicher Frist entschlüsseln. Dazu müsste er jede Artikelnummer in der Liste nachschauen. Bei über 350 000 Einträgen dauert das zu lange.

Mallet könnte das nach Titeln geordnete Plattenverzeichnis zuerst elektronisch erfassen. Dann würde ihm der Computer das Nachschauen der einzelnen Artikelnummern abnehmen. Doch auch das elektronische Erfassen von 350 000 Titeln bedeutet einen zu grossen Aufwand. Kurz: Theoretisch könnte Mallet die Nachricht von Alice an Bob entschlüsseln. In der Praxis ist der Aufwand dafür allerdings zu gross, und er wird es bleiben lassen.

Entschlüsseln mittels Private Key

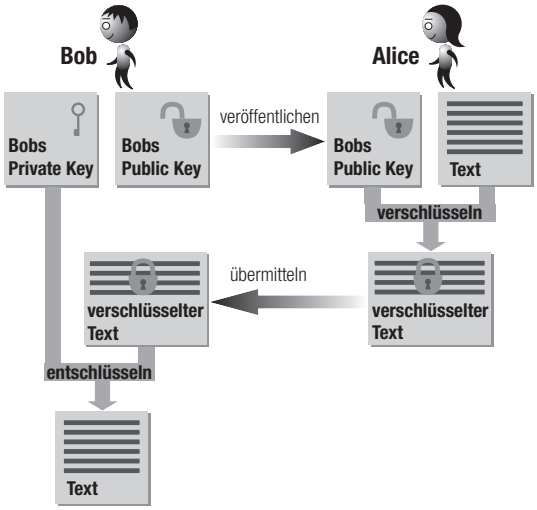
Im Unterschied zu Mallet fällt es Bob leicht, die von Alice verschlüsselte Nachricht zu entschlüsseln. Nur Bob besitzt das Plattenverzeichnis in elektronischer Form. Problemlos kann er das Verzeichnis nach Artikelnummern ordnen lassen. Auf diese Weise entsteht ein zweiter, geheimer Schlüssel, der so genannte *Private Key*. Mit dem neu entstandenen Spezialverzeichnis entschlüsselt Bob verschlüsselte Texte innert kürzester Zeit.

Nummer	Titel
050.11.933	Incidental Seductions
112.13.622	Recycling
112.75.775	Tubercul'House
177.34.222	Tales from the Punchbowl
350.38.445	Still
543.99.814	The Edges of Twilight
873.12.003	An Ordinary Life

Im Gegensatz zum Public Key, den Alice zum Verschlüsseln benutzt, muss Bob den Private Key unbedingt geheim halten. Die Sicherheit der Verschlüsselungsmethode hängt entscheidend von der Geheimhaltung des Private Keys ab.

Eine Frage ist noch ungeklärt: Wie funktioniert es in die Gegenrichtung? Wie verschlüsselt Bob Nachrichten, die er an Alice schickt? Er benutzt dieselbe Methode mit einem anderen Schlüssel.

Dazu muss Alice ihr eigenes Schlüsselpaar, bestehend aus Public und Private Key, erstellen. Sie beschafft sich beim *Backstreet Journal* die Liste aller 720 000 Abonnenten. Jeder Abonnent verfügt über eine Kundennummer. Mit wenig Aufwand erstellt Alice eine Liste mit Vornamen und zugehörigen Kundennummern – nach Vornamen alphabetisch geordnet. Die Liste sendet sie als Public Key an Bob (wobei wir hier den Aspekt des Datenschutzes ignorieren). Der Private Key entsteht analog, indem sie für sich die Abonnentenliste nach Kundennummern ordnet. Auch hier gehen wir davon aus, dass niemand ausser Alice die Liste in elektronischer Form besitzt und mit geringem Aufwand nach Kundennummern ordnen kann.



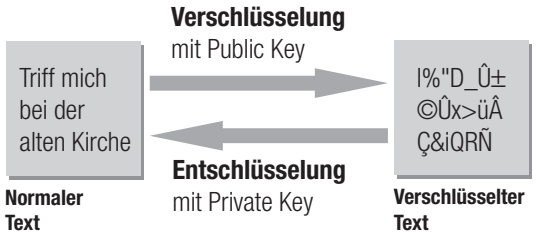
In der Praxis werden selbstverständlich keine Platten- oder Kundenverzeichnisse verwendet. Das Prinzip bleibt jedoch dasselbe und sieht

beispielsweise wie folgt aus: Aus zwei grossen Primzahlen wird das Produkt gebildet. Dadurch entsteht eine Zahl wie 21 290 246 318 258 757 547 497 882 016 271 517 497 806 703 963 277 216 278 233 383 215 381 949 984 056 495 911 366 573 853 021 918 316 783 107 387 995 317 230 889 569 230 873 441 936 471. Diese Ziffernfolge bildet die Grundlage für den Public Key und wird zum Verschlüsseln von Nachrichten verwendet. Um verschlüsselte Nachrichten in vernünftiger Zeit zu entschlüsseln, muss man solche Zahlen in Primfaktoren zerlegen können. Theoretisch ist das kein Problem, nur braucht man dafür selbst mit Computerhilfe sehr viel Zeit. Kennt man hingegen als Zusatzinformation die Primfaktorzerlegung, ist die Entschlüsselung ohne Weiteres möglich. Diese Zusatzinformation liegt in Form des Private Keys vor.

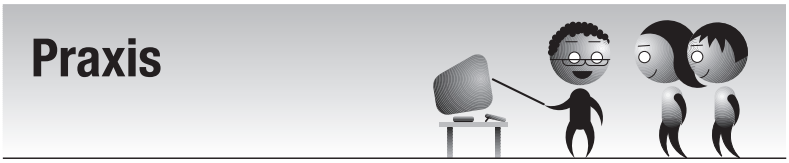
Als Benutzer braucht man glücklicherweise nicht selber mit Primzahlen oder Faktorzerlegungen zu hantieren. Die komplizierte Mathematik wird von geeigneten Programmen übernommen. Viele Programme implementieren eines der bekanntesten Public-Key-Verfahren namens *RSA,* benannt nach den Erfindern Rivest, Shamir und Adleman.

Eigenschaften von Public-Key-Verfahren

Fassen wir zusammen: Public-Key-Verfahren arbeiten mit zwei unterschiedlichen Schlüsseln, dem Public Key und dem Private Key. Der Public Key ist öffentlich zugänglich. Er muss nicht geheim bleiben. Im Gegenteil: Möglichst viele Leute sollen den Public Key kennen, damit sie vertrauliche Informationen verschlüsseln können. Eine verschlüsselte Nachricht kann nur mit dem Private Key entschlüsselt werden. Der Private Key muss unbedingt geheim bleiben.



Die beiden Schlüssel bilden ein festes Paar. Der Private Key ist das Gegenstück zum Public Key und umgekehrt. Was der Public Key verschlüsselt, kann nur mit dem passenden Private Key wieder entschlüsselt werden. Trotz dieser Verflechtung der beiden Schlüssel ist es praktisch unmöglich, den Private Key aus dem Public Key herzuleiten.



Der Schlüssel – je länger, desto sicherer

Sowohl bei den symmetrischen als auch bei den Public-Key-Verfahren ist für die Sicherheit des Verfahrens die Länge der Schlüssel von Bedeutung. Je kürzer ein Schlüssel ist, desto leichter lässt er sich erraten. Genauso verhält es sich beim Kombinationsschloss für ein Fahrrad: Bei drei Ziffern müssen gerade mal tausend Kombinationen durchprobiert werden. Bei sechs Ziffern erhöht sich die Zahl der möglichen Kombinationen auf eine Million. Je mehr Ziffern ein Fahrradschloss benutzt, desto schwieriger ist es, die richtige Kombination zu finden.

In der *Kryptografie* – der Wissenschaft, die sich mit der Verschlüsselung von Daten auseinander setzt – misst man die Länge eines Schlüssels in Bits, der kleinsten Informationseinheit im Computer. Viele Verschlüsselungsprogramme können einen Schlüssel in «menschenlesbarer» Form als Folge von Buchstaben ausgeben. Auf diese Weise können Schlüssel ausgetauscht werden.

```
-----BEGIN PUBLIC KEY BLOCK-----
mQCNAzegTiQAAAEEAM22cjv4lyzzc5FG6T7XPkNgjpEu0h69ki80c7u5nJ2u+pO/
gZexdi54IWtm/SYLuAYZr++5T7xFyPEJznBTnWJQ1omdzr/tT8BuHOP16roG0S3x
pGI6k7DQrDFzOC0Ct8iSi85qn/Nxt6Umc7HYC1IPNdw20fuiQehcKS362bJNAAUR
fb7R8mQQD3hhwJmf2WGAFD4pLbXA0J8NwXmxEMS6+iPSOPqHtQ==mc7HYC1IPNdw
=qHHT
-----END PUBLIC KEY BLOCK-----
```

Ein Schlüssel muss eine gewisse Mindestlänge aufweisen, um als sicher zu gelten. Diese Mindestlänge ist nicht fix. Die Schlüssel werden ständig länger, um den Sicherheitsanforderungen zu genügen. Computersysteme werden leistungsfähiger und sind dadurch besser in der Lage, einen Schlüssel zu erraten. Deshalb kann man nicht sagen, ein Schlüssel mit einer bestimmten Länge sei auch in Zukunft sicher.

Die Schlüssellänge hängt zudem vom verwendeten Algorithmus ab. Wenn zwei unterschiedliche Verschlüsselungsverfahren – zum Beispiel DES und RSA – dieselbe Schlüssellänge verwenden, heisst das nicht, dass die beiden dieselbe Sicherheit bieten.

Natürlich hängt die nötige Schlüssellänge von den Ansprüchen an die Geheimhaltung ab. Wer seine privaten E-Mails vor den Augen Dritter schützen will, wird sich mit einem kürzeren Schlüssel zufrieden geben. Eine Firma hingegen, die sich gegen Industriespionage schützen möchte, verwendet lange Schlüssel.

Pretty Good Privacy

Eines der ältesten weit verbreiteten Werkzeuge zum Verschlüsseln von Daten heisst *PGP – Pretty Good Privacy*. PGP lässt sich gratis aus dem Internet beziehen und auf dem eigenen Rechner einsetzen. Das Programm arbeitet nach dem Prinzip der Public-Key-Verfahren. Die Benutzerin kann Public und Private Keys erzeugen und Dateien ver- oder entschlüsseln.

PGP eignet sich für sämtliche Aufgaben im Zusammenhang mit dem Verschlüsseln von Daten, insbesondere auch für die Verschlüsselung von E-Mails. Allerdings handelt es sich um ein eigenständiges Programm. Das heisst, als Benutzerin muss man die gewünschten Funktionen sozusagen «von Hand» durchführen. Für die meisten Benutzer ist das zu mühsam. Deshalb gehen viele Anwendungen dazu über, den Benutzern das Leben zu erleichtern, indem sie die Daten selber verschlüsseln und entschlüsseln.

Über viele Jahre war es Softwareherstellern in den USA verboten, Verschlüsselungssoftware mit langen Schlüsseln ins Ausland zu exportieren. Die US-Regierung befürchtete, dass Kryptografieprogramme in die Hände Krimineller geraten könnten. PGP jedoch wurde auch

von Firmen ausserhalb der USA vertrieben und bot lange Schlüssel an. Dieser Umstand trug zur grossen Verbreitung von PGP bei. 1999 haben die USA die Exportrestriktionen für Verschlüsselungssoftware stark gelockert. PGP dürfte deshalb an Bedeutung verlieren.

Verschlüsselung im World Wide Web

Alice bestellt bei `www.allbooks.com` ein Buch und möchte es mit ihrer Kreditkarte bezahlen. Um die Vertraulichkeit der Informationen zu gewährleisten, wird mit Verschlüsselung gearbeitet. Bevor Alices Browser die heiklen Kreditkartenangaben an den Server `www.allbooks.com` schickt, werden die Informationen verschlüsselt. Die meisten aktuellen Web-Browser und viele der Web-Server im Internet bieten die Möglichkeit zum Verschlüsseln der zu übertragenden Daten an.

Alice kann üblicherweise an zwei Merkmalen erkennen, dass der Datentransport verschlüsselt erfolgt:

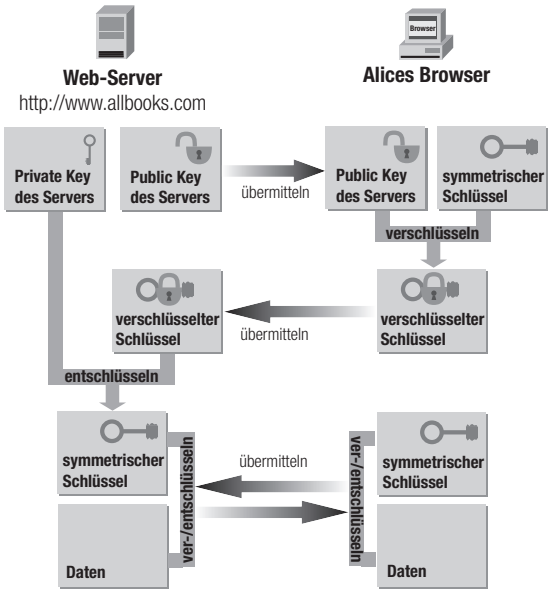
- Im Rand des Browser-Fensters wird zum Beispiel bei Netscapes Navigator ein geschlossenes Schnappschloss angezeigt. Bei unverschlüsselter Übertragung ist das Schloss geöffnet.
- Die aktuelle Adresse im Adressfeld des Browsers beginnt nicht mehr mit `http://` sondern mit `https://`. *HTTP (Hypertext Transfer Protocol)* ist der Name des Internet-Dienstes, mit dem Web-Seiten bezogen werden. *HTTPS* ist die sichere Variante von HTTP.

Für den gesicherten Transport von Daten zwischen Web-Browser und Web-Server wird meistens eine von Netscape Inc. entwickelte Technik namens *SSL (Secure Sockets Layer)* verwendet. Nach der Einführung durch Netscape wurde SSL weiterentwickelt und hat den Sprung zum offiziellen Internet-Standard unter dem Namen *TLS (Transport Layer Security)* geschafft.

Funktionsweise von SSL und TLS

Schauen wir uns etwas genauer an, wie Web-Server und Web-Browser Daten verschlüsselt übertragen können. Zum Verschlüsseln braucht es einen Schlüssel. Woher kennen Browser und Server den Schlüssel? Die Antwort: Sie teilen sich gegenseitig den Schlüssel mit. Bei den Public-Key-Verschlüsselungsverfahren kann man einen Public Key gefahrlos veröffentlichen. Nur der Private Key muss geheim bleiben.

Aber die Public-Key-Verfahren weisen einen grossen Nachteil auf: Sie benötigen viel Zeit, um Daten zu verschlüsseln. Symmetrische Verfahren dagegen arbeiten schneller. Deshalb werden bei SSL/TLS die beiden Klassen von Verschlüsselungsverfahren kombiniert. Unter Verwendung eines Public-Key-Verfahrens einigen sich Web-Browser und Web-Server auf einen gemeinsamen Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Anschliessend werden die eigentlichen Daten – zum Beispiel eine Web-Seite – mit Hilfe des symmetrischen Verfahrens verschlüsselt. Die folgende Grafik zeigt den vereinfachten Ablauf am konkreten Beispiel von Alices Browser und dem Web-Server `www.allbooks.com`.



Zuerst präsentiert der Web-Server dem Browser seine «Visitenkarte». Auf der Visitenkarte stehen einige Angaben zum Server, zum Beispiel der Name `www.allbooks.com` sowie der Public Key des Servers. Die Übertragung dieser Informationen erfolgt unverschlüsselt.

Der Browser empfängt die Visitenkarte des Servers und überprüft anhand des Namens, ob es sich um den richtigen Server handelt. Anschliessend generiert der Browser einen beliebigen Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Der symmetrische Schlüssel soll später zum Verschlüsseln aller Daten zwischen Server und Browser dienen und muss deshalb unbedingt geheim bleiben. Also benutzt der Browser den Public Key des Servers und verschlüsselt damit den symmetrischen Schlüssel. Dann schickt er den verschlüsselten, symmetrischen Schlüssel dem Server.

Der Server nimmt den verschlüsselten Schlüssel vom Browser in Empfang und entschlüsselt ihn. Dazu benutzt er seinen Private Key – das Gegenstück zum Public Key, den der Browser zum Verschlüsseln benutzt hat.

Ab sofort kennen damit beide Seiten – Browser und Server – denselben geheimen Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Diesen Schlüssel benutzen sie fortan, um alle zu übertragenden Daten zu verschlüsseln und nach der Übertragung zu entschlüsseln.

Wichtig dabei ist: Die Benutzerin bemerkt von diesem Hin und Her nichts. Die im Browser enthaltene Software erledigt die Verschlüsselung hinter den Kulissen. Sobald mit Verschlüsselung gearbeitet wird, erfährt das die Benutzerin – zum Beispiel anhand des Schnappschloss-Icons in Netscapes Navigator.

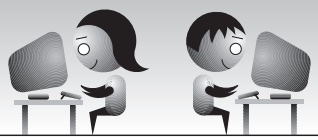
Verschlüsselung von E-Mails

Die verschlüsselte Übertragung von Web-Seiten stellt für Alice kein Problem dar. Der Austausch der benötigten Schlüssel erfolgt automatisch dann, wenn Alice eine Web-Seite zum Beispiel via SSL beziehen möchte.

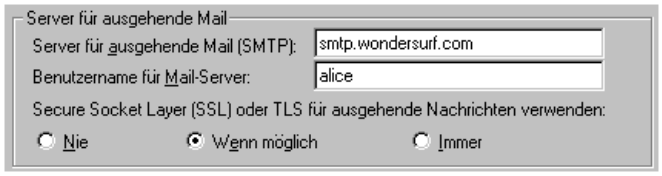
Anders sieht es beim Verschlüsseln von E-Mails aus. Wenn Alice eine E-Mail an Bob schreibt, besteht keine direkte Verbindung

zwischen den beiden Rechnern. Folglich müssen sich Bob und Alice zunächst den jeweiligen Public Key besorgen, bevor sie E-Mails verschlüsseln können. Das bedeutet für die beiden einen Mehraufwand gegenüber der verschlüsselten Übermittlung von Web-Seiten.

Anwendung



Alice und Bob schreiben sich regelmässig E-Mails. Meistens benutzt Alice dafür den Computer in ihrem Büro beim *Backstreet Journal*. Sie hatte dabei immer ein ungutes Gefühl: Können die Administratoren beim *Backstreet Journal* ihre Nachrichten an Bob abfangen? In den Einstellungen ihres Mail-Programms hat Alice entdeckt, dass sie für die Datenübermittlung den Verschlüsselungsstandard SSL oder TLS verwenden kann.

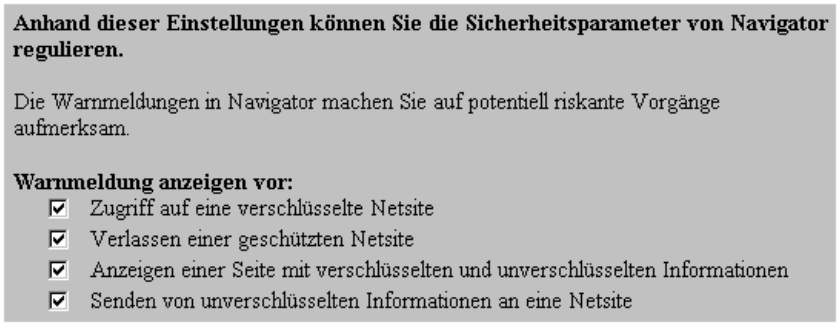


Leider ist damit nur ein Teil des Problems gelöst. Mit dieser Einstellung ist lediglich die Verbindung von Alices Computer bis zum Mail-Server, der die E-Mails entgegennimmt, geschützt. Der Transport der E-Mails durch den Rest des Internets findet meistens unverschlüsselt statt. Alice fragt sich, ob das auch anders geht ...

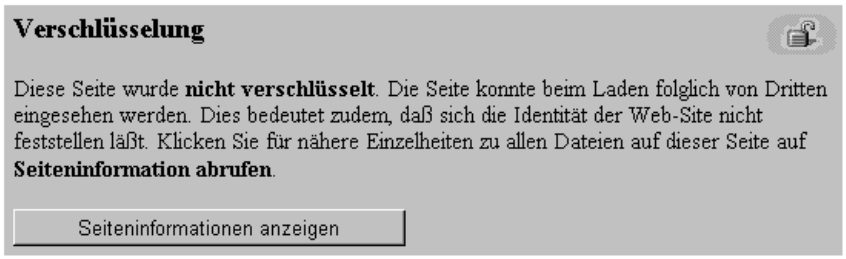
Vor der Übermittlung von Kreditkarteninformationen oder Passwörtern an einen Web-Server achtet Alice darauf, dass die Daten über eine sichere Verbindung übertragen werden. Sie erkennt den Einsatz von SSL beziehungsweise TLS am Bild eines intakten Schlüssels oder eines zugeschnappten Vorhängeschlosses im Browser-Rand.

Bei manchen Web-Servern kann Alice die Verschlüsselung manuell erzwingen, indem sie den Anfang der angezeigten Adresse im Browser von `http://` zu `https://` erweitert.

Alice kann in ihrem Browser verschiedene Sicherheitseinstellungen vornehmen. Zum Beispiel kann sie sich vor dem «Betreten» oder dem «Verlassen» von verschlüsselten Web-Seiten warnen lassen. Auf diese Weise braucht sie nicht ständig auf den Zustand des Schnappschlosses oder des Schlüssel-Icons zu achten. Zudem hat Alice festgelegt, dass sie vor dem Versenden von unverschlüsselten Informationen an einen Web-Server gewarnt wird.

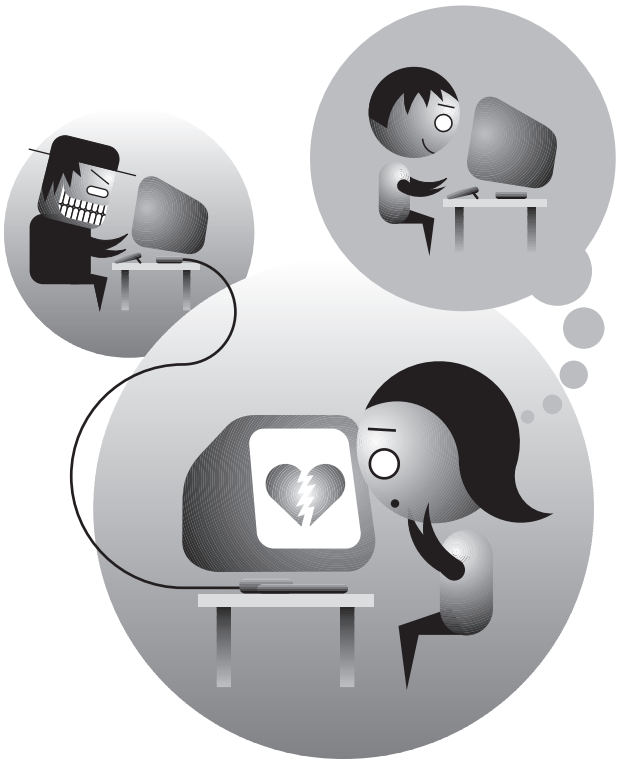


Zu jeder Web-Seite, die Alice gerade betrachtet, kann der Browser Sicherheitsinformationen anzeigen. Die folgende Abbildung zeigt die Sicherheitsinformationen im Fall einer unverschlüsselt übertragenen Web-Seite.


Verschlüsselung
Diese Seite wurde nicht verschlüsselt. Die Seite konnte beim Laden folglich von Dritten eingesehen werden. Dies bedeutet zudem, daß sich die Identität der Web-Site nicht feststellen läßt. Klicken Sie für nähere Einzelheiten zu allen Dateien auf dieser Seite auf Seiteninformation abrufen.
Seiteninformationen anzeigen

Kapitel 3

Identifizieren im Internet



Alice benutzt ein Verschlüsselungsprogramm zum Verschlüsseln von vertraulichen E-Mails an Bob. Das Programm verschlüsselt alle Nachrichten vor dem Absenden mit dem Public Key von Bob. Damit hat Mallet keine Chance – zumindest dachte das Alice, bis sie eines Tages eine äusserst merkwürdige E-Mail von Bob erhält. Alice kann nicht glauben, dass Bob so etwas schreiben würde. Sie ahnt Böses: Woher weiss sie, dass die Mail von Bob stammt und nicht etwa von Mallet?

Auch Bob traut der vermeintlichen Sicherheit im Internet nicht so recht. In letzter Zeit erhält er häufig Plattenbestellungen per E-Mail. Viele der Bestellungen werden allerdings nach der Auslieferung von der Post an Bobs Adresse zurückgeschickt, weil der Empfänger nicht bekannt ist. Vielleicht hat Mallet die Finger im Spiel? Er könnte der Urheber der falschen Bestellungen sein. Gibt es eine Möglichkeit, dass Bob seine Kunden eindeutig identifizieren kann?

Eben hat Alice bei Bob angerufen. Sie ist völlig aus dem Häuschen: Auf der Web-Site einer kleinen fernöstlichen Nachrichtenagentur hat Alice per Zufall die Wahnsinnsmeldung des Jahres entdeckt, brandneu! Es gilt keine Minute zu verlieren, denn bald wird auch die Konkurrenz von der Nachricht erfahren. Gleichzeitig kommen Alice erste Zweifel. Sie weiss zwar, dass die Nachrichtenagentur existiert. Aber wäre es nicht möglich, dass jemand wie Mallet den Web-Server fälscht? Wie kann sie die Echtheit des Servers überprüfen?

Aspekte der Kommunikationssicherung

Alice übermittelt elektronische Liebesgrüsse an Bob. Den eifersüchtigen Mallet kann sie nicht ohne weiteres daran hindern, den Kommunikationskanal zwischen ihr und Bob zu «belauschen». Doch mit Hilfe von Verschlüsselung lässt sich der Text so verändern, dass nur der Schlüsselbesitzer – zum Beispiel Bob – die korrekte Bedeutung rekonstruieren kann. Mallet kann die abgehörten Botschaften nicht entziffern. Durch die Verschlüsselung werden Daten vertraulich gehalten. *Vertraulichkeit* ist das Geheimhalten von Informationen gegenüber Unbefugten.

Die Gewährleistung der Vertraulichkeit von Daten ist jedoch nur ein Aspekt der Datensicherheit. Mallet kennt den Public Key von Alice und könnte ihr eine verschlüsselte Botschaft in Bobs Namen zukommen lassen. Es braucht eine Möglichkeit, sich der Identität der Kommunikationspartner zu versichern. Dieses Identifizieren der Kommunikationspartner wird *Authentifizierung* genannt.

Damit der Kommunikationskanal zwischen Alice und Bob als sicher bezeichnet werden kann, muss er mehrere Anforderungen erfüllen. Die zwei wichtigsten sind Vertraulichkeit und Authentifizierung. Eine weitere wichtige Forderung ist die *Integrität* der verschickten Daten. Die Integrität von Daten ist dann gewährleistet, wenn die Daten während der Übermittlung nicht verändert wurden.

In den folgenden Abschnitten werden wir *digitale Unterschriften* kennen lernen, die zum Beglaubigen von digitalen Dokumenten benutzt werden und gleichzeitig die Integrität von Daten gewährleisten. Im Anschluss daran befassen wir uns mit den *Zertifikaten*. Sie dienen als digitale Identitätsausweise und ermöglichen damit die Authentifizierung von Personen oder Rechnern im Internet.

Digitale Unterschriften

Alice schickt Bob zur Abwechslung einen Brief auf normalem Papier. Woher weiss Bob, dass die Nachricht tatsächlich von Alice stammt? Auch Mallet könnte einen Brief verfassen und Alices Namen darunter setzen. Wenn da nicht die Unterschrift wäre. Die Unterschrift identi-

fiziert Alice als Absenderin des Briefes.

Im Alltag verwendet Alice ihre handschriftliche Unterschrift bei vielen Gelegenheiten. Wie aber kann Alice eine E-Mail unterschreiben? Ist das überhaupt möglich? Wie muss man sich das technisch vorstellen?

Eigenschaften von Unterschriften

Eine Unterschrift soll einen Text, einen Vertrag oder eine schriftliche Aussage bestätigen und bekräftigen. Sie verbindet das Geschriebene mit einer bestimmten Person und klärt somit, wer für das Geschriebene verantwortlich ist.

Die Unterschrift garantiert für alles, was auf demselben Stück Papier steht. Demnach hält das Papier physisch den Text zusammen, der zu einer Unterschrift gehört. Das Papier *bindet* die Unterschrift an den Text.

Natürlich darf der Text nach der Unterzeichnung nicht mehr verändert werden. Auch hier hilft das Papier, weil auf diesem Medium eine Änderung meistens Spuren hinterlässt und rasch auffällt. Zudem werden von wichtigen Dokumenten oft Kopien angefertigt, die zum Vergleich hinzugezogen werden können.

Zusammenfassend die wichtigsten Eigenschaften von Unterschriften:

- Eine Unterschrift ist *eindeutig* und *überprüfbar*. Jeder Mensch sollte eine eigene Unterschrift haben. So lässt sich feststellen, von welcher Person eine gewisse Unterschrift stammt.
- Unterschriften sollten möglichst *nicht fälschbar* sein. Bei Unterschriften von Hand ist diese Anforderung nicht immer erfüllt. Immerhin können Experten in der Regel eine Fälschung entlarven.
- Unter den geschilderten Umständen *identifiziert* eine Unterschrift eine bestimmte Person, sofern eine Referenzunterschrift in einem amtlichen Dokument (Pass, Identitätsausweis usw.) vorliegt.

Digital unterschreiben

Eine herkömmliche Unterschrift von Hand wird einfach zum betreffenden Dokument hinzugefügt. Das Papier sorgt dafür, dass die Unterschrift mit dem Text in Verbindung gebracht wird.

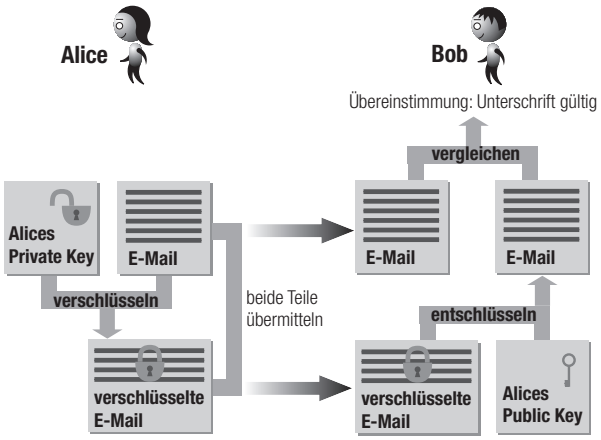
Bei digitalen Dokumenten ist das nicht so einfach. Es genügt nicht, die Unterschrift dem Text mitzugeben. Damit bestünde keinerlei Beziehung zwischen Text und Unterschrift, denn digitale Dokumente können problemlos und vor allem spurlos verändert werden. Neue Textstellen können hinzugefügt und bestehende Abschnitte entfernt werden. Jemand könnte sogar die digitale Unterschrift aus dem Dokument kopieren und ein anderes Dokument damit unterzeichnen.

Aus diesen Gründen müssen bei digitalen Dokumenten der Dokumentinhalt und die Unterschrift untrennbar miteinander «verwoben» werden. Die Unterschrift muss den Inhalt in irgendeiner Form enthalten.

Hier helfen die Public-Key-Verschlüsselungsverfahren weiter. Es kommen zwei Schlüssel zum Einsatz: Der Public Key dient zum Verschlüsseln von Informationen und wird einer breiten Öffentlichkeit zugänglich gemacht. Was der Public Key verschlüsselt, kann nur mit dem Private Key entschlüsselt werden.

Zur Realisierung von digitalen Unterschriften tauschen Public und Private Key die Rollen: Alice verschlüsselt die zu unterzeichnende E-Mail mit ihrem Private Key. Anschliessend schickt sie die verschlüsselte E-Mail sowie die Mail im Klartext an Bob. Bob kann die Unterschrift überprüfen, indem er die verschlüsselte E-Mail mit Alices Public Key entschlüsselt und das Resultat mit dem Klartext der E-Mail vergleicht. Stimmen die beiden Versionen überein, so ist die Unterschrift gültig. Andernfalls ist etwas schief gelaufen.

Ein Fehler kann verschiedene Gründe haben: (1) Bob verwendet nicht den korrekten Public Key von Alice. (2) Die Mail wurde nicht mit dem Private Key von Alice unterzeichnet. (3) Der verschlüsselte oder der unverschlüsselte Text wurde vorsätzlich geändert. (4) Einer der Texte wurde durch Fehler bei der Übertragung modifiziert.



In der Praxis wird nicht die vollständige E-Mail zweimal verschickt. Nur die Klartext-Version wird vollständig übermittelt. Die zu verschlüsselnde Version wird zunächst vorverarbeitet, indem eine mathematische Funktion eine «Zusammenfassung» (einen so genannten *Hash-Wert*) des Inhalts erzeugt. Der Hash-Wert dient lediglich zur Effizienzsteigerung, damit die verschickte Datenmenge reduziert wird. Prinzipiell ist die Vorstellung korrekt, dass die E-Mail gleichzeitig in lesbarer und in verschlüsselter Form übertragen wird.

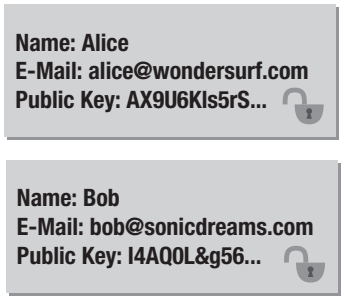
Durch das Vertauschen der Rollen von Public Key und Private Key werden zwei wichtige Voraussetzungen von Unterschriften erfüllt: Nur Alice soll ein Dokument mit ihrer Unterschrift versehen können und verwendet dazu folglich den Private Key. Auf der anderen Seite müssen beliebige Personen die Unterschrift prüfen können. Deshalb wird zur Überprüfung einer Unterschrift der Public Key benutzt.

Mit Hilfe der digitalen Unterschrift wird die Authentizität einer E-Mail gewährleistet. Um auch die Vertraulichkeit des Inhalts zu garantieren, wird Alice ihre Mail zusätzlich mit dem Public Key von Bob verschlüsseln.

Authentifizierung durch digitale Zertifikate

Wichtige Voraussetzung für das Funktionieren von Public-Key-Verschlüsselungsverfahren ist das Veröffentlichen der Public Keys. Will eine Drittperson Alice und Bob eine verschlüsselte E-Mail schicken, benötigt sie die Public Keys von Alice und Bob. Möglichst viele Leute sollen sich die Public Keys von Alice und Bob besorgen können. Auch Bob und Alice müssen in der Lage sein, sich die Public Keys von Dritten zu beschaffen.

Es genügt nicht, nur die Schlüssel alleine bekannt zu geben. Public Keys werden zusammen mit dem Namen der Besitzerin veröffentlicht. Es ist denkbar und sinnvoll, weitere Angaben wie E-Mail-Adresse oder Geburtsdatum anzufügen. So entsteht eine «virtuelle Visitenkarte» mit den wichtigsten Angaben zu einer Person. Bob kann Alice seine persönliche Visitenkarte schicken. Damit erhält Alice den Public Key von Bob und kann ihm verschlüsselte E-Mails zukommen lassen.



Ein Problem bleibt: Alice sucht nach Bobs Public Key und findet eine «Visitenkarte» mit dem Namen «Bob», der E-Mail-Adresse `bob@freemail.net` und einem Schlüssel. Handelt es sich um einen anderen Bob? Hat Bob eine zweite E-Mail-Adresse? Oder könnte Mallet dahinter stecken, der unter falschem Namen auftritt?

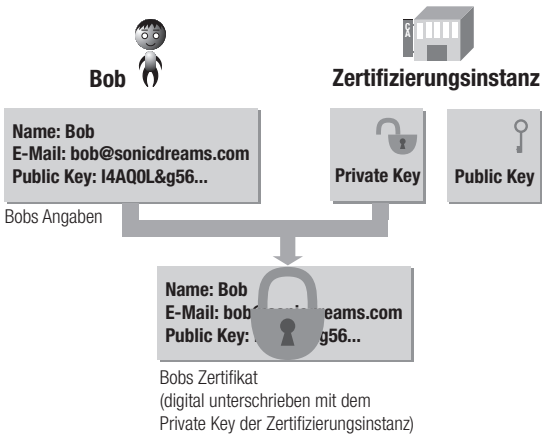
Im Alltag kann Mallet problemlos gefälschte Visitenkarten mit Bobs Namen drucken lassen. Genauso kann Mallet eine virtuelle Visitenkarte mit Bobs Namen und einer eigens zu diesem Zweck erstellten E-Mail-Adresse veröffentlichen. Fällt Alice auf den Schwindel

rein, verschlüsselt sie fortan ihre E-Mails mit dem falschen Schlüssel und schickt sie an Mallets Adresse.

Es fehlt ein Bindeglied zwischen dem Public Key und der Person, die dahinter steckt. Diese Lücke schliessen die digitalen *Zertifikate*. Ein Zertifikat soll beweisen, zu welcher Person ein bestimmter Public Key gehört – analog zu einem Pass im Alltagsleben, der gewisse Angaben einer Person amtlich bestätigt.

Bob möchte sich ein digitales Zertifikat beschaffen. Dazu sucht er eine so genannte *Zertifizierungsinstanz* auf. Eine Zertifizierungsinstanz ist beispielsweise eine Firma, die sich auf die Ausgabe von Zertifikaten spezialisiert hat.

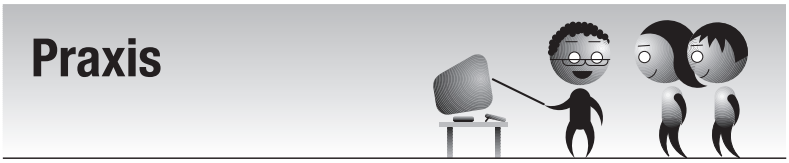
Bob legt der Zertifizierungsinstanz seinen Public Key vor und beweist seine Identität mit Hilfe eines anerkannten Ausweises. Die Zertifizierungsinstanz stellt anschliessend ein digitales Dokument mit Bobs persönlichen Angaben und seinem Public Key zusammen. Zum Abschluss wird das Dokument mit Hilfe des Private Keys der Zertifizierungsinstanz digital unterschrieben. Damit erhält Bob einen digitalen Identitätsausweis.



Welchen Nutzen zieht Alice aus Bobs Zertifikat? Sie besorgt sich sein Zertifikat und den Public Key der Zertifizierungsinstanz. Mit Hilfe des Public Keys der Zertifizierungsinstanz überprüft sie, ob das

Zertifikat korrekt signiert ist. Verläuft die Überprüfung erfolgreich, kann Alice davon ausgehen, dass sie es mit dem «richtigen» Bob zu tun hat.

Damit sind jedoch nicht alle Probleme gelöst. Wieso soll Alice der Zertifizierungsinstanz vertrauen? Schliesslich könnte es sich um eine Hochstaplerfirma handeln. Zwei Möglichkeiten: Erstens, die Zertifizierungsinstanz lässt sich ihrerseits zertifizieren. Damit wird das Problem aber lediglich verlagert. Zweitens, die Zertifizierungsinstanz hat sich einen derart seriösen Ruf verschafft, dass ihr gemeinhin Vertrauen entgegengebracht wird.

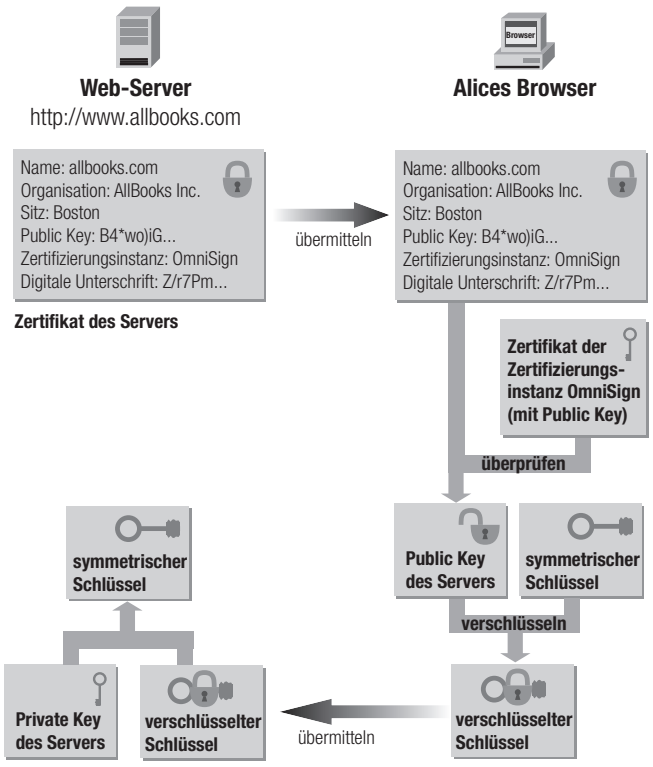


Zertifikate im World Wide Web

Alice kauft beim Online-Buchladen unter der Adresse `www.allbooks.com` ein. Sie tippt ihre Kreditkartenangaben ein und kann dank der SSL/TLS-Technik davon ausgehen, dass ihre kostbaren Informationen vor der Übertragung verschlüsselt werden.

Wie aber steht es um die Echtheit des Web-Servers? Mallet könnte selber einen Web-Server einrichten und ihm den Namen `www.allbooks.com` geben. Dann würde er Anfragen an den Originalserver zu seinem gefälschten Server umleiten und so die Kreditkarteninformationen von Kunden erfahren. Das Fälschen eines Web-Servers ist zwar aufwendig, technisch aber durchaus realisierbar.

Die Lösung gegen gefälschte Web-Server heisst Authentifizierung. Der Server muss sich beim Benutzer mit Hilfe eines Zertifikats ausweisen. Bei SSL/TLS schickt der Server deshalb in einem ersten Schritt sein eigenes Zertifikat an den Browser.



Das Zertifikat ist der Ausweis des Servers. Darin sind alle wichtigen Angaben enthalten, mit denen der Server sowie die betreibende Organisation oder Privatperson identifiziert werden können. Die Kundin Alice kann sich das Zertifikat anschauen und aufgrund der Angaben prüfen, ob es sich um den richtigen Server handelt. Sie findet im Zertifikat auch Angaben darüber, welche Zertifizierungsinstanz für die Informationen bürgt. Mit Hilfe des Public Keys der Zertifizierungsinstanz kann Alice die Echtheit des Zertifikats prüfen. Die Firma AllBooks Inc. musste der Zertifizierungsinstanz nämlich alle Informationen schriftlich belegen: zum Beispiel den Firmennamen, den Sitz der Firma sowie den Namen der Internet-Domain. Eine *Domain* bezeichnet eine Gruppe von Rechnern, die im Namen dasselbe Suffix aufweisen, zum Beispiel alle Rechner mit der Endung `allbooks.com`.

Den Public Key der Zertifizierungsinstanz kann Alice auf zwei Arten erhalten: (1) Von einigen Zertifizierungsinstanzen sind die Zertifikate inklusive Public Keys fest im Web-Browser installiert. (2) Falls der Public Key vom Browser-Hersteller nicht eingebaut wurde, besorgt sich Alice den Schlüssel von der Web-Site der Zertifizierungsinstanz.

Sichere E-Mails mittels S/MIME

Um neben reinen Textdokumenten auch Bilder, Tondateien oder andere Dokumentarten in E-Mails einbinden zu können, wurden die *Multipurpose Internet Mail Extensions* (kurz: *MIME*) geschaffen. MIME ist ein Standard, der die Übertragung und Codierung solcher Zusätze (Extensions) zu E-Mails regelt. *S/MIME* steht für *Secure MIME* und regelt, durch welche Techniken die Vertraulichkeit, Authentizität und Integrität von E-Mails garantiert werden können.

Bevor Alice eine sichere E-Mail an Bob verschicken kann, muss sie einige Dinge beachten: Alice benötigt einen Private Key, einen Public Key sowie ein zugehöriges Zertifikat. Das Mail-Programm versieht die E-Mail mit Hilfe des Private Keys mit einer digitalen Unterschrift und verschickt anschliessend die signierte E-Mail zusammen mit Alices Zertifikat. Auf der Gegenseite benutzt Bobs E-Mail-Programm das Zertifikat von Alice, um die Unterschrift zu überprüfen. Bob kann nun davon ausgehen, dass Alice die Urheberin der Botschaft ist und niemand den Text nachträglich geändert hat.

Alice möchte die E-Mail zusätzlich verschlüsseln, um die Vertraulichkeit der Informationen zu gewährleisten. Zum Verschlüsseln benötigt sie den Public Key von Bob. Dazu lässt sie sich von Bob eine signierte E-Mail schicken und gelangt so in den Besitz von Bobs Zertifikat.

Die Übermittlung von sicheren E-Mails ist komplizierter als die Übermittlung von sicheren Web-Seiten. Bei SSL (oder TLS) geschieht der Austausch der Schlüssel automatisch. Die Benutzerin bemerkt nichts davon.

Anders bei sicheren E-Mails: Alice muss sich zunächst bei einer Zertifizierungsinstanz ein Zertifikat besorgen. Das Zertifikat lässt sie

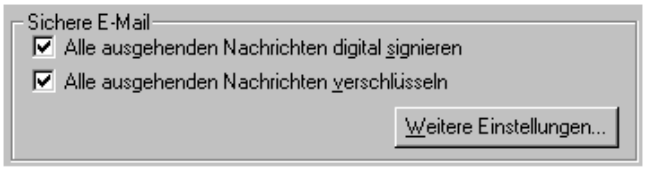
Bob zukommen. Genauso braucht Bob sein eigenes Zertifikat, das er Alice schickt. Erst wenn sie ihre Zertifikate ausgetauscht haben, können sich Alice und Bob gegenseitig verschlüsselte E-Mails zustellen.

Zertifikate im Browser oder E-Mail-Programm

In den meisten Web-Browsern gibt es einen speziellen Bereich mit Informationen und Einstellungen zum Thema Sicherheit. Dort hat Alice die Möglichkeit, ihr eigenes Zertifikat (vielleicht sind es auch mehrere) anzuschauen. Ausserdem kann sie die Zertifikate von bereits besuchten, mit Zertifikaten ausgestatteten Web-Servern begutachten. Weiter sind die Zertifikate von anderen Personen sowie von bekannten Zertifizierungsinstanzen gespeichert. Auch der Private Key von Alice ist im Browser abgelegt. Den Private Key schützt Alice mit einem Passwort vor dem Zugriff durch unbefugte Personen.

Zu jeder besuchten Web-Seite kann Alice gewisse Sicherheitsinformationen anzeigen lassen. So findet Alice heraus, ob die Seite verschlüsselt oder unverschlüsselt übertragen wurde. Bei verschlüsselten Web-Seiten, die von einem SSL/TLS-fähigen Web-Server stammen, kann sie das Zertifikat des Servers betrachten.

In vielen Mail-Programmen lassen sich zwei wichtige Einstellungen vornehmen: (1) Ausgehende E-Mails können digital unterschrieben werden, falls Alice über ein persönliches Zertifikat verfügt. (2) Ausgehende E-Mails lassen sich zusätzlich verschlüsseln, falls Alice das Zertifikat des jeweiligen Empfängers besitzt.

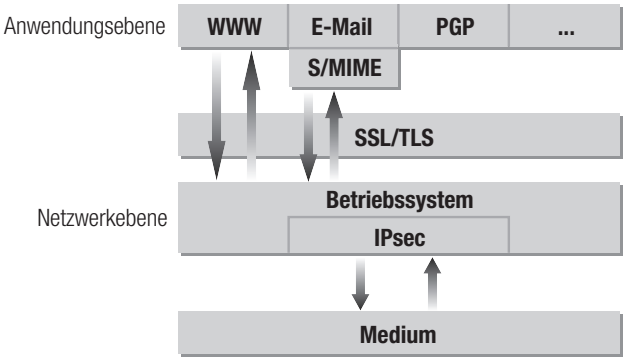


Die Zertifikate im Web-Browser oder E-Mail-Programm können von beliebigen Zertifizierungsinstanzen stammen, solange sie sich an gewisse Standards halten. Der am weitesten verbreitete, internationale Standard für Zertifikate heisst *X.509*.

Sichere Kommunikation im Überblick

Wir haben einige Techniken zur Kommunikationssicherung kennen gelernt: SSL, TLS, S/MIME und PGP. Wir betrachten im Folgenden die Techniken nochmals in einem Überblick, der die Vor- und Nachteile aufzeigen soll. Dazu nehmen wir den Versand von Daten via Internet unter die Lupe: Wie gelangt eine E-Mail, die in einem Mail-Programm getippt wurde, ins Internet?

Der Datenversand folgt einem einfachen Schichtenmodell. Jede Schicht hat eine klar definierte Aufgabe – ähnlich wie bei der Fliessbandproduktion eines Autos, wo jede Station einen festen Einzelschritt durchzuführen hat. In der obersten Schicht auf *Anwendungsebene* befindet sich das E-Mail-Programm auf dem Computer von Alice. Das Mail-Programm reicht die E-Mail weiter an die darunter liegende Schicht, die *Netzwerkebene*. Dort wird der Text in kleinere Pakete zerlegt und jedes Paket mit der Zieladresse versehen. Zum Schluss wird das Datenpaket über die Telefonleitung oder ein anderes Medium übertragen. Beim Empfänger läuft der Prozess in umgekehrter Richtung ab, bis der vollständige Text in Bobs Mail-Programm erscheint.



Welche Schicht soll die Verantwortung für die Kommunikationssicherung übernehmen? Das E-Mail-Programm auf Anwendungsebene kann alle Informationen verschlüsseln, bevor sie an die Netzwerkebene weitergereicht werden. Nicht verschlüsselt sind dann die anderen

Internet-Dienste, zum Beispiel die Übertragung von Web-Seiten mittels HTTP.

Alternativ kann die Verschlüsselung von der Netzwerkebene im Betriebssystem übernommen werden. Jedes Anwendungsprogramm übergibt seine Daten an die Netzwerkebene und kann wählen, ob Verschlüsselung oder Authentifizierung aktiviert werden soll. Der Vorteil liegt auf der Hand: Jede Anwendung – ob Web-Browser, E-Mail-Programm oder eine Online-Banking-Applikation – kann von den Verschlüsselungsmechanismen auf Netzwerkebene profitieren.

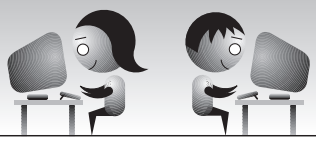
Das Verschlüsselungstool PGP ist auf Anwendungsebene einzuordnen. PGP ist eine eigenständige Anwendung, mit der beliebige Daten verschlüsselt oder signiert werden können. Ebenfalls auf Anwendungsebene arbeitet S/MIME, das üblicherweise im E-Mail-Programm integriert ist. SSL/TLS ist zwischen Netzwerkebene und Anwendungsebene einzuordnen. SSL und TLS nehmen Daten von einer Anwendung entgegen, verschlüsseln sie und reichen sie an die Netzwerkebene weiter.

IPsec

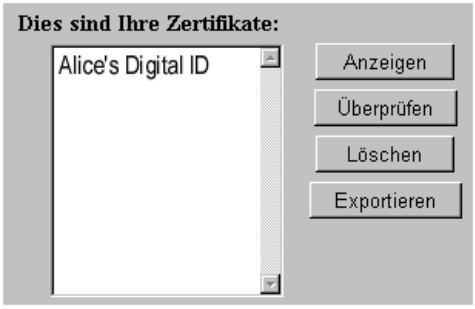
Damit die Kommunikation funktioniert, müssen sich die Rechner im Internet an ein Regelwerk halten. Diese Regelwerke heissen *Protokolle*. Im Internet wird meistens eine Protokollkombination namens *TCP/IP (Transmission Control Protocol/Internet Protocol)* eingesetzt. TCP/IP stammt aus der Zeit, als das Internet noch nicht als moderner Markt- und Tummelplatz für Millionen von Benutzern konzipiert war. Deshalb wurden Sicherheitsaspekte lange Zeit vernachlässigt.

Besserung verspricht *IPsec*. IPsec beschreibt eine Sammlung von zusätzlichen Protokollen, welche die Kommunikationssicherung nach Bedarf durch Verschlüsselung und Authentifizierung erlauben. IPsec kann zusammen mit der aktuellen Version von IP (IPv4) eingesetzt werden. Die Neuauflage von IP namens IPv6 unterstützt IPsec standardmässig.

Anwendung



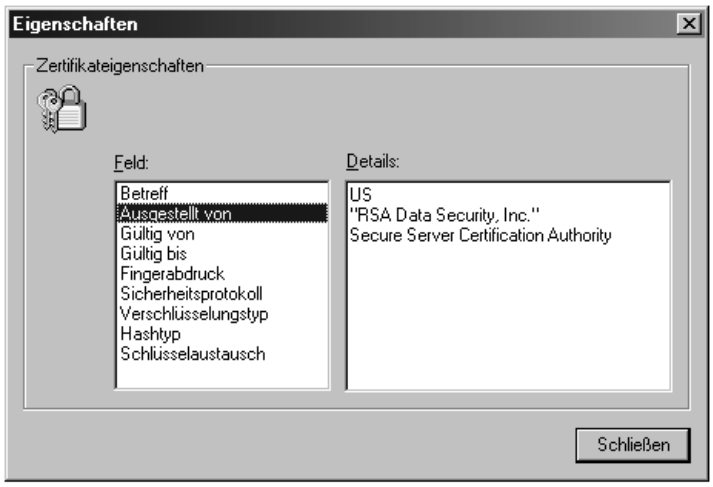
E-Mails können verschlüsselt und digital unterschrieben werden. Allerdings muss sich Alice um diese Dinge selbst kümmern. Sie hat die Sicherheitseinstellungen in ihrem Browser und ihrem Mail-Programm eingehend studiert. Alice kann zum Beispiel ihr persönliches Zertifikat registrieren und damit ausgehende E-Mails bei Bedarf unterzeichnen.



Ausserdem führt der Browser Buch über die Zertifikate anderer Leute oder Web-Sites. So kann Alice die Identität von Web-Sites oder die Absender eingehender E-Mails überprüfen.

Der Web-Browser und das E-Mail-Programm benötigen Zusatzinformationen, um die Echtheit von Zertifikaten zu überprüfen. Deshalb sind in den meisten Web-Browsern schon einige Zertifikate von Zertifizierungsinstanzen fest gespeichert. Trotzdem fehlt ab und zu ein Zertifikat. Dann muss Alice die Web-Site der betreffenden Zertifizierungsinstanz besuchen, das Zertifikat herunterladen und in ihrem Browser ablegen.

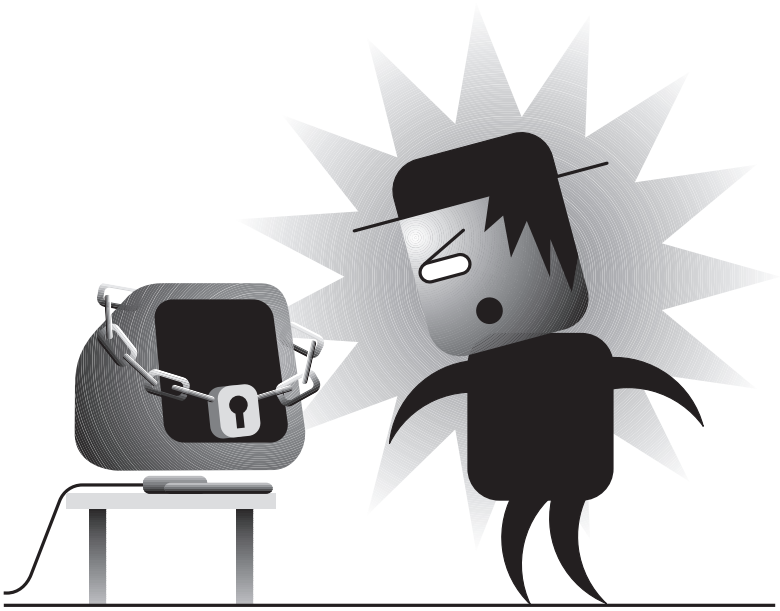
Mit Hilfe der gespeicherten Zertifikate kann Alice die Echtheit eines Web-Servers prüfen. Gleichzeitig erfährt sie, welche Zertifizierungsinstanz für die Angaben bürgt:



Alice befasst sich mit der brandheissen Wahnsinnsmeldung auf der Web-Site der fernöstlichen Nachrichtenagentur. Sie prüft die Vertrauenswürdigkeit der Web-Site und stellt fest: Die Site verfügt über kein Zertifikat, und alle Seiten werden unverschlüsselt übermittelt.
Eine unsichere Sache! Alice ist das Risiko zu gross. Sie beschliesst, dieser Meldung nicht zu trauen und die Finger davon zu lassen. Oder Alice greift zum Telefon und lässt sich die Nachricht persönlich bestätigen.

Kapitel 4

Zugriffe kontrollieren



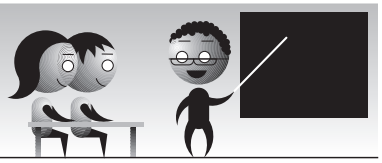
Alice und Bob wollen verhindern, dass eines Tages Mallet in ihre Büroräume eindringt und sich an ihren Computern zu schaffen macht, vertrauliche Informationen zu sehen bekommt oder in ihrem Namen E-Mails verschickt. Deshalb schützen beide ihre Computer mit einem Passwort. Da Alice häufig auf Bobs Rechner arbeitet, kennt sie auch sein Passwort. Damit Alice sich nicht ständig ein neues Passwort merken muss, hat Bob sein Passwort seit längerer Zeit nicht mehr geändert.

Die Mailbox beim Internet-Provider von Alice ist ebenfalls durch ein Passwort geschützt. `Ni3@.tPt` lautet das vom Provider vorgegebene, komplizierte Passwort. Alice hat sich die kryptische Zeichenfolge bis heute nicht merken können. Weil sie nicht weiss, wie man das Passwort ändern kann, hat sie es kurzerhand auf ein PostIt-Zettelchen notiert und an das Gehäuse ihres Monitors geklebt.

Alice verwendet verschiedene Passwörter für gewisse Informationsdienste und kostenpflichtige Datenbanken im Internet. Und vermehrt benutzt Alice Online-Shops für ihre Einkäufe. Hier drängt es sich oft auf, ein persönliches Benutzerprofil zu erstellen. Andernfalls müssen bei jedem Einkauf alle Angaben wie Lieferadresse und Zahlungsweise neu eingegeben werden. Kurz: Alice ist mit einer Unzahl von Passwörtern konfrontiert und hat sich deshalb für ein einziges Passwort – `iLoveBob` – entschieden.

Alice ist klar, dass sie dieses eine Passwort, mit dem sie auch den Zugriff auf das eigene Notebook schützt, strikt geheim halten muss. Doch gestern wollte eine befreundete Journalistin das Notebook für eine Reise ausleihen. Als hilfsbereiter Mensch sagte Alice spontan zu, nur war da wieder dieses verflixte Passwort. Ohne Passwort kein Zugang zum Notebook. Der Kollegin gegenüber wollte Alice nicht den Eindruck erwecken, sie würde ihr misstrauen. Also flüsterte Alice der Kollegin das Passwort ins Ohr, und diese versprach hoch und heilig, das Passwort niemandem weiterzusagen und nach der Reise gleich zu vergessen.

Theorie



Identifikation von Personen

Eine Bank bewahrt Geld und Wertgegenstände in einem Tresor auf. Wünscht eine Person Zugang zum Tresor, muss sie sich ausweisen. Anders ausgedrückt: Die Person muss sich identifizieren und dadurch ihre Zugangsberechtigung beweisen. Üblicherweise wird diese Benutzeridentifikation mit Hilfe von Badges oder durch die Eingabe einer geheimen Nummernkombination erreicht.

Auch in der Computerwelt wird vieles geschützt. Und wo etwas geschützt wird, muss der Zugriff geregelt werden. Dazu müssen die Personen identifiziert werden können, die Zugriff auf eine bestimmte Information oder auf ein gewisses Angebot wünschen. Sobald eine Person identifiziert ist, kann geprüft werden, ob diese Person für den gewünschten Zugriff berechtigt ist. Das Ermächtigen des Zugriffs wird *Autorisation* genannt. Ein Beispiel aus dem Alltag: Zu einem abgeschlossenen Auto hat typischerweise lediglich die Besitzerin Zugangsberechtigung. Dieses Recht beweist die Besitzerin, indem sie sich mit Hilfe des Schlüssels gegenüber dem Auto «identifiziert».

In der Computerwelt gibt es verschiedene Möglichkeiten, Benutzer zu identifizieren. Die häufigste, billigste und oftmals unsicherste Methode sind Passwörter oder PINs. Wesentlich sicherer sind Einmal-Passwörter, die zum Beispiel durch SecurID-Systeme realisiert werden. Auch digitale Zertifikate können zur Identifikation von Benutzern eingesetzt werden. Die wirksamsten, aber aufwendigsten Methoden basieren auf biometrischen Eigenschaften einer Person: zum Beispiel Fingerabdrücke, DNA-Sequenzen oder der Verlauf der Blutgefässe im Auge.

Passwörter

Die Benutzeridentifikation wird häufig mit *Passwörtern* realisiert. Der Grundsatz: Wer das Passwort weiss, ist zum Zugriff auf ein System berechtigt. Leider haben Passwörter schwer wiegende Nachteile:

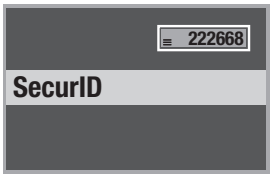
- Benutzer vergessen ihre Passwörter.
- Viele Benutzer halten ihre Passwörter schriftlich fest.
- Oft werden sehr leicht zu erratende Passwörter gewählt.
- Passwörter werden selten geändert.

Trotz dieser Nachteile sind Passwörter nach wie vor die bevorzugte Art der Zugriffskontrolle. Ähnlich beliebt sind die *PINs* oder *Personal Identification Numbers*. PINs sind Passwörter, die ausschliesslich aus Zahlen bestehen.

Einmal-Passwörter

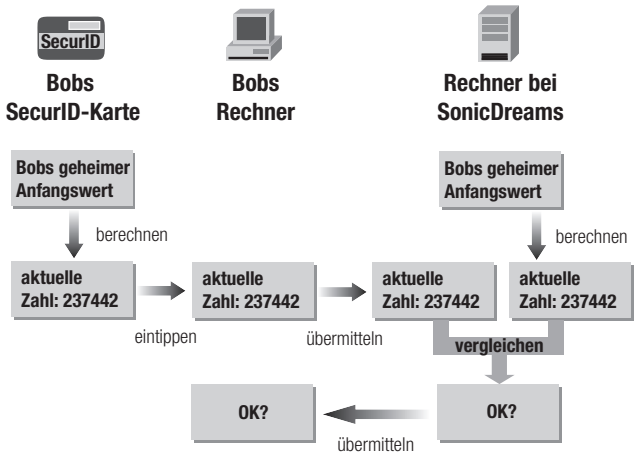
In vielen Fällen bieten Passwörter einen genügenden Schutz vor dem Zugriff durch Unberechtigte. Manche Anwendungen müssen jedoch einen besseren Schutz garantieren. Hier bieten sich so genannte *Einmal-Passwörter* an, denn sie genügen höheren Sicherheitsanforderungen als fixe Passwörter, weil für jeden Zugriff auf eine Anwendung ein neues Passwort verwendet wird. Als Beispiel für solche kurzlebigen Einmal-Passwörter, die nur gerade für einen Zugriff berechtigen, werden nachfolgend die *SecurID-Systeme* vorgestellt.

Wesentlicher Bestandteil von SecurID-Systemen ist die SecurID-Karte. Es handelt sich dabei um einen Mikroprozessor, der in einer robusten Metallkarte von der Grösse einer Kreditkarte untergebracht ist:



Jede Karte verfügt über einen eigenen, geheimen Anfangswert, der fest in der Karte eingebrannt ist. Aus diesem Anfangswert berechnet ein Kleinstcomputer innerhalb der Karte in regelmässigen Abständen einen neuen Wert, typischerweise im Abstand von einer Minute.

Bob besitzt eine SecurID-Karte. Damit kann er sich von zu Hause in sein Computersystem bei SonicDreams einwählen und finanzielle Transaktionen veranlassen. Beim Anmelden fragt ihn das System nach dem aktuellen Wert auf der Karte, und Bob liest den Wert von der Anzeige ab und gibt ihn ein. Das Computersystem bei SonicDreams kennt den geheimen Anfangswert der Karte ebenfalls und kann daraus gleichermassen die aktuell gültige Zahl berechnen. Falls die von Bob eingetippte Zahl stimmt, erhält er Zugriff auf den SonicDreams-Rechner.



Die Sicherheit von SecurID-Karten kann weiter gesteigert werden: Es gibt eine Variante der Karte, die mit einer Zahlentastatur ausgestattet ist. Der Benutzer muss eine geheime PIN eingeben, bevor die Karte den richtigen Zahlenwert liefert. Die grössere Sicherheit basiert darauf, dass der Benutzer zwei Voraussetzungen zu erfüllen hat: Er muss erstens im Besitz der SecurID-Karte sein und zweitens die korrekte PIN kennen. Auch SecurID-Karten ohne Zahlentastatur können

die Kenntnis einer PIN voraussetzen. Die auf der PC-Tastatur eingetippte PIN wird dann zusammen mit dem aktuellen Kartenwert übermittelt und vom SecurID-System geprüft.

Streichlisten

Streichlisten sind eine andere Möglichkeit, Einmal-Passwörter zu realisieren. Ein Benutzer erhält eine lange Liste mit PINs. Für jeden Zugriff auf eine Anwendung wird eine neue PIN verwendet und anschliessend von der Liste gestrichen. Dabei muss die Reihenfolge der PINs unbedingt befolgt werden. Die Überprüfung der PINs übernimmt ein Computersystem, das die Zahlenfolge auch kennt.

Streichlisten funktionieren prinzipiell gleich wie SecurID-Karten. Die SecurID-Karte ist nichts anderes als eine «automatisierte Streichliste». Sowohl bei bei SecurID-Karten wie auch bei Streichlisten ist die sorgfältige Aufbewahrung wichtig, damit Unbefugte nicht an die geheimen PINs kommen.

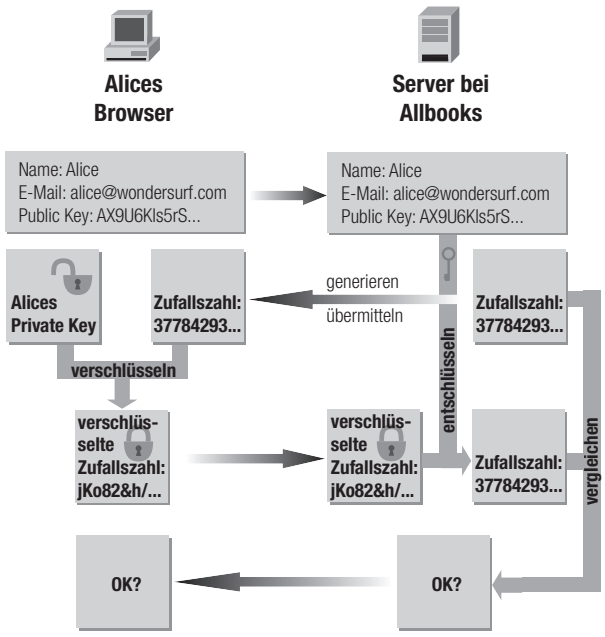
Identifikation mit Zertifikaten

Die Identifikation von Personen aufgrund von *Zertifikaten* basiert auf der Tatsache, dass der Private Key ausschliesslich einer Person bekannt sein sollte. Also wird geprüft, ob die zu identifizierende Person im Besitz des richtigen Private Keys ist.

Beispiel: Der Web-Server von AllBooks möchte Alice anhand ihres Zertifikats authentifizieren. Der Browser von Alice schickt in einem ersten Schritt Alices Zertifikat zum Server. Aus dem Zertifikat erfährt der Web-Server den Namen und weitere Angaben über Alice. Im zweiten Schritt wird sichergestellt, dass das Zertifikat tatsächlich von Alice stammt. Dazu prüft der Web-Server, ob Alice im Besitz des Private Keys ist, der zum Zertifikat gehört. Der AllBooks-Server generiert eine zufällige Zahl und schickt diese an Alices Browser. Der Browser verschlüsselt die Zahl mit Alices Private Key und schickt das Resultat zurück.

Der Server entschlüsselt die empfangene Zahl mit Hilfes des Public Keys aus dem Zertifikat und vergleicht das Resultat mit dem ur-

sprünglichen Wert. Bei einer Übereinstimmung geht der Server davon aus, dass er es mit der «echten» Alice zu tun hat.



Smart Cards

Der Private Key zu einem Zertifikat ist von grosser Bedeutung. Mit ihm werden Daten entschlüsselt, Dokumente unterzeichnet oder Personen identifiziert. Um Missbrauch vorzubeugen, muss der Private Key gut geschützt werden. Wichtig sind die sorgfältige Aufbewahrung sowie der Zugriffsschutz mit einem geeigneten Passwort.

Guten Schutz des Private Keys bieten die *Smart Cards*. Eine Smart Card hat die Form einer Kreditkarte und ist mit einem Mikroprozessor ausgestattet, der das Zertifikat sowie Public und Private Key enthält. Das Zertifikat und der Public Key können bei Bedarf von der Karte gelesen werden. Der Private Key dagegen verlässt die Karte nie. Stattdessen wird beispielsweise ein zu unterzeichnendes

Dokument an den Mikroprozessor der Smart Card übermittelt, der das unterzeichnete Dokument zurückliefert.

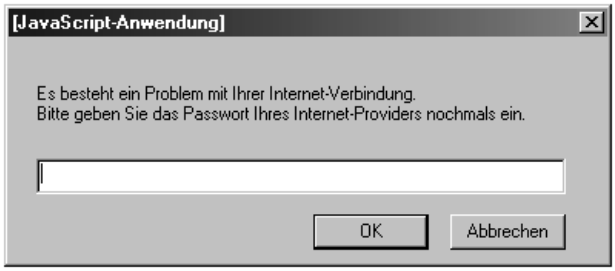
Durch den Einsatz von Smart Cards wird neben einem Mehr an Sicherheit zusätzliche Mobilität gewonnen. Ein Benutzer kann seine Zertifikate und Schlüssel bequem mit sich tragen. Allerdings werden für die Benutzung von Smart Cards geeignete Kartenleser benötigt. Ausserdem besteht die Gefahr des Verlusts der Smart Card.

Social Engineering

Trotz der technischen Massnahmen zur Zugriffskontrolle bleibt oft der Mensch die grösste Schwachstelle. Beim *Social Engineering* geht es darum, Personen zu «verschaukeln». Das heisst, es wird einer Person eine falsche Seriosität vorgespielt und sie dazu gebracht, sensible Informationen preiszugeben. Etwa so, wie wenn sich im Alltagsleben jemand als Polizist ausgibt und sich auf diese Weise den Zugang zu einer Wohnung verschafft.

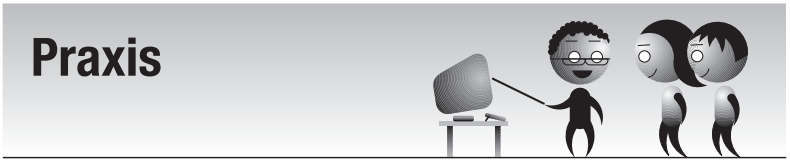
Im Internet kann Mallet ähnliche Dinge anstellen. Beispielsweise kann Mallet Alice anrufen und sich als Mitarbeiter ihres Internet-Providers ausgeben: «Guten Tag, ich bin Administrator bei WonderSurf. Es gibt Probleme mit Ihrem Konto bei uns. Können Sie mir bitte Ihren Benutzernamen und Ihr Passwort nennen. Ich werde dann alles in Ordnung bringen.» Nichtsahnend verrät Alice ihr Passwort. Fortan kann Mallet Alices Konto gratis benutzen, ihre E-Mails lesen und ihre Homepage abändern.

Oder: Mallet stellt eine Web-Seite für seine Zwecke zusammen. Sobald ein nichtsahnendes Opfer die Seite anwählt, wird es mit der nachfolgenden Meldung konfrontiert.



Viele Benutzer sind darauf getrimmt, alle Aufforderungen, die am Bildschirm erscheinen, zu befolgen. Deshalb ist die Wahrscheinlichkeit gross, dass der eine oder andere Benutzer der oben gezeigten Aufforderung nachkommt und sein Passwort eingibt, das dann bei Mallet landet.

Gegen solche Formen des Angriffs gibt es kein Patentrezept. Man sollte grundsätzlich keine sensiblen Informationen an Personen weitergeben, von deren Identität man nicht überzeugt ist. Eine gesunde Portion Misstrauen ist angebracht. Bevor man eine Aufforderung am Bildschirm befolgt, sollte man sich Gedanken darüber machen, wie sinnvoll die Aktion ist und was die Konsequenzen sind. So gibt es zum Beispiel keinen ersichtlichen Grund, warum bei einer funktionierenden Internet-Verbindung die Benutzerangaben erneut eingegeben werden sollten.



Ungeeignete Passwörter

Eigentlich gibt es nur eine simple Regel: Leicht zu erratende Passwörter sind schlechte Passwörter! Einige Beispiele:

- Passwörter, die aus einem einzigen oder einigen wenigen Buchstaben bestehen.
- Offensichtliche Zahlen: Geburtsdaten, Telefonnummern, Postleitzahlen oder Autokennzeichen
- Tastaturmuster: `qwertz`, `mnbvcxy` oder `wsxedcrfv`
- Zahlenmuster: `12345678` oder `97531`
- Der eigene Name, der Name der Freundin, des Ehemannes, eines Popstars, eines Filmhelden, einer Stadt oder Automarke
- Wörter aus einem Wörterbuch beliebiger Sprache
- Variationen von existierenden Wörtern: `Alice`, `alicE`, `ALICE10` oder `7ecila`

Mit diesen Passwörtern hat Mallet ein leichtes Spiel. Es ist ziemlich einfach, Namen, Geburtstag, Autonummer usw. einer Person herauszufinden. Zudem kann Mallet ein Programm einsetzen, das in kurzer Zeit ganze Wörterbücher durchprobiert, bis ein gültiges Passwort gefunden wurde. Eine grosse Zahl von Passwörtern kann geknackt werden, weil die obigen Regeln nicht beachtet werden.

Gute Passwörter

Ein gutes Passwort ist schwierig zu erraten. Das heisst: Ein gutes Passwort soll nicht zu kurz sein, sondern acht Zeichen und mehr umfassen. Ideal ist, wenn das Passwort aus Gross- und Kleinbuchstaben besteht und Zahlen sowie Sonderzeichen wie «@» oder «!» enthält.

Unglücklicherweise ist ein nicht leicht zu erratendes Passwort auch nicht leicht auswendig zu lernen. Man kann sich aber mit einem Trick behelfen und sein Passwort aus einer «Eselsbrücke» zusammenbauen. Dazu überlegt man sich einen mehr oder weniger sinnlosen Satz wie zum Beispiel «Wenn mein Handy klingelt, sag ich nett ‹hallo›». Nun kombiniert man die Anfangsbuchstaben der Wörter zu einem Passwort. Ausserdem wird die Gross- und Kleinschreibung variiert. Resultat: `wMHksInH`. Ein anderes Beispiel: Aus dem Satz «The

angry dragon's mouth stinks of foul fish» entsteht `t@DMsOfF`. Anstelle des Buchstabens «O» wird hier die Ziffer «0» verwendet. Für das «a» steht das Sonderzeichen «@». Bei diesem Vorgehen ist zu beachten, dass der Satz für die «Eselsbrücke» nicht zu offensichtlich gewählt werden darf. Wer phantasievoll ist und sich Wörter gut merken kann, kann sich auch ein Phantasiewort ausdenken und als Passwort benutzen.

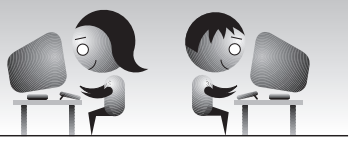
Angriffe auf Passwortsysteme

Mallet hat verschiedene Möglichkeiten, an eines der Passwörter von Alice heranzukommen:

- Mallet versucht, ein Passwort zu erraten. Wenn er Glück hat, verwendet Alice Passwörter wie `alice` oder `ecila`.
- Mallet erfährt ein Passwort, indem er die Internet-Verbindung von Alice «abhört». Dagegen hilft der Einsatz von Verschlüsselungstechniken oder Einmal-Passwörtern.
- Mallet errät ein Passwort durch systematisches Probieren einer grossen Zahl von möglichen Passwörtern. Es gibt Programme, die automatisch Passwörter generieren und durchprobieren. Diese Programme verwenden eine Sammlung von Wörterbüchern zu unterschiedlichen Themen und in verschiedenen Sprachen. Mit Hilfe solcher Werkzeuge lassen sich überraschend viele Passwörter erraten.

  Manche Computersysteme erlauben es Mallet sogar, Programme zum Passwort-Raten via Internet einzusetzen. Mallet kann ein solches Programm vom eigenen Rechner gegen ein Computersystem im Internet einsetzen und wird benachrichtigt, wenn ein gültiges Passwort gefunden wurde. Gegen das systematische Passwort-Raten hilft die Wahl von guten Passwörtern oder der Einsatz von Einmal-Passwörtern.

Anwendung



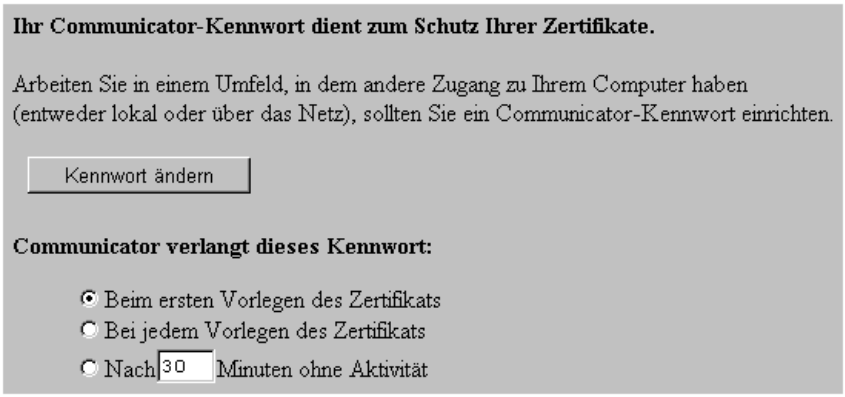
Mit ihrem einzigen Passwort `iLoveBob` hat sich Alice die Sache zu leicht gemacht. Das hat sie spätestens dann festgestellt, als sie ihrer Kollegin das Passwort für ihr Notebook verraten musste. Da wusste die Kollegin auch gleich Alices Passwort für das E-Mail-Konto oder den Verkehr mit ihrer Hausbank.

Das soll Alice nicht mehr passieren. Sie verwaltet jetzt ihre Passwörter systematisch. Dazu bildet sie Gruppen von Anwendungen, die etwa dieselbe Sicherheit erfordern, und wählt für jede Gruppe ein geeignetes Passwort. Alice hat sich für vier Arten von Passwörtern entschieden: Eines für den Zugang zum Computer, eines zum Schutz ihres Private Keys, eines für den Zugang zum Internet-Provider, zum Mail-Server sowie zu Online-Shops und ein letztes für den Zugriff auf kostenfreie Informations- und Nachrichtendienste im Internet.

Alice ist eigentlich kein misstrauischer Mensch. Aber für die Kaffee- und Mittagspause schützt sie ihren PC im Büro mit Hilfe des Bildschirmschoners. Der Bildschirmschoner kann so eingestellt werden, dass er nach dem Passwort fragt, bevor der Zugriff zum Computer freigegeben wird. Damit stellt Alice sicher, dass sich in ihrer Abwesenheit niemand am Rechner zu schaffen macht.

Für Online-Einkäufe verwendet Alice immer dasselbe Passwort: `B&JvesWE`. Das merkt sie sich mit Hilfe der Eselsbrücke «Bob und ich verbringen ein schönes Wochenende». Für ihre vielen Abonnemente bei weniger kritischen Online-Informationsdiensten benutzt Alice das Kennwort `ThBaStJo` – «The Backstreet Journal».

Auch den Private Key zu ihrem Zertifikat schützt Alice mit einem Passwort:



Sie kann wählen, ob das Passwort nur einmal, bei jedem Zugriff auf den Private Key oder in regelmässigen Abständen erfragt wird. Diese Einstellung hängt davon ab, ob mehrere Benutzer denselben Computer verwenden.

Kapitel 5

Bezahlen im Internet

Alice hat schon mehrmals im Internet eingekauft. Buchbestellungen bei AllBooks bezahlt sie mit ihrer Kreditkarte. Das funktioniert bestens. Trotzdem ist Alice nicht immer wohl dabei, denn sie kann nicht prüfen, was mit ihren Kreditkartenangaben geschieht. Was, wenn ein Online-Shop zum Beispiel mehr als den Rechnungsbetrag belastet? Oder wenn die Kartendaten vom Server des Online-Shops gestohlen werden?

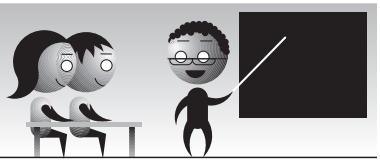
Im Alltag benutzt Alice ihre Kreditkarte für grössere Einkäufe oder im Restaurant. An vielen Orten lohnt sich die Kreditkarte allerdings kaum. Ausserdem akzeptieren Kioske oder Lebensmittelgeschäfte meist keine Kreditkarten, weil die Gebühren zu hoch sind.

Ihre täglichen Einkäufe bezahlt Alice deshalb in bar, mit Geldnoten und Münzen. Für kleinere Beträge ist die Barzahlung einfach und unkompliziert. Gibt es Bargeld auch im Internet? Wie muss man sich das vorstellen?

Alice erledigt ihre Bankgeschäfte mit papiernen Formularen, die sie per Post verschickt. Sie verlässt sich auf die Zuverlässigkeit der Post beim Transport der Zahlungsanweisungen. Die Bank kann anhand der Unterschrift prüfen, ob es sich um legitime oder um gefälschte Anweisungen handelt.

Unterdessen bieten viele Banken Online-Banking an. Damit könnte Alice jederzeit auf ihre Konten zugreifen und Transaktionen auslösen. Doch Alice zögert – welche Sicherheiten hat sie beim Online-Banking? Wie wird verhindert, dass Unbefugte auf ihr Konto zugreifen?

Theorie



Elektronische Zahlungssysteme

Elektronische Zahlungssysteme ermöglichen es, Produkte und Dienstleistungen ohne Münzen, Geldscheine oder ein anderes materielles Gut zu bezahlen. «Digitales Geld» ist nichts Neues. Banken beispielsweise kennen den elektronischen Zahlungsverkehr zur Abwicklung von Transaktionen mit anderen Banken seit Jahrzehnten. Auch Bancomaten oder Kreditkarten werden seit langem im Alltag eingesetzt.

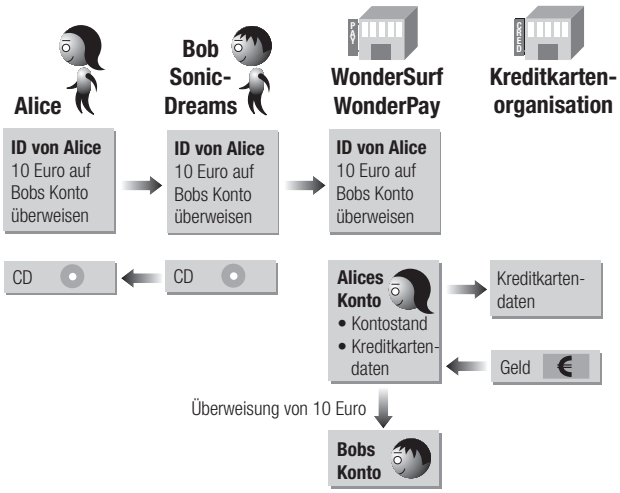
Im Internet gewinnen elektronische Zahlungssysteme zunehmend an Bedeutung. Softwarehersteller vertreiben ihre Programme häufig via Internet und möchten die Bezahlung vorzugsweise auf demselben Weg abwickeln. Verleger von Online-Publikationen sind daran interessiert, bei ihren Kunden einige Pfennige, Rappen oder Cents für das Lesen eines Artikels einzufordern.

Es gibt eine Vielzahl von Ansätzen zur Realisierung von digitalem Geld. Wir präsentieren eine mögliche Kategorisierung in *Kreditkartensysteme*, *Kontensysteme* und *Bargeldsysteme*.

Die drei Kategorien von Zahlungssystemen haben unterschiedliche Vor- und Nachteile, die vom Verwendungszweck abhängen. Kauft Alice beispielsweise ein teures Möbelstück via Internet, so ist die Höhe der fälligen Transaktionsgebühren nicht entscheidend. Zudem muss Alice ihre Wohnadresse für die Auslieferung bekannt geben. Folglich braucht die Bezahlung nicht anonym zu erfolgen. Beim Bezug einer Illustration aus einer Bilddatenbank dagegen sollen möglichst keine Transaktionsgebühren anfallen, und die Bezahlung erfolgt im Idealfall anonym.

Kreditkartensysteme

Kreditkarten werden im Alltag breit eingesetzt für den bargeldlosen Zahlungsverkehr und eignen sich genauso für die Bezahlung von Gütern und Dienstleistungen im Internet. Der Ablauf einer Bezahlung im Internet ist derselbe wie im Alltag.



Alice hat bei `www.sonicdreams.com` eine CD gefunden und zum Kauf ausgewählt. Bei der Bezahlung wird ihr ein Online-Formular präsentiert, in das sie ihren Namen und die Nummer sowie das Ablaufdatum ihrer Kreditkarte eintippt. Anschliessend schickt sie die Informationen zu SonicDreams.

Mit Hilfe der Kartendaten fordert SonicDreams den Betrag für die CD bei der Kreditkartenorganisation ein. Dabei fällt eine Transaktionsgebühr an, die sich häufig aus einer festen Grundgebühr sowie einem gewissen Prozentsatz des Rechnungsbetrags zusammensetzt. Die Transaktionsgebühren gehen zu Lasten des Händlers – die Kreditkartenbesitzer bezahlen in der Regel eine fixe Jahresgebühr.

Um Zahlungen per Kreditkarte entgegenzunehmen und abwickeln zu können, musste sich SonicDreams bei der Kreditkartenorganisation als autorisierter Händler registrieren lassen. Nachdem SonicDreams Alices Zahlungsfähigkeit überprüft hat, wird die bestellte CD ausgeliefert. Alice wiederum erhält zum Monatsende eine Rechnung von der Kreditkartenorganisation. Alternativ kann Alice die ausstehenden Rechungen der Kreditkartenorganisation mittels Lastschriftverfahren begleichen. Beim Lastschriftverfahren werden die fälligen Beträge automatisch von Alices Bankkonto abgebucht.

Der Ablauf eines Einkaufs mit Kreditkarte wurde hier leicht vereinfacht geschildert. Häufig sind neben der Kreditkartenorganisation

auch die Banken von SonicDreams und Alice involviert. Die Kreditkartenorganisation legt dann lediglich die «Spielregeln» fest, nach denen die Banken die Transaktion abwickeln.

Gefahren

Drei Informationen genügen, um Alices Kreditkarte zu belasten: Name der Inhaberin, Kartennummer und Ablaufdatum. Wer diese Informationen kennt, kann mit der Karte von Alice im Internet einkaufen. Deshalb kommt der Übermittlung der Kartendaten grosse Bedeutung zu. Viele Online-Anbieter begegnen diesem Problem, indem sie die verschlüsselte Übertragung mittels SSL unterstützen.

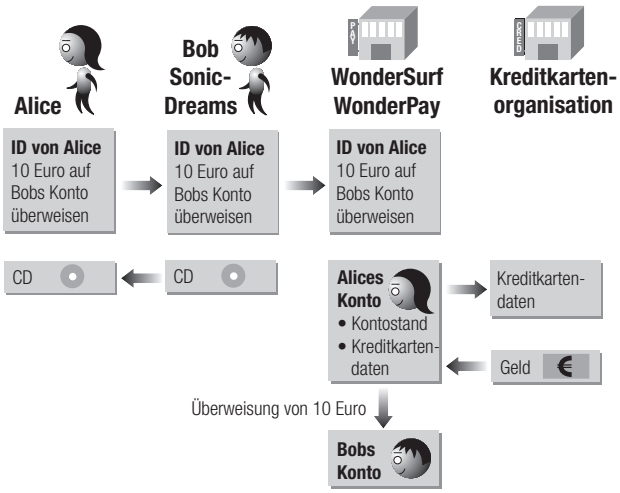
Neben der Übermittlung ist die Lagerung der Kartendaten auf Anbieterseite ein heikler Punkt. Gelingt Unbefugten der Einbruch in das Computersystem eines Online-Anbieters, sind häufig die Kreditkartendaten von tausenden von Kunden in Gefahr. Umsichtige Firmen gewährleisten den Schutz ihrer Datenbestände durch weitreichende Sicherheitsmassnahmen.

Ein weiteres Problem von Kreditkarten ist die fehlende Anonymität. Die Kreditkartenorganisation weiss über die Aktivitäten ihrer Kunden Bescheid. Sie kennt Zeitpunkt, Ort und Grund aller Zahlungen.

Kontensysteme

Kontensysteme setzen eine dritte Stelle voraus, welche die Abwicklung von Transaktionen sowie die Verwaltung der Konten übernimmt. Benutzer eines Kontensystems können für das eigene Konto Schecks ausstellen oder eine Überweisung auf ein anderes Konto veranlassen.

Fiktives Beispiel: Alices Internet-Provider WonderSurf bietet das Kontensystem WonderPay an. Alice benutzt die Dienstleistung und hat sich mit einigen persönlichen Angaben sowie ihren Kreditkartenangaben registrieren lassen. Auch SonicDreams nimmt Zahlungen via WonderPay entgegen. Deshalb existiert ein Konto für Alice und eines für SonicDreams.



Alice kauft bei SonicDreams ein. Bei der Bezahlung identifiziert sich Alice gegenüber SonicDreams – zum Beispiel mit Passwort oder Zertifikat. Anschliessend wird bei WonderPay eine Überweisung von Alices Konto auf das Konto von SonicDreams veranlasst. Zudem wird der Betrag der Kreditkarte von Alice belastet.

Grundsätzlich wird bei einem Kontensystem dieser Art indirekt mittels Kreditkarte bezahlt. Der Umweg über WonderPay hat jedoch einen wichtigen Vorteil: Alices Kreditkartenangaben werden nicht via Internet verschickt, und die Online-Anbieter kennen die Karteninformationen nicht. Dadurch werden die Probleme im Zusammenhang mit der Übermittlung und Lagerung von Kartendaten entschärft.

Ausserdem hat WonderPay die Möglichkeit, Transaktionen auf Alices Konto zusammenzufassen und die fälligen Beträge gesammelt der Kreditkarte zu belasten. Auf diese Weise werden grössere Beträge belastet, und die Transaktionsgebühren fallen weniger ins Gewicht. Kontensysteme eignen sich deshalb für das so genannte *Micropayment* – das Bezahlen von sehr kleinen Beträgen.

Für Alice als Kundin von WonderSurf hat der Dienst WonderPay einen weiteren Vorteil: Sie braucht ihre Einkäufe nicht der Kreditkarte zu belasten, sondern kann sie auf die monatliche Internet-Provider-Rechnung setzen lassen.

Bargeldsysteme

Ein wichtiges Merkmal von Geldnoten und Münzen im Alltag ist die Anonymität. In der Regel kann niemand zurückverfolgen, welche Note von welcher Person wo ausgegeben worden ist. In der Computerwelt wird diese Anonymität zum Beispiel durch digitale Bargeldsysteme gewährleistet.

Wie im Alltag wird neben dem Anbieter und der Kundin eine dritte, unabhängige Stelle benötigt. Das kann eine Firma sein, die ein Bargeldsystem anbietet. Die Firma – nennen wir sie NetCash – stellt digitale Münzen – NetCoins – aus und bürgt dafür.

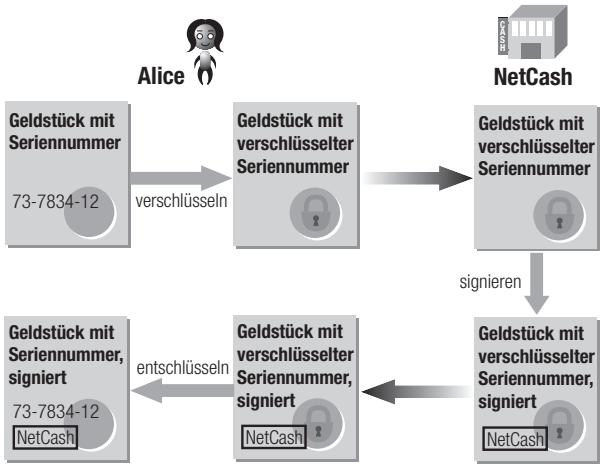
Alice schreibt sich bei NetCash als Kundin ein und eröffnet gleichzeitig ein Konto bei NetCash, über das ihre Transaktionen abgewickelt werden. Alice erhält eine elektronische Geldbörse. Dabei handelt es sich um ein Programm, das den Bezug, die Verwaltung und die Übermittlung der NetCoins erledigt.

Digitales Bargeld erstellen

Alice füllt ihre Geldbörse mit einer Menge von NetCoins. Dazu erstellt sie die gewünschte Menge von NetCoins, die alle mit einer Seriennummer ausgestattet sind. Damit sind die NetCoins aber noch nicht gültig, denn niemand bürgt dafür. Deshalb werden die digitalen Geldstücke verschlüsselt und an die Firma NetCash verschickt.

NetCash empfängt die Münzen und belastet den entsprechenden Betrag auf dem Konto von Alice. Anschliessend werden die NetCoins digital unterschrieben und somit als gültig erklärt. NetCash schickt dann die Münzen zurück. Von Alices elektronischer Geldbörse werden die Münzen entschlüsselt und abgespeichert.

Wichtig: NetCash hat die Seriennummer der NetCoins nicht erfahren, weil sie beim Unterschreiben verschlüsselt waren. In der Fachsprache wird dieses Unterschreiben eine *blinde Signatur* genannt. Dahinter verbirgt sich ein kompliziertes kryptografisches Verfahren, das hier nicht weiter erläutert werden soll. Entscheidend ist, dass NetCash digitale Geldstücke unterzeichnen und damit beglaubigen kann, ohne deren Seriennummer zu kennen.



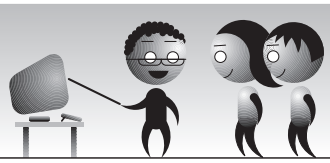
Digitales Bargeld ausgeben

Ein weiteres Mal kauft Alice bei SonicDreams ein. Die NetCash-Software bei SonicDreams sendet eine Zahlungsaufforderung an die elektronische Geldbörse auf Alices Rechner. Nachdem Alice die Zahlung akzeptiert hat, wird die notwendige Anzahl NetCoins abgebucht und an SonicDreams geschickt.

SonicDreams schickt die NetCoins sogleich weiter an NetCash zur Überprüfung. NetCash kontrolliert zunächst, ob die digitale Unterschrift der Münzen intakt ist. Im Anschluss daran werden die Seriennummern der NetCoins registriert. Alle Seriennummern sämtlicher jemals ausgegebenen NetCoins werden aufgezeichnet. So kann NetCash prüfen, ob eine Münze ein zweites Mal ausgegeben wird, was natürlich nicht zulässig ist.

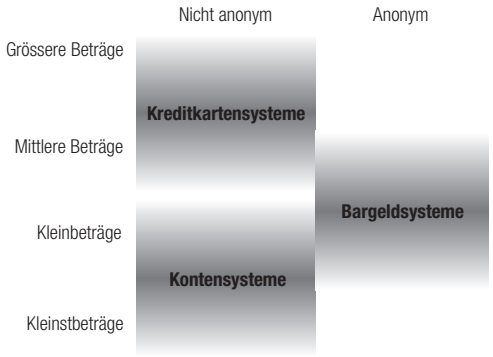
Sind die NetCoins in Ordnung, werden sie dem SonicDreams-Konto bei NetCash gutgeschrieben. Alice erhält von SonicDreams eine Bestätigung über den erfolgreichen Eingang der Zahlung. NetCash kennt nun zwar die Seriennummer der NetCoins, kann diese aber nicht mit Alice in Verbindung bringen.

Praxis



Elektronische Zahlungssysteme im Überblick

Drei Klassen von elektronischen Zahlungssystemen wurden vorgestellt: Kreditkarten-, Konten- und Bargeldsysteme. Alle Systeme haben ihre Vor- und Nachteile. Manche eignen sich für grössere Beträge, andere für kleine Zahlungen für einen Zeitungsartikel oder Ähnliches. Einige Systeme gewährleisten Anonymität, während andere jede Zahlung genau aufzeichnen.



Nach wie vor ist die Kreditkarte das am weitesten verbreitete Zahlungsmittel im Internet. Eine Vielzahl von Firmen bieten Variationen der anderen Techniken an, doch konnte sich bisher keine der Alternativen im grossen Stil durchsetzen. Die fehlende Akzeptanz hat zwei wichtige Gründe: (1) Kreditkarten sind aus dem Alltag gut bekannt. Sehr viele Leute sind bereits im Besitz einer Kreditkarte. (2) Für die Bezahlung mittels Kreditkarte müssen die Kunden keine zusätzliche Software auf ihren Rechnern installieren.

Smart Cards

Smart Cards sind herkömmliche Plastikkarten, die mit einem Mikroprozessor ausgestattet sind. Der Mikroprozessor eignet sich beispielsweise zur Speicherung von Zertifikaten inklusive Public und Private Key.

Smart Cards können aber auch als elektronische Bargeldsysteme eingesetzt werden. Die Karte wird über ein Bankkonto mit einem bestimmten Betrag geladen. Danach kann der gespeicherte Betrag wie herkömmliches Bargeld ausgegeben werden.

Der Einsatz von Smart Cards setzt das Vorhandensein eines Kartenlesers voraus. Im Alltag sind beispielsweise manche Getränkeautomaten oder Parkuhren mit einem Kartenleser ausgerüstet. Für die Bezahlung im Internet muss der jeweilige Computer über einen Kartenleser verfügen.

Smart Cards haben den Sicherheitsvorteil, dass die darauf gespeicherten Informationen nur schwer veränderbar sind. Nachteilig dagegen ist die enge Verwandtschaft mit alltäglichem Bargeld: Geht die Karte verloren, kann der Finder das Geld problemlos ausgeben.

Online-Banking

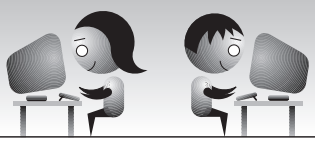
Viele Banken bieten Online-Banking als Dienstleistung an. Die häufigsten Bankgeschäfte wie Zahlungsverkehr oder Börsentransaktionen lassen sich beim Online-Banking bequem am eigenen Rechner erledigen.

Die potenziellen Risiken beim Online-Banking sind gross. Entsprechend hoch werden deshalb die Sicherheitsanforderungen angesetzt. Wichtig ist beispielsweise die Zugriffskontrolle. Viele Banken identifizieren ihre Benutzer durch eine Vertrags- oder Kundennummer und den Einsatz von PINs, Passwörtern, Streichlisten, SecurID-Codes oder Zertifikaten.

Umgekehrt muss sich das Online-Banking-System gegenüber dem Kunden identifizieren können. Das geschieht mit digitalen Zertifikaten. Dadurch erhalten die Kunden die Möglichkeit, die Echtheit des Systems zu überprüfen.

Neben der Zugriffskontrolle ist die Vertraulichkeit der übermittelten Informationen von Bedeutung. Deshalb kommen Verschlüsselungstechniken mit langen Schlüsseln zum Einsatz. Manche Online-Banking-Systeme verwenden den Web-Browser für die Kommunikation, andere Systeme setzen die Installation von spezieller Software auf Kundenseite voraus.

Anwendung



Dem Zahlungsverkehr im Internet steht grundsätzlich nichts mehr im Weg. Ob grosse oder kleine Beträge – für alle Transaktionen gibt es geeignete technische Lösungen. Leider sind die Lösungen von Anbieter zu Anbieter, von Land zu Land verschieden und kaum standardisiert. Häufig muss Zusatzsoftware installiert werden, was Alice als Anwenderin wenig sympathisch ist. Der Eindruck von Alice: Zahlungsverkehr im Internet ist noch nicht ausgereift. Auf digitales Kleingeld und ähnliche Dinge verzichtet Alice deshalb vorderhand. Sie wartet ab, bis einfachere Systeme Einzug halten und bis sich standardisierte Techniken etablieren.

Mit ihrer Hausbank hat Alice einen Online-Banking-Vertrag abgeschlossen. Nun ist sie ausgerüstet mit der Zugangssoftware, einem Passwort sowie einer SecurID-Karte. Nach anfänglichen Problemen mit der Installation der Software funktioniert das Online-Banking bestens. Alice kann sich jederzeit einen Überblick über die Aktivitäten auf ihrem Konto verschaffen und ihre Zahlungen via Internet erledigen. Dadurch kann sie etwas Zeit sowie einen Teil der Transaktionsgebühren sparen.

Die Kreditkarte ist für Alice nach wie vor die bequemste und verbreitetste Variante zur Bezahlung von Dienstleistungen und Gütern im Netz. In diesem Zusammenhang achtet sie auf zwei Dinge: (1) Sie verschickt die Kreditkartendaten ausschliesslich in verschlüsselter Form, zum Beispiel über eine SSL-Verbindung. (2) Alice tritt den Online-Shops mit einer gesunden Portion Misstrauen gegenüber. Sie schickt ihre Angaben nur an möglichst vertrauenswürdige Web-Sites. Immerhin besteht bei unseriösen Sites die Gefahr, dass die Kartendaten missbraucht oder nur ungenügend geschützt gelagert werden.

Allenfalls können weitere Massnahmen getroffen werden: Alice kann zwei Kreditkarten verwenden. Die eine Karte hat eine hohe Limite. Alice benutzt sie im Alltagsleben, wenn sie selber bei der Bezahlung anwesend ist. Die andere Karte hat eine sehr tiefe Limite. Diese Karte benutzt Alice vor allem im Internet. So ist bei einem allfälligen Missbrauch zumindest der finanzielle Verlust begrenzt.

Kapitel 6

Spuren im Netz

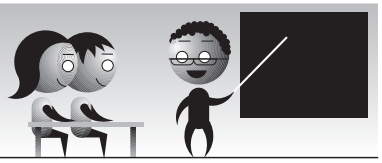
Alice surft häufig während der Arbeitszeit im Netz. Dabei kann sie der Versuchung nicht widerstehen, ab und zu auch einen Link anzuklicken, der nichts mit ihrer Arbeit beim *Backstreet Journal* zu tun hat. Zum Beispiel verfolgt sie regelmässig die Kurse eines Anlagefonds, und auch Online-Einkäufe tätigt sie gerne vom Arbeitsplatz aus. Zwischendurch zieht es Alice in einen Chatroom. Besonders hochstehend sind die Diskussionen dort zwar nicht, aber als Abwechslung ...

Ein Arbeitskollege von Alice hat kürzlich in der Pause erzählt, das *Backstreet Journal* sei aus Gründen der Effizienz und der Sicherheit über einen so genannten Proxy-Server ans Internet angeschlossen. So könne exakt Buch geführt werden, welche Web-Seiten die Mitarbeiter abrufen. Im dritten Stock hätte ein Journalist sogar die Kündigung angedroht erhalten, weil er während seiner Arbeitszeit öfters Web-Seiten mit pornografischem Inhalt aufgerufen habe. Alice ist verunsichert: Können ihre Aktivitäten im Internet tatsächlich so gut überwacht werden? Und was ist ein Proxy-Server?

Beim Einkaufen im Netz fällt Alice immer wieder auf, dass die von ihr aufgerufenen Seiten meistens auf ihre persönlichen Vorlieben zugeschnitten sind. Bei AllBooks werden immer gleich die Neuerscheinungen aus dem Bereich «Reisen in südamerikanischen Ländern» angeboten – das sind Alices Lieblingsdestinationen. Und wenn sich Alice bei AllBooks mit ihrem Passwort identifiziert, erscheinen im Bestellformular persönliche Daten wie Lieferadresse oder Zahlungsmodus. Das ist bequem und stört Alice nicht weiter. Nur: Warum weiss AllBooks auch, dass sie gestern lange nach einem Buch zum Töpferhandwerk auf Bali gesucht hat? Es kann doch kein Zufall sein, dass ihr heute als Sonderangebote speziell Bücher über Bali angeboten werden.

Bei Bob zu Hause hat Alice festgestellt, dass es oft genügt, wenn sie nur die ersten Buchstaben einer früher aufgerufenen Adresse eintippt. Der Browser bei Bob scheint ein «Gedächtnis» zu haben. Gibt Alice die Adresse `www.dirtyjokesaboutmen.com` ein, vervollständigt der Browser die Adresse bereits, wenn sie erst `www.dirt` eingetippt hat. Kann Bob etwa herausfinden, auf welchen Seiten Alice jeweils herumsurft?

Theorie



Surfen im Netz hinterlässt Spuren

In den letzten Kapiteln ging es unter anderem darum, wie man im Internet Personen identifiziert. Zu diesem Zweck werden beispielsweise Zertifikate, Passwörter oder SecurID-Karten eingesetzt. Doch die Identifikation von Personen hat auch ihre Schattenseiten. Bei der Internet-Benutzung möchte man nicht immer identifiziert werden können, sondern häufig anonym bleiben und seine Privatsphäre wahren. Das Spannungsfeld zwischen unerwünschter und notwendiger Identifikation bildet den Hintergrund für dieses Kapitel.

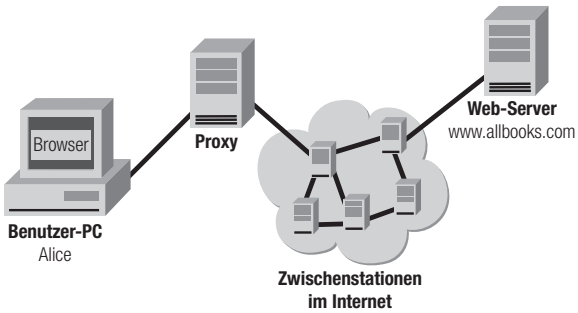
So viel vorweg: Im Internet ist man nur selten anonym. Ausserdem ist das Internet kein rechtsfreier Raum. In der Regel kann jede Aktivität mit genügend Aufwand zum Urheber zurückverfolgt werden, denn eine Benutzerin wie Alice hinterlässt an jeder «virtuellen Ecke» ihre Spuren. Einige dieser Spuren stellen wir in den folgenden Abschnitten vor. Doch zunächst ein paar Worte zum Ursprung dieser Spuren.

Vom Browser zum Server und zurück

Alice befindet sich auf einer ihrer Rundreisen im World Wide Web. Dabei schaut sie auch auf Bobs Web-Site SonicDreams vorbei und stösst auf eine Web-Seite über ihren Lieblingskomponisten: John Cage. Innerhalb der Seite erscheint ein Hyperlink auf die Biografie von Cage, die man im Online-Buchladen AllBooks kaufen kann. Alice wählt den Link an. Was geschieht?

Der Web-Browser auf Alices Computer registriert, dass Alice den Link angewählt hat. Die gewünschte Adresse lautet `http://www.allbooks.com/biographies/jcage.html`. Also schickt der Browser

eine entsprechende Anfrage ins Internet. Bei Privatbenutzern gelangt die Anfrage zunächst zum Internet-Provider, wo ein bestimmter Rechner – der *Proxy* – für die Kommunikation zwischen den Benutzerrechnern und den Rechnern im Internet zuständig ist. Der Proxy reicht die Anfrage anhand der Zieladresse an eine passende Zwischenstation im Internet weiter. Anschliessend «hüpft» die Anfrage von einer Station zur nächsten, bis sie beim Web-Server von AllBooks ankommt.



Nun nimmt der Web-Server die Anfrage in Empfang. Falls die verlangte Web-Seite existiert, wird in der Folge eine entsprechende Antwort zusammengestellt. Diese Antwort enthält in erster Linie den Inhalt der von Alice angeforderten Web-Seite. Ausserdem wird die Antwort mit der Adresse von Alices Computer ausgestattet. Diese Adresse wurde mit der Anfrage mitgeschickt und ist natürlich unverzichtbar, sonst findet die Antwort den Weg zu Alices Computer nicht.

Sobald die Antwort bereitsteht, schickt sie der Web-Server ins Internet in Richtung Proxy-Server bei Alices Internet-Provider. Der Proxy-Server leitet die Antwort weiter an Alices Rechner, wo der Browser die Informationen entgegennimmt und die Web-Seite auf dem Bildschirm darstellt.

Das sind die wichtigsten Schritte bei der Kommunikation eines Web-Browsers mit einem Web-Server. Neben den beiden offensichtlichen Kommunikationspartnern Browser und Server sind weitere Systeme bei der Übermittlung von Daten beteiligt: zum Beispiel die

Zwischenstationen im Internet oder – je nach Internet-Anbindung – der Proxy-Server beim Internet-Provider. All diese Systeme «sehen» natürlich die Daten, die sie übermitteln. Dieses Grundverständnis ist wichtig, um zu erkennen, wo man als Benutzer seine Spuren im Internet hinterlässt. Wir werden nun einige «Brennpunkte» genauer betrachten.

Aufzeichnungen im Web-Server: die Log-Datei

Web-Server vermerken jeden Zugriff auf eine Web-Seite in einer Datei, der so genannten *Log-Datei*. In der Log-Datei wird zum Beispiel festgehalten, von welchem Rechner die Anfrage stammt und welches Objekt verlangt wird. Auch die Zeit des Zugriffs wird vermerkt.

Die Log-Datei des Web-Servers unter `www.allbooks.com` könnte wie folgt aussehen:

```
president.whitehouse.gov [01/Jul/1999:05:10:17]
      ''GET /authors/camus.html HTTP/1.0''
      ''http://www.allbooks.com/books/authors/all.html''
194.231.42.178 [01/Jul/1999:05:10:23]
      ''GET /books/new/houellebecq.html HTTP/1.0''
      ''http://www.allbooks.com/new.html''
proxy.wondersurf.com [01/Jul/1999:05:11:34]
      ''GET /biographies/jcage.html HTTP/1.0''
      ''http://www.sonicdreams.com/composers/johncage.html''
```

Der Ausschnitt zeigt drei Anfragen an den Server. Zur Erläuterung der Einträge müssen einige Fachbegriffe geklärt werden:

- *IP-Adressen:* Jeder Rechner im Internet muss über eine weltweit eindeutige Adresse verfügen, sonst können die Millionen von Rechnern nicht miteinander kommunizieren. IP-Adressen bestehen aus vier Zahlen, die zwischen 1 und 255 liegen – zum Beispiel 194.231.42.178. Die Länge der IP-Adressen ist allerdings nicht zwingend. In Zukunft werden allmählich längere Adressen eingeführt, um dem steigenden Bedarf gerecht zu werden.

Manche Rechner verfügen über fest zugeteilte IP-Adressen. Dazu zählen beispielsweise alle Server sowie viele Benutzerrechner, die eine ständige Verbindung ins Internet unterhalten. Heimanwender, die sich mittels Modem beim Internet-Provider einwählen, erhalten beim Verbindungsaufbau eine temporäre IP-Adresse zugeteilt. Diese Adresse kann mit jedem Einwählen ändern. Man spricht von *dynamischen IP-Adressen*.

- *Host-Namen:* IP-Adressen sind ideal für Computer, aber Menschen können sich die Zahlenfolgen nur schlecht merken. Aus diesem Grund gibt es ein zweites System, um Rechner im Internet zu identifizieren: die *Host-Namen*. Bei Alices Internet-Provider zum Beispiel gibt es einen Web-Server mit dem Namen `www.wondersurf.com`. Dabei ist `www` der eigentliche Name des Servers und `wondersurf.com` die Domain, in der sich der Server befindet. Neben dem Web-Server sind weitere Server auf diese Weise mit einem Namen ausgestattet: Der Proxy-Server heisst `proxy.wondersurf.com` und der Mail-Server entsprechend `mail.wondersurf.com`.

  Im Zusammenhang mit IP-Adressen und Host-Namen ist ein Grundsatz wichtig: Jeder Rechner im Internet muss zwingend über eine IP-Adresse verfügen. Die IP-Adresse ist eine aus technischer Sicht notwendige Voraussetzung für die Kommunikation. Die Host-Namen hingegen sind vor allem für die menschlichen Benutzer des Internets eingeführt worden. Längst nicht jeder Rechner im Internet verfügt über einen Host-Namen. Deshalb taucht in der Beispiel-Log-Datei ein Eintrag ohne Host-Namen auf.

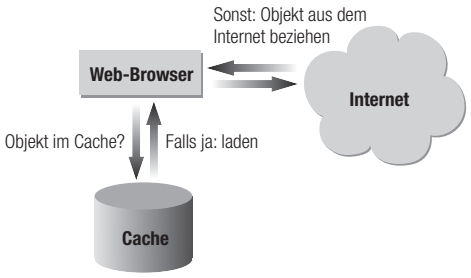
- *Referer:* Der *Referer* hält fest, von welcher Web-Seite die jeweilige Benutzerin auf die aktuelle Seite gelangt ist. Somit ist der Server bestens informiert, auf welcher Seite eine Benutzerin zuvor war. Die Referer-Informationen sind nützlich, um beispielsweise die Effektivität von Online-Werbung abzuschätzen. Betreiber von Web-Angeboten können damit allerdings auch ein detailliertes Verhaltensprofil ihrer Benutzer erstellen.

Kommen wir zurück auf das oben gezeigte Beispiel einer Log-Datei. Der erste Eintrag zeigt, wie jemand vom (erfundenen) Rechner des US-Präsidenten zunächst die Liste mit allen Autoren bei AllBooks betrachtet und sich dann für Albert Camus entscheidet. Im zweiten Eintrag schaut sich jemand von einem Rechner mit der IP-Adresse `194.231.42.178` die Liste der Neuerscheinungen an und wählt daraus das neue Werk von Michel Houellebecq. Der letzte Eintrag zeigt Alice, die via SonicDreams zur Biografie von John Cage gelangt. Hier wird nicht Alices eigener Rechner registriert sondern der Proxy-Server ihres Internet-Providers. Der Grund: Alices Computer kommuniziert eigentlich nur mit dem Proxy. Der Proxy wiederum stellt eine separate Anfrage an den jeweiligen Web-Server.

Surfgeschichten: Cache und History

Die Log-Dateien eines Web-Servers sind ein möglicher Ort, an dem ein Internet-Benutzer seine Spuren hinterlässt. Doch man muss gar nicht so weit gehen. Auch auf dem eigenen Rechner sammeln sich Spuren an. Zum Beispiel im lokalen *Cache* auf der Festplatte.

Der Cache funktioniert als Zwischenspeicher. In diesem Zwischenspeicher legt der Web-Browser Objekte ab, die er aus dem Internet bezieht. Meistens handelt es sich bei den abgelegten Objekten um einzelne Bilddateien oder um ganze Web-Seiten.



Der Vorteil: Bevor eine Web-Seite oder ein Bild aus dem Internet angefordert wird, schaut der Browser im Cache nach. Vielleicht ist

das gewünschte Objekt im Cache bereits vorhanden – dann wird es sofort dargestellt. Andernfalls lädt der Browser das Bild oder die Seite wie gewohnt aus dem Internet. So erklärt sich die hohe Geschwindigkeit beim erneuten Laden von Seiten, die man erst kürzlich betrachtet hat. Der Cache ist immer dann nützlich, wenn sich gewisse Gestaltungselemente innerhalb einer Web-Site wiederholen. Das ist beispielsweise bei Firmenlogos oder bei grafischen Auswahlmenüs der Fall.

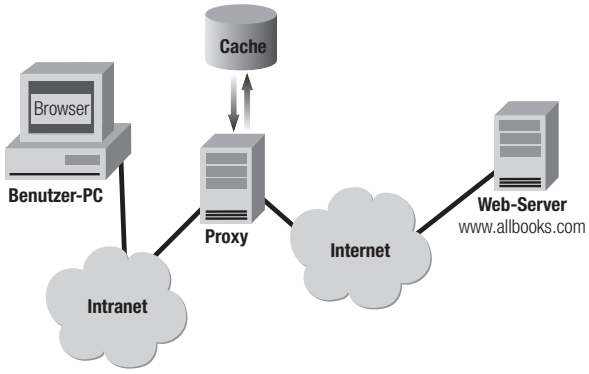
Die Objekte verweilen so lange im Cache, bis sie durch neuere Versionen oder durch gänzlich andere Objekte ersetzt werden. Das Überschreiben von Objekten ist nötig, um eine vorgegebene Maximalgrösse des Caches einzuhalten.

Trotz des Überschreibens sind in einem typischen Cache viele Web-Seiten und Bilder gespeichert. Dieser Umstand wird immer dann zum Problem, wenn beispielsweise Alice ihren Arbeitsplatzrechner sowie dasselbe Benutzerprofil mit einem oder mehreren Arbeitskollegen teilt. Mit Hilfe des Caches können sich die Kollegen nämlich ein Bild von Alices Reisen im Internet machen. Das Problem ist auch bei der Benutzung von Rechnern an einem öffentlich zugänglichen Ort – zum Beispiel in einer Bibliothek oder im Internet-Café – von Bedeutung.

Darüber hinaus gibt es noch einen weiteren Weg, die Surftouren anderer Benutzer desselben Browsers im Nachhinein in Erfahrung zu bringen: Die meisten Browser zeichnen die Adressen aller besuchten Web-Seiten in einer Liste mit dem Namen *Verlauf* oder *History* auf. Die Liste hilft Benutzern, eine schon besuchte Web-Seite rasch wiederzufinden. Die Liste ist zudem nützlich bei der automatisierten Vervollständigung von nur teilweise eingetippten URLs im Adressfeld des Browsers. Allerdings kann dieselbe Liste grundsätzlich auch von Dritten untersucht werden.

Nützliche Zwischenhändler: Proxy-Rechner

Die meisten Anwender benutzen das Internet weder vom privaten PC noch vom Arbeitsplatzrechner über eine direkte Verbindung. Stattdessen werden alle Verbindungen über eine Zwischenstation geleitet. Diese Zwischenstation heisst *Proxy-Server* oder kurz *Proxy*.



Ein Proxy hat für Benutzerinnen wie Alice vor allem einen Vorteil: Der Proxy merkt sich die Seiten, die er einmal heruntergeladen hat, inklusive Inhalt, Bildern usw. Wenn die Benutzerin auf ein zwischengespeichertes Objekt – beispielsweise ein Bild oder eine Web-Seite – zugreift, muss das Objekt nur noch vom Proxy übermittelt werden anstatt vom ursprünglichen Web-Server. Oft erfolgt die Übertragung dadurch schneller. Der Proxy arbeitet also wie ein Cache. Das funktioniert selbst dann, wenn andere Benutzer derselben Firma oder des gleichen Internet-Providers auf den Proxy zugreifen.

Ein Proxy-Server birgt aber auch problematische Aspekte für die Benutzer in sich. Der Proxy-Server protokolliert üblicherweise sämtliche Benutzeranfragen. Mit Hilfe dieser Angaben lässt sich detailliert das Verhalten der Benutzer verfolgen. Aus Sicht des Datenschutzes ist das heikel. In einer Firma beispielsweise kann mit Hilfe eines Proxys der gesamte Datenverkehr zwischen Internet und dem firmeninternen Netzwerk – *Intranet* genannt – mitgeschnitten werden. Anhand der Aufzeichnungen kann geprüft werden, ob die Mitarbeiter das Internet vor allem für die Arbeit einsetzen oder in erster Linie für private Zwecke.

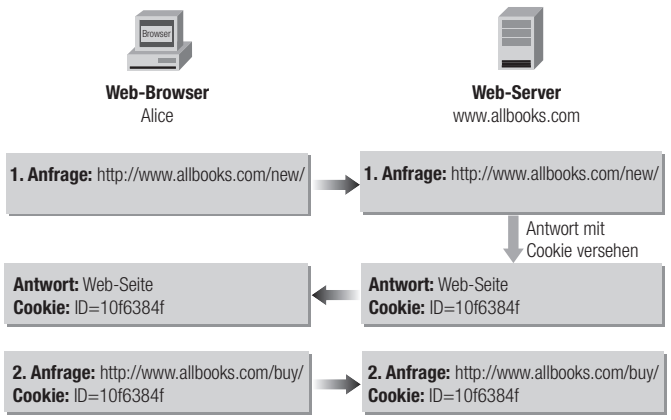
Der Proxy hat in seiner Rolle als Zwischenhändler neben der Geschwindigkeitssteigerung einen weiteren Vorteil. In den Log-Daten der angesprochenen Web-Server taucht nur noch der Proxy als anfragender Rechner auf. Die Benutzerrechner stellen ihre Anfragen an den Proxy und sind im Internet nicht mehr direkt sichtbar. Damit

können Betreiber von Web-Servern ihre Anfragen nicht zu einem spezifischen Benutzerrechner zurückverfolgen, sondern lediglich zum gemeinsamen Proxy-Server einer Firma oder eines Internet-Providers.

Informationsspeicher Cookies

Ein Web-Server hat die Möglichkeit, auf dem Benutzerrechner Informationen abzuspeichern. Damit kann der Server beispielsweise einen Benutzer bei jedem Besuch wiedererkennen, denn die gespeicherten Informationen werden vom Browser des Benutzers mit jeder Anfrage an den Server zurückgeschickt.

Der Ablauf: Der Benutzer stellt eine Anfrage für eine bestimmte Web-Seite an den Web-Server. Daraufhin schickt der Server die verlangte Web-Seite zurück und fügt der Antwort gleichzeitig eine kleine Informationseinheit an. Diese Informationseinheit wird *Cookie* genannt. Der Browser nimmt das Cookie zusammen mit der Web-Seite entgegen und speichert es in einer Datei ab.



Eine Eigenschaft von Cookies ist wichtig: Sie werden in einer Datei abgelegt und stehen damit permanent zur Verfügung. Das heisst, wenn der Benutzer Tage später die Web-Site erneut besucht, wird das Cookie normalerweise nach wie vor zum Server geschickt.

Die Cookies-Datei ist eine normale Textdatei, die man sich als Benutzer anschauen kann. Es lässt sich mitverfolgen, wie viele und welche Cookies auf der Festplatte abgelegt sind. Die Datei könnte vereinfacht wie folgt aussehen:

```
.allbooks.com      ID=10f6384f
.sonicdreams.com   Username=Alice
.wondersurf.com    81DC6131-8761-67D9-CFFD
```

Mit Hilfe von Cookies lassen sich fast beliebige Informationen abspeichern. Im obigen Fall etwa wird bei jeder Anfrage an einen Server in der Domain `sonicdreams.com` der Benutzername «Alice» mitgeschickt. Meistens unterhalten Online-Angebote allerdings eine Datenbank mit allen gesammelten Benutzerdaten, während im Cookie lediglich eine Benutzeridentifikation – zum Beispiel die Kundennummer – gespeichert wird. Im Beispiel ist das die Identifikation «10f6384f» für die Domain `allbooks.com`. Bei einer Anfrage wird in der Datenbank nachgeschaut, um welchen konkreten Benutzer es sich handelt.

Wo liegen die Vor- und Nachteile von Cookies? Auf der einen Seite machen Cookies den Benutzern von Online-Angeboten das Leben leichter. Ohne Cookies muss Alice bei jeder Buchbestellung bei AllBooks sämtliche benötigten Angaben wie Lieferadresse oder Zahlungsart neu eingeben. Mit Hilfe von Cookies dagegen fällt diese Tipparbeit weg. Alice gibt ihre Angaben nur einmal ein. Anschliessend landen die Informationen in einer Datenbank, und auf Alices Rechner wird ein Cookie gesetzt. Fortan kann AllBooks Alice bei jedem Besuch erkennen und die entsprechenden Informationen aus der Datenbank heraussuchen.

Auf der anderen Seite weisen Cookies durchaus problematische Aspekte auf: Für Web-Angebote ist es von grossem Vorteil, wenn die Benutzer bei jedem Besuch wiedererkannt werden. So können beispielsweise umfangreiche Datenbanken mit den Vorlieben, Abneigungen und Einkaufsgewohnheiten der Besucher aufgebaut werden. Die Benutzer sind folglich vor die Wahl gestellt zwischen Bequemlichkeit und dem Verlust von Anonymität und Privatsphäre.

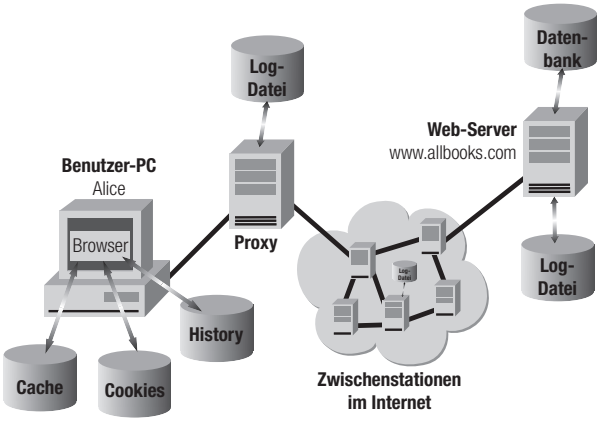
Benutzerkonten

Zum Thema Komfort kontra Datenschutz gehören auch diejenigen Online-Angebote, die über getrennte Konten für jeden Benutzer verfügen. Ein Web-Server benötigt nicht unbedingt Cookies, um seine Besucher zu identifizieren. Es genügt auch ein anderes eindeutiges Merkmal – zum Beispiel eine E-Mail-Adresse oder ein Benutzername, vielleicht inklusive Passwort für den Zugriffsschutz.

Oft muss man im WWW auch bei kostenfreien Angeboten ein Benutzerkonto einrichten. Mit Hilfe solcher Konten werden Benutzer identifiziert, um die getätigten Zugriffe zu registrieren und wiederum in einer Datenbank zu sammeln.

Spuren im Web: ein Überblick

Die vorhergehenden Abschnitte präsentierten eine kurze Rundreise zum Thema «Spuren im Web». Eine Auswahl von Brennpunkten auf dem Weg zwischen Web-Browser und Web-Server wurden vorgestellt. Nun wird es Zeit für einen zusammenfassenden Überblick:

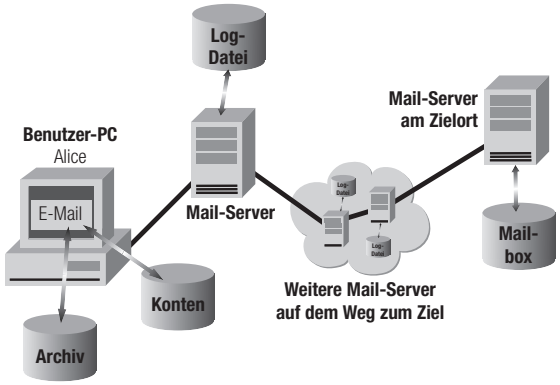


Bei der Kommunikation im WWW (und im Internet allgemein) sind in aller Regel nicht nur die beiden Kommunikationspartner – zum Beispiel Browser und Server – beteiligt. Stattdessen haben eine ganze Reihe von Zwischenstationen ebenfalls «die Hand im Spiel». Es kostet nahezu keinen Aufwand, in diesen Zwischenstationen den abgearbeiteten Datenverkehr aufzuzeichnen. Speicherplatz ist typischerweise im Übermass vorhanden. Die meisten Rechner im Internet führen Log-Dateien, mit deren Hilfe sich ein Grossteil der Aktivitäten zur jeweiligen Benutzerin rückverfolgen lassen.

Zu den Log-Dateien kommen andere Formen von Aufzeichnungen: Auf Serverseite sind das Datenbanken mit mehr oder weniger weit reichenden Benutzerdaten. Auf Browserseite werden im Cache vollständige Web-Objekte, in der History die besuchten URLs und in der Cookies-Datei typischerweise Benutzeridentifikationen abgelegt.

Internet ist nicht nur WWW: E-Mail-Spuren

Bisher haben wir uns ausschliesslich mit dem World Wide Web beschäftigt. Aber das Internet stellt weitere Dienste zur Verfügung: allen voran E-Mail. Auch E-Mails hinterlassen Spuren. Diesbezüglich besteht kein grosser Unterschied zwischen dem Abrufen von Web-Seiten oder dem Versenden von E-Mails.

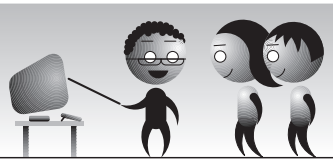


Beispielszenario: Alice sitzt an ihrem Rechner. Darauf läuft ein E-Mail-Programm, mit dem Alice eine Nachricht an Bob verfasst. Sie schickt die E-Mail ab. Dann geschehen zwei Dinge: Das E-Mail-Programm speichert die Nachricht in einem lokalen Archiv auf dem Rechner. Ausserdem wird die Nachricht an den Mail-Server bei Alices Internet-Provider WonderSurf geschickt. Der Mail-Server nimmt die Mail entgegen und leitet sie weiter. Nun «hüpft» die Mail von Server zu Server, bis sie schliesslich in Bobs Mailbox bei seinem Mail-Server landet.

Alle betroffenen Mail-Server können je nach Konfiguration Log-Dateien unterhalten, in denen der Weg der E-Mail aufgezeichnet wird. Der Weg einer E-Mail wird in den so genannten *Header-Einträgen* festgehalten. Ein allzu neugieriger Administrator bei einem der beteiligten Server könnte sogar «mithören» und die ankommenden Mails vor dem Weitersenden lesen. Das gilt genauso für den E-Mail-Verkehr in einem Firmenintranet, der ebenfalls über einen (firmeneigenen) Mail-Server abgewickelt wird.

Es lauern weitere Gefahren auf dem Benutzerrechner: Im Archiv werden alle verschickten oder empfangenen Mails abgelegt. Zudem speichert das E-Mail-Programm die benutzerspezifischen Angaben – Adresse des Mail-Servers, Benutzername und vielleicht sogar das Passwort – in einem Benutzerkonto. Das ist problematisch, wenn man seinen Rechner mit anderen Personen teilt oder seine Mails von einem öffentlich zugänglichen Computer abruft oder verschickt. Unter Umständen erhalten Unbefugte auf diese Weise Zugriff auf die eigene Mailbox.

Praxis



Was der Browser dem Server verrät

Alice findet bei SonicDreams einen Verweis auf eine Biografie von John Cage bei AllBooks. Mittels Mausklick weist sie ihren Browser an, die Seite bei AllBooks herunterzuladen. Als Reaktion schickt der Browser eine entsprechende HTTP-Anfrage an den Web-Server bei AllBooks. Das folgende Beispiel zeigt, wie ein Ausschnitt aus einer solchen Anfrage aussehen könnte:

```
GET /biographies/jcage.html HTTP/1.0
Referer: http://www.sonicdreams.com/composers/johncage.html
User-Agent: Mozilla/4.51 [de] (Win98; I)
```

Der Web-Server erfährt aufgrund dieser Anfrage bereits einiges über Alice. Die erste Zeile ist unverzichtbar und gibt Auskunft darüber, welche Web-Seite übermittelt werden soll. Es folgt der Referer-Eintrag, der die zuvor besuchte Web-Seite wiedergibt. Nicht jeder Browser schickt die Referer-Informationen zum Server.

Nach der Referer-Information wird vermerkt, welcher Web-Browser die Anfrage stellt. In derselben Zeile stehen die Browser-Version, die Sprache des Browsers sowie das Betriebssystem, das auf dem Client-Rechner benutzt wird.

Zusätzlich zu den Informationen aus der HTTP-Anfrage erkennt der Web-Server, von welchem Rechner die Anfrage stammt. In unserem Beispiel ist das der Proxy-Rechner bei WonderSurf mit der Adresse `proxy.wondersurf.com`.

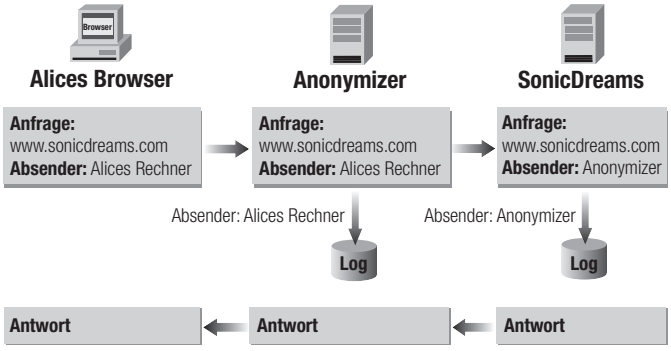
Internet-Spuren verwischen

Alice getraut sich kaum mehr ins Internet. Überall hinterlässt sie eine Datenspur – lokal auf ihrem Rechner, beim Provider und auf den Web-Servern. Leider kann Alice nicht gegen alle Spuren etwas unternehmen. Beispielsweise lässt sich nicht verhindern, dass die Rechner im Internet Log-Daten aufzeichnen. Trotzdem gibt es das eine oder andere Mittel zum Schutz vor unerwünschten Spuren. Einige davon werden wir hier vorstellen.

Anonym ins Web

Im Internet existieren verschiedene Dienste, die «anonymes» Surfen erlauben. Wir nennen diese Dienste *Anonymizers*. Ein Anonymizer funktioniert nach dem Prinzip eines Proxy-Servers.

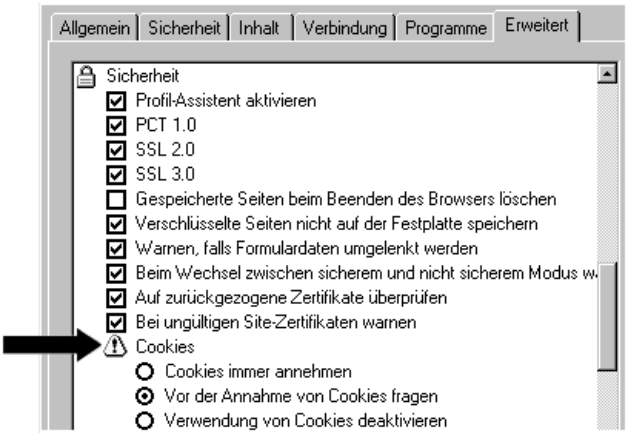
Beispiel: Alice möchte die Web-Seite mit der Adresse `http://www.sonicdreams.com/reviews.html` beziehen. Nun stellt sie diese Anfrage nicht direkt an den SonicDreams-Server, sondern an einen Anonymizer-Dienst. Der Anonymizer fordert die betreffende Seite bei SonicDreams an und leitet sie anschliessend weiter an den Browser von Alice. Der Effekt: In der Log-Datei bei SonicDreams taucht nicht Alices Rechner auf, sondern nur der Anonymizer.



Was gewinnt Alice durch dieses Vorgehen? Leider nicht sehr viel. Der Proxy-Server bei ihrem Internet-Provider beziehungsweise im Firmennetz weiss oftmals nach wie vor, welche Seiten sie abruft. Zudem verlagert sich das Problem lediglich. Zwar kennt der Ziel-Web-Server den Ursprung der Anfragen nicht, dafür verfügt der Anonymizer über alle Informationen. Hinzu kommt, dass Alice Einbussen in Bezug auf die Geschwindigkeit beim Runterladen der Seiten in Kauf nehmen muss, weil die Kommunikation mit dem Web-Server neu über einen Umweg führt.

Die Cookies verkrümeln sich

Bei den meisten Browsern kann Alice beeinflussen, wie Cookies zu behandeln sind. Es stehen verschiedene Möglichkeiten zur Auswahl: Alice kann sämtliche Cookies ohne Rückfrage akzeptieren oder ablehnen lassen. Oder Alice lässt sich bei jedem Cookie warnen, bevor es gesetzt wird. So kann sie bei jeder Web-Seite neu entscheiden, ob sie ein Cookie zulassen möchte oder nicht.



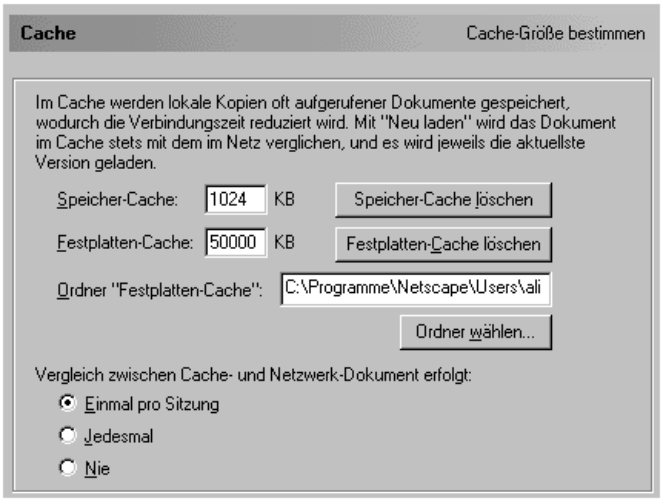
Aber: Das Internet ist voll von Cookies. Ein Grossteil der kommerziellen Web-Sites will mindestens ein oder sogar mehrere Cookies setzen. Bei einem solchen Ansturm wird das manuelle Bestätigen oder Verwerfen jedes einzelnen Datenkrümels rasch zu anstrengend. Deshalb können bei manchen Browsern die Cookies-Einstellungen für spezifische Web-Sites angepasst werden.

Dem Cache an den Kragen

Der Cache speichert alle einmal heruntergeladenen Objekte aus dem Internet für eine bestimmte Zeit. Soll der Browser ein neues Objekt – zum Beispiel eine Web-Seite – aus dem Internet beziehen, schaut er zuerst im Cache nach. Befindet sich das Objekt bereits im Cache, wird es nicht via Netz heruntergeladen. Unter einer Voraussetzung:

Das gleiche Objekt im Internet darf nicht neueren Datums sein. Deshalb erfrägt der Bowser zuerst das Änderungsdatum beim betreffenden Web-Server.

Der Cache ist problematisch, weil man durch die darin gespeicherten Informationen die von einem Benutzer besuchten Web-Seiten in Erfahrung bringen kann. Aus diesem Grund erlauben die meisten Web-Browser das Löschen der im Cache abgelegten Informationen.



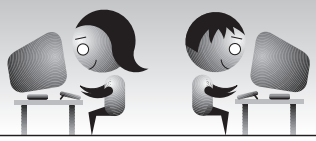
Aus dieser Grafik ist ersichtlich, dass der Zwischenspeicher in zwei Varianten auftreten kann. Der Cache auf der Festplatte bleibt bestehen, auch wenn der Browser heruntergefahren und neu gestartet wird. Der Cache im Hauptspeicher dagegen ist weniger problematisch. Er besteht nur, solange der Browser aktiv ist. Nach dem Herunterfahren gehen die darin gespeicherten Informationen verloren, oder sie werden im Disk-Cache abgelegt. Der Disk-Cache sollte immer dann geleert werden, wenn man seinen Computer mit anderen Benutzern teilt. Auf diese Weise wird das «Spionieren» im Cache stark erschwert.

Weitere Problemzonen im Browser

Die meisten Web-Browser zeichnen in der History die Adressen von besuchten Web-Seiten auf. Das Löschen dieser Liste ist nicht immer einfach. Bei Netscapes Navigator beispielsweise muss man die entsprechende Datei auf der Festplatte suchen und manuell entfernen. Bei Microsofts Internet Explorer lässt sich die «Verlauf» genannte Liste in den Browser-Einstellungen bequem mittels Knopfdruck löschen.

Viele moderne Browser unterstützen Benutzerinnen ausserdem beim Ausfüllen von Online-Formularen. Solche Browser merken sich, auf welcher Web-Seite die Benutzerin welche Informationen eintippt. Das ist bequem, wirft aber auch Probleme auf. Oft werden in Formularen heikle Informationen wie Benutzeridentifikationen und Passwörter eingegeben. Merkt sich der Browser diese Daten, so müssen sie auch irgendwo auf der Festplatte abgespeichert sein. Und was abgespeichert ist, kann mit genügend Aufwand durch Unbefugte aufgefunden und ausgelesen werden. Es kann daher sinnvoll sein, das automatische Ausfüllen von Formularen im Web-Browser zu deaktivieren.

Anwendung



Ob sie will oder nicht, Alice hinterlässt Spuren im Netz. Die Online-Angebote sammeln von Alice mehr Daten als ihr lieb ist. Einerseits kann Alice alle Cookies zurückweisen. Dann wird vielleicht das Einkaufen im Netz zur mühsamen Angelegenheit. Andererseits kann Alice allen Web-Sites das Setzen von Cookies erlauben. Dann bleibt ihre Privatsphäre bald auf der Strecke. Also muss sich Alice überlegen, was ihr wichtiger ist, und irgendwo zwischen Bequemlichkeit und Sicherheit einen akzeptablen Mittelweg finden.

Im Prinzip ist es wie im Alltag: Der Supermarkt, in dem Alice regelmässig einkauft, bietet den Kunden eine «Supersparkarte» an. Wer diese Karte benützt und seine Einkäufe darüber abwickelt, kommt in den Genuss unzähliger Vergünstigungen und Aktionen. Der Supermarkt erhält als Gegenleistung ein präzises Kundenprofil mit allen gekauften Artikeln der Kartenbenutzer. Alice verzichtet auf die Supersparkarte. Der Supermarkt soll nicht über ihre Einkaufsgewohnheiten Bescheid wissen. Einziger Nachteil für Alice ist die lästige Frage «Sind Sie Supersparerin?» an der Kasse.

Im Netz geht es Alice ähnlich: Schaltet sie im Browser die Cookies aus, so werden bei manchen Web-Sites nützliche Informationen von früheren Besuchen nicht aufgezeichnet. Lässt Alice vor dem Akzeptieren von Cookies warnen, so wird sie andauernd mit Meldungen der Art «Die vorliegende Web-Seite möchte ein Cookie setzen» konfrontiert. Absoluter Schutz der Privatsphäre und bequemes Navigieren im Netz, das lässt sich nicht optimal unter einen Hut bringen. Es bleibt persönliche Entscheidungssache, welcher Aspekt wichtiger ist.

Alice hat einen Blick in das von ihrem Browser angelegte Verzeichnis auf ihrer Festplatte geworfen. Tatsächlich, in einem Unterverzeichnis hat Alice den Cache entdeckt:

Name	Internetadresse	Größe	Letzte Änderung	Letzter Zugriff
button3_on.gif	http://www.safeshopping.org/images/buttons/button3_on.gif	2.23 KB	19.11.99 21:44	30.12.99 13:11
buttons_02-over...	http://www.safeshopping.org/images/buttons/buttons_02-over.gif	1.66 KB	22.10.99 20:45	30.10.99 10:11
buttons_03-over...	http://www.safeshopping.org/images/buttons/buttons_03-over.gif	1.59 KB	22.10.99 20:45	30.10.99 10:11
buttons_08.gif	http://www.safeshopping.org/images/buttons/buttons_08.gif	1.66 KB	22.10.99 20:45	30.10.99 10:11
buttons_04.gif	http://www.safeshopping.org/images/buttons/home/buttons_04.gif	1.68 KB	22.10.99 20:45	30.10.99 10:10
homebutton11_...	http://www.safeshopping.org/images/buttons/homebutton11_on.gif	2.94 KB	19.11.99 21:45	30.12.99 13:11
homebutton5_o...	http://www.safeshopping.org/images/buttons/homebutton5_on.gif	2.12 KB	19.11.99 21:45	30.12.99 13:11
homedelivery_te...	http://www.safeshopping.org/images/top_text/homedelivery_text.gif	907 Byte	19.11.99 21:46	30.12.99 13:11
hometips_text.gif	http://www.safeshopping.org/images/top_text/hometips_text.gif	826 Byte	19.11.99 21:46	30.12.99 13:11
security_menu.h...	http://www.safeshopping.org/security/security_menu.html	1.01 KB	22.10.99 20:48	30.10.99 10:11

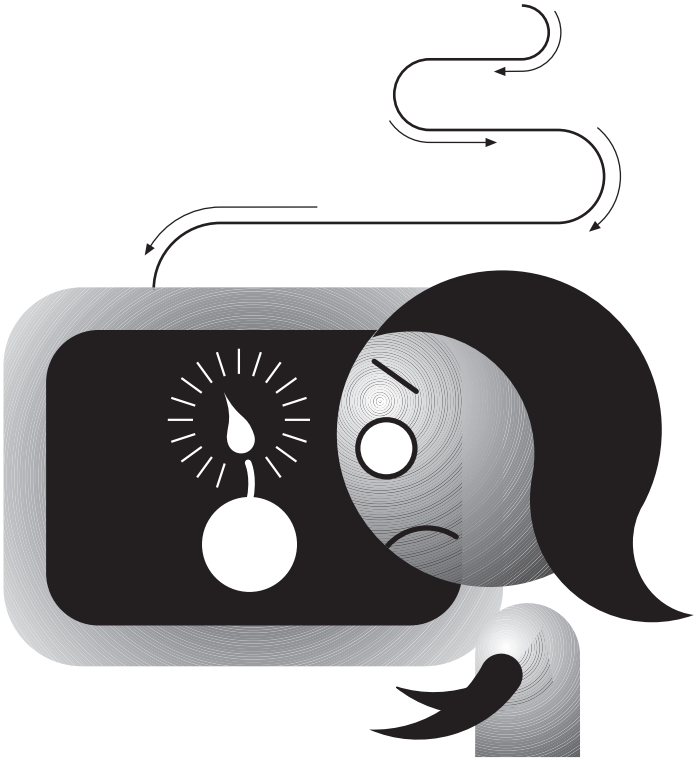
Die meisten der von Alice in letzter Zeit besuchten Web-Seiten sind hier zwischengespeichert. Das ist weiter nicht schlimm, schliesslich lässt Alice niemanden an ihren Computer ran. Ausserdem ist der Zugang zum Rechner durch ein Passwort geschützt. Alice merkt sich aber, dass sie heikle Daten wie den Cache, die History oder andere

private Informationen auf der Festplatte «wegräumt», bevor sie den Rechner zu einer allfälligen Reparatur bringt.

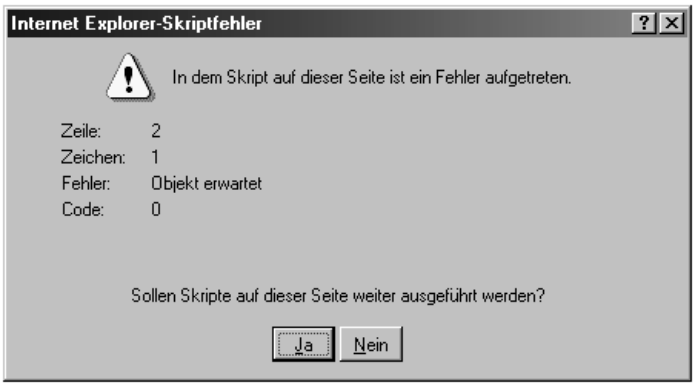
Inzwischen weiss Alice auch, was ein Proxy ist. Alle von ihr aufgerufenen Web-Seiten gelangen via den Proxy-Server des *Backstreet Journals* zu Alice. Alice kann demzufolge nicht ausschliessen, dass beim *Backstreet Journal* ihre Streifzüge im Netz aufgezeichnet und kontrolliert werden. Eigentlich nichts Neues: Es ist ohne weiteres möglich, den Briefverkehr von Alice zu überwachen. Briefumschläge lassen sich mit etwas Geschick öffnen und anschliessend wieder schliessen, ohne dass Alice etwas bemerkt. Der wesentliche Unterschied im Internet besteht darin, dass sich der Datenverkehr einfacher mitverfolgen lässt.

Kapitel 7

Programme aus dem Netz



Mit einem lästigen Problem ist Alice zum Glück relativ selten, aber doch mit hartnäckiger Regelmässigkeit konfrontiert: Gerade bei bunten, animierten Web-Seiten stürzt ihr Rechner bisweilen ab. Kein Mausklick und kein Tastendruck helfen dann weiter – Alice muss den Browser oder gar den ganzen Rechner neu starten. Bob meint, vielleicht sei ihr Rechner zu alt. Alice kann das nicht glauben. Auch auf Bobs neuem Rechner erscheinen gelegentlich eigenartige Fehlermeldungen, die manchmal zum Absturz des Browsers führen.



Mit Computerviren hat sich Alice schon vor dem Internet-Zeitalter herumgeschlagen. Nur allzu gut vermag sie sich an den Tag zu erinnern, als beim *Backstreet Journal* fast gar nichts mehr lief. Die meisten Computersysteme waren von einem Virus lahm gelegt. Seit diesem Vorfall ist es beim *Backstreet Journal* strikte verboten, private Programme auf den Firmenrechnern zu installieren. Und die Leute vom Informatiksupport rufen alle Mitarbeiterinnen und Mitarbeiter dazu auf, möglichst keine Programme aus dem Internet herunterzuladen. Auch in den Zeitungen liest Alice immer wieder von Computerviren, die sich über das Internet verbreiten. Sogar E-Mail-Nachrichten könnten Viren enthalten. Ob das wohl stimmt?

Alice sitzt bei einer Tasse Kaffee im gemütlichen Wohnzimmer und verbringt die Zeit surfend im Internet. Irgendwann landet sie auf einer spannenden Web-Site, welche die allerneusten und -besten Techniken im Bereich Audio und Video auszureizen verspricht. Doch bevor man in den Genuss dieser Multimedia-Köstlichkeiten kommt, muss ein Plug-in heruntergeladen und installiert werden.

Alice ist verunsichert. Soll sie das Plug-in beziehen oder besser auf den angekündigten Augen- und Ohrenschmaus verzichten? Welche Risiken geht sie durch das Installieren des Plug-ins ein? Und was ist überhaupt ein Plug-in?

Hacker, Programmierfehler oder Fehlbedienung?

Die erschreckenden Schlagzeilen aus den Medien sind bestens bekannt. Der stereotype Hacker, der mit grimmigem Gesicht an einem Computer sitzt und Tag und Nacht Systeme zu knacken versucht, ist jedoch für die meisten Privatanwenderinnen nicht das grösste Problem. Viele Hacker, die in fremde Systeme einzubrechen versuchen, haben es auf die Systeme von kommerziellen Anbietern, militärischen Institutionen usw. abgesehen. Dort ist der potenzielle Nutzen grösser. Ausserdem sind viele Hacker-Methoden nur bei Server-Systemen anwendbar, weil diese Systeme komplexer sind und mehr Angriffsmöglichkeiten bieten.

Das grösste Problem für private Internet-Benutzer sind fremde Programme. Ein Hacker kann ein Programm verfassen, das einen Privatrechner ausspioniert und geheime Daten aufstöbert. Dann muss es der Hacker nur noch schaffen, das Programm auf dem entsprechenden Rechner auszuführen. Typischerweise geht das, indem das bösartige

Programm als seriöse Anwendung getarnt wird. Um sich unbefugten Zugriff zu einem Rechner zu verschaffen, nützt der Hacker Programmfehler und Sicherheitslücken im Betriebssystem, Web-Browser oder einer anderen Anwendung oder schlicht das Fehlverhalten von Benutzern aus.

Eine andere Art von «unbefugtem» Zugriff hat keinen mutwillig boshaften Hintergrund. Auch rechtmässige Benutzer können einem Computersystem durch unsachgemässe Bedienung versehentlich Schaden zufügen. Zudem gibt es immer wieder Programme, die aufgrund von Programmfehlern zu Datenverlusten führen.

Daten aus dem Netz: Downloads

Beim Browsen im Internet lädt man von irgendwelchen Servern auf der Welt Daten auf den eigenen Rechner herunter. Das Herunterladen wird in Englisch *Downloading* genannt. Meistens sind die heruntergeladenen Daten harmlos. Das trifft insbesondere auf «normale» Web-Seiten zu, die aus Text und einigen Layoutangaben bestehen. Der Web-Browser hat in diesem Fall lediglich die Aufgabe, den Text aufgrund der Layoutvorgaben auf dem Bildschirm darzustellen.

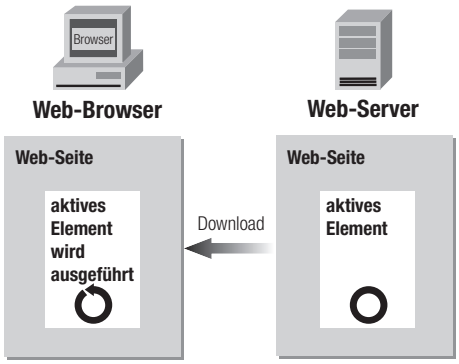
Schriller, bunter, lauter – und gefährlicher

Ursprünglich war die Datenautobahn so grau wie der Asphalt auf einer physischen Autobahn. Das Internet basierte ausschliesslich auf Texten. Später folgte der Siegeszug des World Wide Web – ab sofort musste jede Web-Seite multimedial daherkommen. Typische Web-Browser sowie die HTML-Layoutsprache sind allerdings nur bedingt auf irrwitzige grafische und akustische Effekte ausgelegt. Hauptaufgabe eines Web-Browsers ist das Anzeigen von Texten und unbewegten Bildern.

Deshalb wurden neue Möglichkeiten geschaffen, um dem WWW mehr Leben einzuhauchen. Heute gibt es zahlreiche Techniken zur Erzeugung von aktiven Elementen in einer Web-Seite. Ein *aktives Element* ist ein Programm, das vom Web-Browser ausgeführt wird und eine Web-Seite mit einer bestimmten Funktionalität anreichert.

Meistens sind aktive Elemente harmlos und stellen vielleicht eine willkommene Bereicherung für eine Internet-Anwenderin dar. Beispielsweise können Taschenrechner, ein Action-Spiel, ein animiertes Modell einer Sonnenfinsternis oder eine interaktive Navigationsoberfläche angeboten werden. Aktive Elemente werden im englischen Sprachraum zusammenfassend mit *Active Content* bezeichnet.

Viele Techniken zur Erzeugung von aktiven Elementen funktionieren nach dem gleichen Prinzip: Die zu Grunde liegende Web-Seite wird erstellt und bei einem Web-Server zugänglich gemacht. Soll an einer bestimmten Stelle auf der Web-Seite eine Animation erscheinen, baut die Verfasserin der Web-Seite dort ein aktives Element ein. Sobald eine Internet-Anwenderin wie Alice den Web-Server besucht und die Seite abruft, werden der HTML-Code der Seite sowie das aktive Element zu Alices Rechner übertragen. Der Web-Browser stellt die Seite dar und führt das aktive Element aus – Alice kommt in den Genuss der Animation.



Bei aktiven Elementen handelt es sich um Programme, die auf dem Benutzer-PC ausgeführt werden. Damit sind gewisse Risiken verbunden.

Programmfehler

Die meisten Programme enthalten unbeabsichtigte Fehler. Je umfangreicher und komplexer ein Programm ausfällt, desto höher ist

die Wahrscheinlichkeit, dass Fehler darin enthalten sind.

Folglich besteht bei jedem aktiven Element ein gewisses Risiko, dass damit einem fehlerhaften Programm der Zugriff auf den eigenen Computer ermöglicht wird. Vielleicht hat ein allfälliger Programmfehler keine schwer wiegenden Konsequenzen. Unter Umständen wird durch den Fehler aber auch irreparabler Schaden angerichtet.

Vorsätzliche Angriffe

Ein böswilliger Zeitgenosse wie Mallet kann herunterladbare Programme gezielt für seine Zwecke ausnützen. Er kann zum Beispiel ein Programm schreiben, das einen fremden Rechner ausspioniert. Das Programm versteckt er innerhalb einer harmlos erscheinenden Web-Seite. Wenn Alice die Web-Seite herunterlädt, wird das Programm ausgeführt, und es werden persönliche Informationen an Mallet übermittelt.

Vielleicht möchte Mallet einfach nur Vandalismus betreiben. In diesem Fall schreibt er ein Programm, das Alices Festplatte löscht oder ihren Rechner zum Absturz bringt.

Oder: Mallet schreibt ein Programm, das den Rechner von Alice blockiert. Einfach zu realisieren sind beispielsweise Programme, die hunderte und tausende von unnützen Browser-Fenstern öffnen. Resultat: Der Computer ist so stark beschäftigt, dass er auf Alices Eingaben nicht mehr reagiert. Häufig hilft dann nur das gnadenlose Ausschalten des Rechners. Angriffe dieser Art sind als *Denial-of-Service-Angriffe* bekannt, weil dabei eine bestimmte Dienstleistung oder Funktionalität zum Erliegen gebracht wird.

Aktive Elemente

Schauen wir uns einige konkrete Techniken zur Realisierung von aktiven Elementen an. Wir werden nur diejenigen erwähnen, auf die man im Internet häufig trifft.

JavaScript

JavaScript der Firma Netscape Inc. ist eine Programmiersprache, deren Befehle man direkt in eine Web-Seite einbinden kann. JavaScript stellt Möglichkeiten bereit, um das Aussehen und das Verhalten des Web-Browsers zu beeinflussen. So können Meldungen an den Benutzer dargestellt, Formulare automatisch ausgefüllt, neue Browser-Fenster geöffnet oder ein interaktives Navigationsmenü erstellt werden.

Um ein gewisses Mass an Sicherheit zu bewahren, gibt es in JavaScript keine Funktionen für den Zugriff auf das Dateisystem des Rechners oder für das Aufbauen einer Netzwerkverbindung zu einem anderen Rechner.

Trotzdem sind gewisse Risiken mit JavaScript verbunden. Manche JavaScript-Programme weisen Fehler auf und belästigen die Internet-Benutzerin mit entsprechenden Fehlermeldungen. Ausserdem kann nicht ausgeschlossen werden, dass gewisse Lücken in den Sicherheitsvorkehrungen bestehen. Solche Mängel können zur Umgehung der Sicherheitsmassnahmen ausgenutzt werden.

ActiveX

ActiveX ist eine von Microsoft entwickelte Infrastruktur. Eine Web-Seite kann mittels ActiveX mit einer speziellen Funktionalität ausgestattet werden. ActiveX-Komponenten können mit einer beliebigen Programmiersprache erzeugt werden. Die Komponenten werden in einer Web-Seite eingebunden und automatisch auf den Benutzer-PC heruntergeladen und dort ausgeführt.

Innerhalb der ActiveX-Infrastruktur gibt es keine Sicherheitsvorkehrungen. Eine ActiveX-Komponente hat typischerweise uneingeschränkten Zugriff auf einen Rechner und die darauf gespeicherten Daten. Das potenzielle Risiko solcher Komponenten ist entsprechend gross.

Visual Basic Script

Die Programmiersprache Visual Basic Script (VBS) von Microsoft ist vergleichbar mit JavaScript. Ein VBS-Programm kann direkt in eine

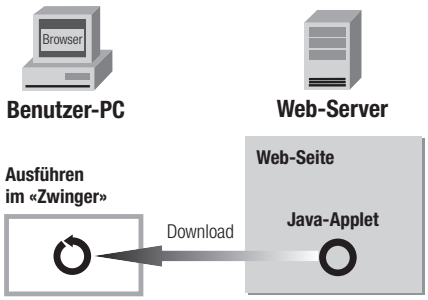
Web-Seite eingebunden werden, um beispielsweise die Benutzereingaben in einem Formular auf ihre Gültigkeit zu überprüfen.

VBS bietet ähnliche Sicherheitsvorkehrungen wie JavaScript. Beispielsweise stehen keine Funktionen für das Öffnen oder Verändern von Dateien auf dem Benutzerrechner zur Verfügung. Doch dieser Schutz ist trügerisch. Ein VBS-Programm kann auf ActiveX-Komponenten zugreifen. Weil ActiveX-Komponenten keinen Sicherheitsvorkehrungen unterliegen, kann ein VBS-Programm über diesen Umweg potenziell gefährliche Funktionen wie das Verschicken von E-Mails oder das Manipulieren von Dateien ausführen.

Java

Java ist eine Programmiersprache, die von der Firma Sun Microsystems entwickelt wurde. Java erlaubt das Schreiben von Programmen, die via Internet in den Web-Browser geladen und ausgeführt werden. Diese Programme werden *Java-Applets* oder kurz *Applets* genannt.

Im Unterschied zu ActiveX-Komponenten werden Applets typischerweise unter weit reichenden Sicherheitsvorkehrungen ausgeführt. Zum Beispiel haben Applets keinen Zugriff auf die Hardware oder das Betriebssystem eines Rechners. Man kann das mit einem Hundezwinger vergleichen: Ein (potenziell) gefährlicher Hund wird in einem Zwinger gehalten. Dort kann er sich begrenzt austoben und trotzdem seiner Umwelt nicht schaden.



Aufgrund dieses «Zwingers» sind Java-Applets weit weniger gefährlich als beispielsweise ActiveX-Programme. Leider bleibt ein Problem

bestehen: Die Sicherheitsvorkehrungen sind teilweise lückenhaft oder weisen Programmierfehler auf. Diese Sicherheitslücken können von einem bösartigen Applet ausgenützt werden. Etwa so wie der Hund, der ein Loch im Zwinger findet und entwischt.

Plug-ins

Plug-ins erfüllen einen anderen Zweck als JavaScript, ActiveX und Java. Plug-ins sind Browser-Erweiterungen. Programme also, die den Web-Browser mit zusätzlichen Funktionen ausbauen. Häufig ermöglichen Plug-ins das Betrachten von speziellen Datentypen wie Video- oder Tonsequenzen, mit denen der Browser alleine nichts anfangen kann.

Plug-ins werden vom Benutzer heruntergeladen und manuell installiert. Ab diesem Moment steht das Plug-in bei Bedarf bereit. Es gibt zum Beispiel Plug-ins zum Abspielen von bestimmten Musikdateien oder zur Anzeige von filmähnlichen Multimedia-Präsentationen.

Leider gibt es bei Plug-ins keinerlei Sicherheitsvorkehrungen. Ein Plug-in kann sich auf einem Rechner beliebig zu schaffen machen. Man muss als Benutzer selber entscheiden, wie stark man dem Anbieter eines Plug-ins vertraut und ob es sich im Hinblick auf den erwartbaren Nutzen lohnt, das Risiko einzugehen.

Helper Applications

Die so genannten Helper Applications erfüllen grundsätzlich denselben Zweck wie Plug-ins. Die «Hilfsanwendungen» ermöglichen die Verarbeitung von speziellen Arten von Dokumenten aus dem Internet. Im Gegensatz zu den Plug-ins sind Helper Applications allerdings keine Browser-Erweiterungen. Es handelt sich vielmehr um eigenständige Anwendungsprogramme, die bei Bedarf automatisch durch den Browser aufgestartet werden. So könnte zum Beispiel beim Empfang einer Microsoft-Excel-Datei die zugehörige Anwendung – die Tabellenkalkulation Excel – gestartet werden. Die Tabellenkalkulation stellt dann die Datei dar.

Auf der einen Seite ist die beschriebene Automatik für den Benutzer natürlich angenehm. Er muss sich nicht darum kümmern, welche

Anwendung er für welche Datei benützen soll. Auf der anderen Seite verliert der Benutzer die Kontrolle darüber, welche Programme auf seinem Rechner ausgeführt werden. Zum Beispiel könnte die empfangene Datei ein bösartiges Programm enthalten. Das Programm würde also automatisch ausgeführt, ohne dass der Benutzer eingreifen kann.

Shareware und Konsorten

Neben den aktiven Elementen, die zusammen mit einer Web-Seite den Weg auf den PC finden, gibt es eine andere wichtige Sorte von herunterladbaren Programmen. Im Internet steht eine enorme Anzahl von kleinen Hilfsprogrammen und ausgewachsenen Anwendungen zur Verfügung. Diese Programme können gratis *(Freeware)* oder gegen einen meist geringen Unkostenbeitrag *(Shareware)* bezogen werden. Viele dieser Programme sind nicht sehr ausgereift und schlecht programmiert. Andere überzeugen durch ihre Professionalität und sind von grossem Nutzen.

Shareware- und Freeware-Programme werden via Internet heruntergeladen und auf dem eigenen Rechner installiert. Sie können auf alle Komponenten des Rechners und des Betriebssystems zugreifen. Programmfehler können zu Datenverlusten oder zu einer anderen Beeinträchtigung des Systems führen. Ein Übeltäter wie Mallet kann ein bösartiges Programm vorsätzlich in Umlauf bringen.

Trojanische Pferde

Eine besonders heimtückische Art von bösartigen Programmen sind die so genannten Trojanischen Pferde. In Anlehnung an die griechische Sage handelt es sich um Programme, die eine böse Überraschung in sich bergen: Oberflächlich wird eine nützliche Funktion angeboten, doch im Hintergrund geht etwas Schädliches vor sich.

Beispiel: Mallet programmiert eine Textverarbeitung mit einigen sehr nützlichen Funktionen und stellt sie als kostenlose Freeware zur Verfügung. Alice bezieht die Anwendung und ist begeistert davon. Ab sofort schreibt sie alle Briefe mit Mallets Textverarbeitung. Was sie allerdings nicht weiss: Mallet hat versteckte, zerstörerische Funk-

tionen eingebaut. Von Alice unbemerkt löscht die Textverarbeitung eine zufällig gewählte Datei auf der Festplatte. Ausserdem löscht sie manchmal ein Wort aus einem von Alices Briefen oder fügt neue Wörter hinzu.

Trojanische Pferde sind sehr schwierig zu entlarven. Auch bei Shareware und Freeware stellt sich folglich die Frage, inwiefern man einem bestimmten Anbieter Vertrauen schenkt. Zudem können Shareware- und Freeware-Programme Viren mit sich tragen.

Cyberkrankheiten: Computerviren

Erschöpft, fiebrig und geschwächt schält sich Alice aus einem halben Dutzend Bettdecken und schleppt sich in die Küche, wo sie sich einen weiteren Liter heissen Tee zubereitet. Alice hat sich ein Virus eingefangen und versucht verbissen, das garstige Ding loszuwerden.

Einige Tage später ist Alice wieder bei Kräften – die Krankheit schon fast vergessen. Doch Alice hat sich vorgenommen, einige Vorsichtsmassnahmen zu beachten: Sie geht auf Abstand bei Personen, die von einem Virus befallen sind. Und sie lässt sich impfen, damit sie über geeignete Antikörper verfügt.

Computerviren verhalten sich ähnlich wie die aus dem Alltag bekannten Krankheitserreger. Sogar manche Gegenmassnahmen sind ähnlich.

Was sind Computerviren?

Viren im Alltag sind Krankheitserreger, die sich durch die Veränderung des genetischen Codes von lebenden Zellbestandteilen vermehren können. Auch in der Computerwelt gibt es Viren. Computerviren können sich ebenfalls selbstständig vermehren, indem sie andere Programme befallen und verändern. Viele Computerviren führen nichts Gutes im Schilde und tarnen deshalb ihre bösartige Funktion, indem sie sich via ungefährlich erscheinende Programme oder Dateien in ein System einschleichen. Wenn sie im Zielsystem aktiviert werden, beginnt ihr destruktives Werk: Daten werden gelöscht, Programme oder Daten an einen anderen Ort verschoben oder umbenannt, Daten

werden verändert usw.

Daneben gibt es viele Viren, die weniger bösartig sind und sich mit unschädlichen, aber nervenaufreibenden Störaktionen begnügen. Manche Viren dieser Sorte beeinträchtigen die Maussteuerung, stellen die Bildschirmanzeige auf den Kopf oder zeigen ab und zu eine Meldung und warten auf einen Tastendruck.

Ein Virus muss nicht sofort aktiv werden. Wenn eine bestimmte Anwendung infiziert wurde, dauert es unter Umständen geraume Zeit, bis diese Anwendung erneut gestartet und gleichzeitig das Virus aktiviert wird. Manche Viren werden nur an einem bestimmten Zeitpunkt in der Zukunft aktiv. Oft handelt es sich um spezielle Daten wie Freitag, den 13.

Infektion

Wie wird ein Computer von einem Virus infiziert? Früher erfolgte die Übertragung beim Austausch von Disketten mit Programmen oder Dateien. Ein Virus versteckte sich auf der Diskette – meist als Anhängsel einer Anwendung – und wurde unbeabsichtigt auf die Festplatte des Computers kopiert.

Im Internet gestaltet sich die Verbreitung von Viren einfacher. Immer wieder lädt man als Internet-Anwender ein nützliches Programm aus dem Internet und installiert es auf dem eigenen Rechner. Dabei kann es vorkommen, dass ein solches Programm von einem Virus infiziert ist. Oder man erhält per E-Mail zur Unterhaltung ein Prográmmchen von einer Arbeitskollegin, das unter Umständen infiziert ist.

Ausführbarkeit

Grundsätzlich gilt: Ein Virus muss aktiviert werden, sonst ist es absolut harmlos! Wenn Alice ein Programm aus dem Internet auf ihren Rechner herunterlädt, braucht sie sich noch keine Sorgen zu machen. Auch wenn das Programm von einem Virus befallen ist – das Virus kann erst aktiv werden, wenn Alice das Programm startet.

Auf einem Computer existieren grundsätzlich zwei Arten von Dateien:

- *Reine Daten* werden nie ausgeführt. Stattdessen braucht es eine passende Anwendung, welche die Daten anzeigen kann. Bei einer Textdatei zum Beispiel braucht es zum Anzeigen einen Texteditor. Für eine Grafikdatei wird ein Grafikprogramm benötigt.

- *Programme* werden durch einen entsprechenden Aufruf (zum Beispiel Doppelklicken mit der Maus) ausgeführt. Anwendungen wie Grafikprogramme, Web-Browser oder Textverarbeitungen sind bestens bekannte Programme. Daneben gibt es zahlreiche andere Programme, die ihren Dienst meist unbemerkt vom Benutzer irgendwo im Betriebssystem verrichten.

Konsequenz: Wenn Alice sicher sein kann, dass es sich bei einer Datei um nicht ausführbare Daten handelt, so kann sie die Datei problemlos anzeigen lassen. Leider ist in der Praxis die Unterscheidung zwischen reinen Daten und ausführbaren Programmen schwierig. Häufig kommt es zu Vermischungen.

Beispiel 1: Word-Dokumente und Makros

Ein Dokument aus einer typischen Textverarbeitung wie Microsofts Word würde man eigentlich als unproblematisch einstufen. Schliesslich kommt in einem Word-Dokument nichts anderes vor als Text- und Formatierungszeichen sowie vielleicht eine Tabelle und das eine oder andere Bild. Doch der Schein trügt. Word beinhaltet eine so genannte *Makro-Programmiersprache*. Ursprünglich dienten Makros dazu, immer wiederkehrende Aktivitäten zu automatisieren. Unterdessen ist Microsofts Makro-Sprache aber derart fortgeschritten, dass die Möglichkeiten fast unbegrenzt sind. Mit Hilfe der eingebauten Makro-Sprache lassen sich zum Beispiel vollautomatische Formulare oder eigene Menüleisten erstellen.

Word-Dokumente sind daher nicht ungefährlich. Wer ein Word-Dokument öffnet, läuft Gefahr, gleichzeitig ein *Makro-Virus* zu aktivieren. Beispiel: Alice findet unter irgendeiner Adresse im WWW eine Liste mit allen bekannten Typen von Computerviren. Die Liste steht nur im Word-Format zur Verfügung. Alice lädt das Dokument

auf ihren Privat-PC und schaut es sich mit Word an. Ironischerweise hat sich in die Virenliste ein Makro-Virus eingeschlichen, das nun aktiviert wird.

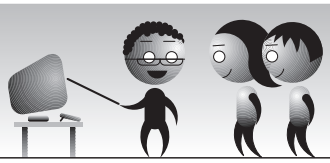
Microsofts Word ist nur ein Beispiel für eine Anwendung mit einer Makro-Programmiersprache. Andere Microsoft-Office-Anwendungen wie Excel oder PowerPoint bieten ebenfalls Makros an. Ausserdem gibt es weitere Hersteller, die Makrosprachen in ihren Anwendungen zur Verfügung stellen.

Beispiel 2: E-Mails mit aktiven Elementen

Auch bei E-Mails würde man eigentlich davon ausgehen, dass sie ungefährlich sind. Es handelt sich ja lediglich um einfache Texte. Viele der modernen E-Mail-Programme akzeptieren allerdings E-Mails im HTML-Format. Genau so, wie ein Web-Browser HTML-Dateien darstellt.

Innerhalb der HTML-Daten einer E-Mail kann sich ein Stück Programmcode verstecken, das beim Anschauen der E-Mail automatisch aktiviert wird. Es handelt sich dabei um aktive Elemente, wie sie auch in Web-Seiten eingesetzt werden – mit demselben Nutzen und demselben Gefahrenpotenzial.

Praxis



Alice kennt nun Downloads wie Plug-ins, Java-Applets oder Shareware-Programme. Zudem hat sie eine Vorstellung davon, was ein Computervirus ist. Aber was kann sie gegen all diese Dinge tun?

Leider gibt es keine Patentlösungen. Wichtig sind eine gewisse Vorsicht und eine gesunde Portion Misstrauen bei der Benutzung des Internets. Schliesslich bittet Alice auch nicht jede beliebige Person in ihr Haus, sondern lässt sich im Zweifelsfall einen Ausweis zeigen.

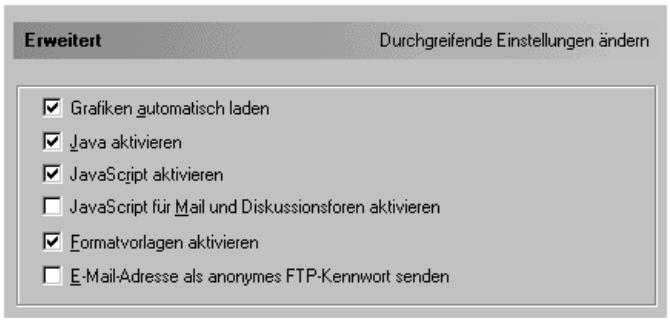
Ähnlich wie im Alltag gibt es im Zusammenhang mit dem Internet einige Vorkehrungen und Vorsichtsmassnahmen, um den eigenen Computer zu schützen.

Downloading mit Bedacht

Alice führt auf ihrem Rechner unbekannte Programme aus. Sie weiss nicht, ob das Programm vielleicht Fehler enthält, ein Virus mit sich trägt oder gar vorsätzlich mit bösartigen Funktionen angereichert wurde.

Ist Alice bereit, aus Sicherheitsgründen auf gewisse Animationen und Multimedia-Spielereien zu verzichten? Wenn ja, wird sie eher selten ein Programm aus dem Internet herunterladen. Umgekehrt wird Alice ein gewisses Risiko eingehen müssen, falls sie die gestalterischen Techniken des World Wide Web voll auskosten möchte. Auf jeden Fall wird Alice bei jedem Shareware-Programm und bei jedem Plug-in zweimal überlegen, ob die Software tatsächlich nötig ist und ob sich der Aufwand für den Bezug und die Installation der Software lohnt.

Alice kann ausserdem mit Hilfe der Sicherheitseinstellungen ihres Web-Browsers steuern, welche Programme der Browser herunterladen und ausführen darf. Beim Netscape Communicator zum Beispiel lässt sich kontrollieren, ob Java-Applets und JavaScript-Elemente in Web-Seiten und E-Mails ausgeführt oder ignoriert werden sollen:



Die Sicherheitsoptionen bei Netscapes Browser sind einerseits hilfreich, denn was nicht ausgeführt wird, kann nicht gefährlich werden. Andererseits sind die Einstellungen ziemlich restriktiv. Sobald JavaScript deaktiviert ist, wird eine grössere Zahl von Web-Seiten nicht mehr wie geplant funktionieren.

Ähnliche Einstellungen lassen sich bei Microsofts Internet Explorer vornehmen. Alice hat die Wahl zwischen drei Sicherheitsstufen. Alternativ kann sie die Einstellungen gänzlich selber vornehmen und ein eigenes Sicherheitsprofil erstellen.

Code Signing

Viele Softwarehersteller preisen das *Code Signing* als Lösung gegen das Herunterladen von bösartigen Programmen aus dem Internet an.

Beim Code Signing wird beispielsweise ein Java-Applet vom Autor digital unterzeichnet. Ein Benutzer kann somit nach dem Herunterladen prüfen, von wem das Applet stammt.

Mit Hilfe von Code Signing wird unterbunden, dass Programme unter falschem Namen veröffentlicht werden. Allerdings kann durch das simple Unterschreiben eines Programmes keine Sicherheit garantiert werden. Auch ein Programm voller Sicherheitslücken oder eines mit schädlichen Funktionen kann ohne weiteres digital unterzeichnet werden.

Sicherheitslöcher stopfen

Die meisten Softwareprodukte weisen Sicherheitslücken auf. Diese Sicherheitslücken lassen sich vielfältig ausnützen: zum Beispiel, um sich unbefugten Zugriff zu einem Rechner zu beschaffen, ein fremdes Programm zur Ausführung zu bringen, Dateien zu lesen, zu löschen oder zu manipulieren oder einen Absturz zu provozieren. Jede Art von Programmen ist von diesem Problem betroffen. Seien es das Betriebssystem, der Web-Browser, das E-Mail-Programm oder eine Anwendung wie die Textverarbeitung oder das Tabellenkalkulationsprogramm.

Verschiedene Gruppierungen, die sich für Informatik-Sicherheit interessieren, machen sich gezielt auf die Suche nach Sicherheitslücken. Manche Sicherheitslöcher werden auch zufällig durch die Anwender eines Programms aufgedeckt.

Nach der Entdeckung werden die Sicherheitslücken in geeigneten Mailing-Listen oder Diskussionsforen einer breiten Öffentlichkeit kundgetan. Die schwer wiegenden Fälle schaffen es bisweilen sogar in die Medien. Ausserdem werden die Herstellerfirmen über die Mängel in den betreffenden Produkten informiert. Handelt es sich um eine verantwortungsbewusste Firma, stellt sie innert nützlicher Frist ein *Patch* her. Beim Patch handelt es sich um ein «Softwarepflaster», welches das Sicherheitsloch behebt. Manche Firmen bieten anstelle von Patches neue *Updates* der entsprechenden Software an.

Patches werden meistens via Internet zum Download angeboten. Benutzer des betroffenen Produktes können die nötigen Patches beziehen und auf ihrem Rechner installieren. Damit ist allerdings

kein unerheblicher Aufwand verbunden, denn häufig sind die Patches gross, und der Download dauert entsprechend lange. Hinzu kommt, dass gerade für Betriebssysteme wöchentlich oder manchmal fast täglich neue Patches hergestellt werden. Trotzdem ist es ratsam, ab und zu einen Blick auf die Web-Sites der Software-Hersteller zu werfen und die wichtigsten Patches zu installieren.

Auf Virenjagd mit Antivirensoftware

Die Standardabwehr von Computerviren heisst *Antivirensoftware*. Virenschutzprogramme wenden verschiedene Techniken an, um Viren in einem Rechner oder auf einem Speichermedium aufzuspüren. Man kann gezielt eine einzelne Datei untersuchen oder das ganze System regelmässig kontrollieren lassen – zum Beispiel bei jedem Aufstarten oder in bestimmten Abständen während des Betriebs. Manche Virenschutzprogramme sind im Hintergrund aktiv und überwachen die Downloads aus dem Internet.

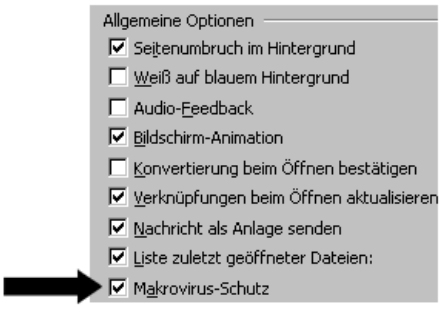
Die Schutzsoftware sollte möglichst viele konkrete Virentypen sowie allgemein gültige Merkmale vieler Viren kennen. So ist die Software in der Lage, Viren zu erkennen und zu entfernen. Allerdings bietet auch eine Antivirensoftware keinen hundertprozentigen Schutz. Nicht jedes Virus wird erkannt, und nicht jedes erkannte Virus kann erfolgreich entfernt werden. Zudem geraten fortlaufend neue Viren in Umlauf, die der Antivirensoftware zunächst nicht bekannt sind.

Die Informationen über die bekannten Virentypen bezieht die Antivirensoftware aus einer *Virendatenbank*. Diese Datenbank sollte immer auf dem aktuellsten Stand gehalten werden, damit die Antivirensoftware gegen neue Viren gewappnet ist. Viele Virenschutzprogramme erlauben das bequeme Aktualisieren der Virendatenbank via Internet.

Makroviren

Alice hat mehrere Möglichkeiten, sich gegen Makroviren zu schützen: (1) Sie beschafft sich ein Antivirenprogramm und lässt es jede neu aus dem Internet heruntergeladene Datei überprüfen. (2) Alice öffnet

keine Dokumente mehr, die sie von Dritten erhalten hat. Wenn sie beispielsweise ein Word-Dokument per E-Mail-Attachment erhält, so verlangt sie eine reine Textfassung des Dokuments. (3) Bei neueren Anwendungen kann Alice den so genannten *Makrovirus-Schutz* aktivieren. Fortan werden neu geöffnete Dokumente auf Makros geprüft. Falls Makros vorkommen, kann Alice wählen, ob sie ausgeführt werden oder nicht.



E-Mail-Viren

Zwei wichtige Technologien zur Realisierung aktiver Elemente in E-Mails sind ActiveX und JavaScript. Also muss Alice als Gegenmassnahme dafür sorgen, dass weder JavaScript noch ActiveX automatisch ausgeführt werden: (1) Alice benutzt ein Mail-Programm, das ActiveX und JavaScript gar nicht versteht. Es gibt nach wie vor Mail-Programme, die ausschliesslich mit harmlosen Texten arbeiten. (2) Bei modernen Mail-Programmen kann man oft wählen, ob E-Mails im HTML-Format angezeigt werden sollen. In diesem Fall kann Alice ihr Mail-Programm anweisen, auch HTML-Daten als normale Texte anzuzeigen. Dann sehen manche E-Mails zwar nicht mehr so schön aus, dafür hat Alice ein Stück Sicherheit hinzugewonnen. (3) Häufig besteht die Möglichkeit, HTML-Daten anzuzeigen, aber aktive Elemente wie JavaScript- oder ActiveX-Komponenten zu unterdrücken. Das ist vermutlich die bequemste Variante.

ILOVEYOU: Würmer

4. Mai 2000, 16.43 Uhr – Alice sitzt an ihrem privaten Rechner und lädt die frisch eingegangenen E-Mails runter. Unter den Neuankömmlingen sticht ihr eine Nachricht von Bob mit dem Titel «ILOVEYOU» ins Auge. Voller Vorfreude schaut sie sich Bobs Mail zuerst an und liest den folgenden kurzen Text: «kindly check the attached LOVELETTER coming from me.»

Eigenartig, wieso schreibt Bob den Liebesbrief nicht direkt in die Mail? Und aus welchem Grund verfasst er die Mail in Englisch? Alice beschliesst, das Attachment nicht zu öffnen. Nach allem, was sie unterdessen weiss, ist ihr das zu heikel.

Im Gegensatz zu Millionen von anderen Internet-Benutzern hat Alice richtig reagiert. Bei «ILOVEYOU» handelt es sich um einen so genannten *Wurm* (Englisch: *Worm*). Ein Internet-Wurm ist ein Programm, das sich selbstständig von Rechner zu Rechner verbreitet. Die meisten Würmer haben das Ziel, eine möglichst grosse Abdeckung zu erreichen. Viele Würmer richten dabei Schaden auf den Zielrechnern an, oder sie bringen Zwischenstationen wie Mail-Server durch Überbelastung zum Absturz.

Der «ILOVEYOU»-Wurm ist ein in Visual Basic Script geschriebenes Programm, das als E-Mail-Attachment verschickt wird. Durch das Öffnen des Attachments wird der Wurm aktiviert und sendet sich selbstständig weiter an sämtliche Adressen im Microsoft-Outlook-Adressbuch des betreffenden Benutzers. Auf diese Weise verbreitet sich der Wurm sehr rasch. Ausserdem macht sich der Wurm auf der Festplatte des Benutzers breit, indem er zum Beispiel Visual-Basic-Script-, JavaScript-, Bild-, Ton-, Text- oder HTML-Dateien durch sich selbst ersetzt.

Der «ILOVEYOU»-Wurm zeigt unmissverständlich, wie wichtig das Wissen um die Risiken im Internet für die Benutzer ist. Allen Mail-Attachments sollte mit Vorsicht begegnet werden, selbst wenn sie von Bekannten stammen, aber eigenartige Inhalte aufweisen.

Prophylaxe für den Worst Case: Backups

Seit einigen Monaten beachtet Alice die vorgeschlagenen Vorsichtsmassnahmen in vorbildlicher Weise. Bisher ist auch alles gut gegangen. Doch was passiert, wenn sich trotz aller Umsicht ein Virus bei ihr einschleicht und wertvolle Daten löscht? Für solche Fälle sollte Alice unbedingt die richtige Vorarbeit geleistet haben. Die Prophylaxe heisst *Backup* oder auf Deutsch *Sicherheitskopie*.

Ein Backup ist eine Kopie von Daten auf eine herkömmliche Diskette, ein ZIP-Medium, eine CD-ROM oder ein anderes Speichermedium. Auf Backups ist man in verschiedenen Situationen angewiesen: nach dem versehentlichen Löschen einer wichtigen Datei durch den Benutzer, bei der Beschädigung von Daten durch einen Programmfehler im Betriebssystem oder in einer Anwendung oder bei Datenverlusten durch Virenbefall.

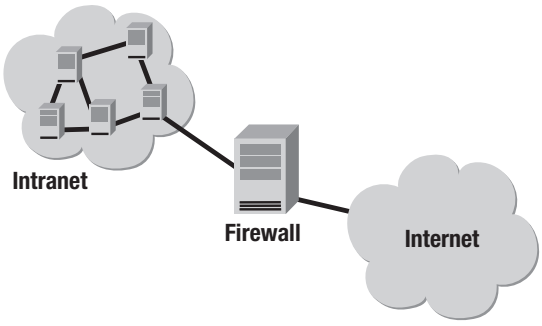
Damit Backups ihren Zweck erfüllen, müssen sie regelmässig und häufig durchgeführt werden. Falls ein Backup sechs Monate alt ist, geht bei einem Datenverlust trotz der Sicherheitskopie viel Arbeit verloren. Beim Backup sollten zumindest alle Benutzerdaten gesichert werden. Die Systemprogramme und die Anwendungen können notfalls frisch installiert werden. Und wer sehr hohe Sicherheitsansprüche verfolgt, bewahrt seine Backups nicht am gleichen Ort wie den Computer auf. Sonst geht bei einem Brand oder Einbruch beides verloren.

Beim Erstellen von Backups muss sichergestellt werden, dass die Originaldaten unbeschädigt vorliegen. Eine Sicherheitskopie sollte beispielsweise nicht selber durch Viren verseucht sein.

Firewalls

Viele Firmen setzen so genannte *Firewall-Rechner* (kurz: Firewalls) für zusätzliche Sicherheit ein. Eine Firewall soll das firmeninterne Computernetzwerk – das Intranet – vor unbefugten Zugriffen aus dem Internet schützen. Deshalb befindet sich die Firewall zwischen Internet und Intranet.

Sämtliche Verbindungen zwischen Intranet und Internet laufen über den Firewall-Rechner. Verbindungen aus dem Intranet in Richtung Internet werden meistens zugelassen. Die andere Richtung ist heikler: Verbindungen aus dem Internet ins Intranet werden überwacht und aufgrund bestimmter Kriterien eventuell zurückgewiesen. Auf diese Weise soll allfälligen Hackern das Leben erschwert werden, weil sie nicht mehr problemlos aus dem Internet in das Firmenintranet eindringen können.



Der Gedanke ist derselbe wie im Mittelalter. Viele Burgen hatten damals hohe Mauern und einen Wassergraben. Fremde konnten nicht an einem beliebigen Ort in die Burg gelangen. Stattdessen mussten alle Leute über die Zugbrücke die Burg betreten. Das hatte den Vorteil, dass man nur an der Zugbrücke Wachposten aufstellen musste, die jede Person überprüfen konnten.

Eine Firewall funktioniert nach demselben Prinzip. Aller Verkehr wird durch eine «schmale» und gut kontrollierte Stelle geführt. Aufgrund der Kontrollen wird über das Recht zum Passieren entschieden.

Auch im Intranet des *Backstreet Journals* steht eine Firewall. Für Alice, die im Intranet arbeitet, sind drei Dinge wichtig: (1) Um die Firewall braucht sie sich nicht zu kümmern. Das ist Aufgabe der Systemverantwortlichen beim *Backstreet Journal*. (2) Trotz Firewall darf sich Alice nicht in falscher Sicherheit wiegen. Auch mittelalterliche Burgen hatten oft geheime Eingänge. Genauso können Sicherheitslöcher in einer Firewall existieren. Zudem sind Firewalls nicht

mehr als ein Bestandteil eines übergeordneten Sicherheitskonzepts. Andere Sicherheitsaspekte wie Passwörter oder Viren dürfen nicht vernachlässigt werden. (3) Es kann vorkommen, dass zum Beispiel ein Java-Applet in Alices Browser nicht korrekt funktioniert, weil die Firewall eine benötigte Verbindung sperrt. Falls das Applet für ihre Arbeit unverzichtbar ist, setzt sich Alice am besten mit der Systemadministration in Verbindung.

Firewalls sind mächtige Hilfsmittel zur Gewährleistung von gewissen Sicherheitsansprüchen. Keine Firewall bietet jedoch vollumfängliche Sicherheit. Zum Beispiel prüft eine Firewall in der Regel keine E-Mails oder Inhalte von Web-Seiten. Dazu ist Zusatzsoftware nötig.

Personal Firewalls

Bei Firmen-Firewalls handelt es sich meist um eigene Rechner, die ausschliesslich für das Überwachen des Datenverkehrs vom und ins Internet zuständig sind. Für fortgeschrittene Heimanwender gibt es *Personal Firewalls*, welche die Funktionsweise ihrer «grossen Schwestern» vereinfacht anbieten.

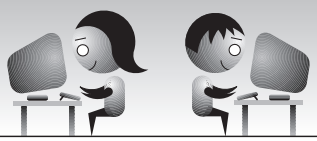
Personal Firewalls werden von verschiedenen Herstellern in unterschiedlichen Ausprägungen angeboten. Alle Produkte haben eines gemeinsam: Die Anwenderin muss über recht viel technisches Knowhow verfügen, um sie korrekt zu konfigurieren oder auf die Meldungen beim Betrieb korrekt zu reagieren.

Die einfacheren Vertreter von Personal Firewalls halten alle Pakete aus dem Internet fern, die ohne ersichtlichen Grund oder ohne zulässiges Ziel den eigenen Rechner erreichen. Ausserdem machen sie die Benutzerin darauf aufmerksam, wenn eine nicht zugelassene Anwendung auf dem PC mit dem Internet kommunizieren möchte. Durch diese Massnahmen werden Angriffsversuche aus dem Internet sowie das verdeckte Verschicken von Informationen ins Internet erschwert.

Personal Firewalls der komplizierteren Art können von der Benutzerin in allen Details frei konfiguriert werden. Es lässt sich jede Kommunikationsform zwischen beliebigen Kommunikationspartnern explizit zulassen oder gezielt einschränken. Die richtige Konfigurati-

on setzt aber fundiertes Hintergrundwissen über die Funktionsweise der verschiedenen, zur Datenübermittlung verwendeten Internet-Protokolle voraus.

Anwendung



In Bezug auf das Herunterladen von unbekannten Daten aus dem Internet sowie in Bezug auf Viren hat sich Alice die folgenden Merkpunkte zusammengestellt:

- Alice hat ein gesundes Misstrauen gegenüber allen Dateien, die aus dem Internet stammen. Auch gegenüber denjenigen von Freunden und Bekannten. Insbesondere startet Alice nie ein unbekanntes Programm, das als E-Mail-Attachment auf ihren Rechner gelangt ist.
- Alice hat auf ihrem Rechner eine Antivirensoftware installiert.
- Jede frisch heruntergeladene Datei wird von Alice mit Hilfe der Antivirensoftware auf der Stelle nach Viren geprüft. Manche Virenschutzprogramme lassen sich so konfigurieren, dass beispielsweise jedes neue E-Mail-Attachment automatisch nach Viren durchsucht wird.
- In regelmässigen Abständen frischt Alice die Virendatenbank ihrer Software auf, damit die Datenbestände immer auf dem neusten Stand sind. Andernfalls werden die Viren der jüngsten Generation nicht erkannt. Viele Virenschutzprogramme erlauben das automatische und unkomplizierte Aktualisieren via Internet.

- Alice erstellt regelmässig Sicherheitskopien von den heiklen Datenbeständen auf ihrer Festplatte. Sollte sich doch einmal ein Virus einschleichen und seinem Zerstörungswerk nachgehen, kann Alice immerhin auf diese Sicherheitskopien zurückgreifen.

- Ausserdem erstellt Alice eine Startdiskette für ihr Betriebssystem. Damit kann sie im äussersten Notfall den Rechner auch dann aufstarten, wenn ein Virus wichtige Systemdateien zerstört hat. Wie eine Startdiskette erstellt wird, ist in den Handbüchern zu Alices Computer beschrieben.

- In ihren Office-Programmen aktiviert Alice den Makrovirusschutz. So wird sie vor dem Öffnen von Office-Dokumenten gewarnt, falls Makros darin enthalten sind. Alice kann dann bequem entscheiden, ob sie die Makros aktivieren möchte oder nicht.

Kürzlich landete Alice auf einer Web-Seite mit der Begrüssung: «Sie verwenden den Browser Netscape Navigator in der Version 4.05 und eine Bildschirmauflösung von 800x600 Punkten mit 256 Farben. Um diese Web-Seite in der ganzen Schönheit mitverfolgen zu können, sollten Sie auf Navigator 4.73 oder höher wechseln und eine höhere Bildschirmauflösung mit 32 768 Farben wählen.» Die Meldung ist ein typisches Beispiel für ein aktives Element. Ein kleines JavaScript-Programm hat hier einige Werte aus dem Web-Browser von Alice ausgelesen und innerhalb der Web-Seite dargestellt. Aktive Elemente werden häufig dazu benutzt, Web-Seiten an die spezifischen Gegebenheiten bei einer Benutzerin anzupassen.

Sind solche aktiven Elemente unsorgfältig programmiert, kann das zu lästigen Fehlermeldungen oder Browserabstürzen führen. Dieser Fall tritt oft bei Web-Seiten ein, welche die aktuellsten technischen Möglichkeiten ausreizen. Letztlich muss Alice in solchen Fällen selber entscheiden, ob sie das Risiko eingehen will.

Um in den Genuss einer Multimedia-Präsentation auf einer Web-Site zu kommen, wird Alice aufgefordert, ein Plug-in herunterzuladen und auf ihrem Rechner zu installieren. Alice überlegt sich zweimal, ob sie das Risiko eingehen will. Einerseits braucht das Herunterladen und Installieren des Plug-ins Zeit, andererseits hat das Plug-in nach der Installation auf Alices Rechner so ziemlich alle Freiheiten. Wenn die entsprechende Web-Site für Alice nicht von grosser Bedeutung ist, verzichtet sie deshalb auf das Plug-in. Einzig gewisse Standard-Plug-ins hat Alice auf ihrem Rechner installiert.

Kapitel 8

Unerwünschte Daten aus dem Netz

E-Mail ist eine bequeme Sache – schnell und günstig. Alice kann sich gar nicht mehr vorstellen, wie das früher ohne E-Mail war. Briefe, die man ausdrucken, in einen Umschlag stecken und zum Briefkasten tragen musste. Ein lästiges Phänomen hat sich aber in die Welt des elektronischen Briefverkehrs hinübergerettet: Unverlangte Werbesendungen zu allem Möglichen und Unmöglichen verstopfen die Mailbox von Alice.

Beim Briefkasten an der Haustüre kann Alice einen «Stopp Werbung»-Kleber anbringen. Auf diese Weise schützt sie sich vor unadressierten Werbesendungen. Einzig gegenüber adressierter Werbung ist Alice machtlos. Ihr Briefträger soll schliesslich nicht jede Sendung zuerst öffnen und kontrollieren. Gibt es auch im Internet «Stopp Werbung»-Kleber?

Soeben fand Alice die folgende Nachricht in ihrer Mailbox:

> Subject: Good Times!
>
> Here is some important information. Beware of a file called "Good Times". Be careful out there. There is a virus on the Internet being sent by e-mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this warning to all your friends. It may help them a lot.

Alice macht sich grosse Sorgen. Kann es wirklich sein, dass im Internet derart gefährliche Dinge im Umlauf sind? Was soll sie tun?

Vor kurzem hat Alice im *Backstreet Journal* einen Artikel über den Vorsitzenden eines lokalen Gewerkschaftsverbands veröffentlicht. Der Artikel war zugegebenermassen eher kritisch. Aber eine derart heftige Reaktion hätte Alice trotzdem nicht erwartet: Der Vorsitzende hat ihr eine E-Mail geschickt, gespickt mit Schimpfworten der übelsten Sorte. Alice wollte die Sache klären und rief den unfreundlichen Herrn per Telefon an. Doch der Mann behauptete steif und fest, nie eine solche E-Mail verfasst zu haben. Trotzdem trug die E-Mail als Absender

die Adresse des Vorsitzenden der Gewerkschaft. Könnte jemand die E-Mail gefälscht haben?

Alices 12-jährige Tochter Virginia ist völlig ins Internet vernarrt. Manchmal verbringt Virginia ganze Sonntage vor dem Computer und erkundet beim Surfen das Internet bis in die letzten Winkel. Alice hat grundsätzlich nichts gegen diese Internet-Begeisterung. Sie macht sich bloss Sorgen wegen gewisser Inhalte im Internet, denn Virginia hat auf alles Mögliche Zugriff. Im Alltag hat Alice gewisse Anhaltspunkte, weil problematische Inhalte im Kino, auf einer CD oder in einem Videofilm entsprechend deklariert werden. Welche Möglichkeiten bieten sich Alice im weltweiten Datennetz an?

Spamming – die Werbeflut aus dem Internet

Das im Internet am häufigsten missbrauchte Stück persönlicher Information ist wohl die E-Mail-Adresse. Wer kennt sie nicht, die ungewünschte elektronische Wurfsendung in der eigenen Mailbox, die das schnelle Geld verspricht oder auf die neuste pornografische Web-Site aufmerksam macht? Die Absenderadresse ist meist frei erfunden.

Spamming, so wird der Massenversand von Werbe-E-Mails genannt. Eine verbreitete Erklärung führt den Begriff auf das gleichnamige amerikanische Büchsenfleisch zurück, das als Massenprodukt vermarktet wurde und ähnlich unbeliebt ist wie Spam-Mails. Die meisten Spam-Mails betreiben Werbung für ein bestimmtes Produkt, eine Dienstleistung oder ein Angebot im Internet. Das folgende Beispiel wirbt passenderweise für das billige Versenden von Spam-Mails.

Subject: BULK E-MAIL CAN WORK 4 YOU!!

We offer some of the best bulk e-mail prices on the Internet. Bulk e-mail can get you the best exposure on the net. What makes this kind of advertising so effective is the fact that you go to the potential customer. Not like search engines or print ads that the potential customer has to do all the searching.
What we offer:

$200.00 for 1 million e-mails sent
$400.00 for 3 million e-mails sent
$600.00 for 5 million e-mails sent
$800.00 for 7 million e-mails sent
$1000.00 for 10 million e-mails sent

So why not give us a call and see what it is that we can do for you. Call anytime 209-669-0176.

Kettenbriefe sind eine besondere Art von Spam-Mails. Kettenbriefe berichten häufig vom herzerweichenden Schicksal einer fiktiven Person. Andere Kettenbriefe haben einen finanziellen Hintergrund. Den Empfängern wird für jede verschickte E-Mail Geld versprochen. In beiden Fällen werden die Empfänger von Kettenbriefen aufgefordert, die Nachricht an möglichst viele Bekannte weiterzuleiten. Das Schneeballprinzip lässt die Zahl der versandten E-Mails oft rasant ansteigen.

Little Jessica Mydek is seven years old and is suffering from an acute and very rare case of cerebral carcinoma. This condition causes severe malignant brain tumors and is a terminal illness. The doctors have given her six months to live.

As part of her dying wish, she wanted to start a chain letter to inform people of this condition and to send people the message to live life to the fullest and enjoy every moment, a chance that she will never have. Furthermore, the American Cancer Society and several corporate sponsors have agreed to donate three cents toward continuing cancer research for every new person that gets forwarded this message. Please give Jessica and all cancer victims a chance.

Die Betreiber von Spamming werden *Spammer* genannt. Manche Spammer verschicken ihre Nachrichten an Millionen von Empfängern. Stellt sich die Frage: Woher kriegen Spammer all die E-Mail-Adressen?

Es gibt verschiedene Möglichkeiten. Normale Web-Seiten etwa lassen sich automatisiert durchsuchen. E-Mail-Adressen zeichnen sich durch das charakteristische «@»-Zeichen aus und sind deshalb leicht aufzuspüren. Ein Grossteil aller Web-Seiten ist mit einer E-Mail-Adresse ausgestattet, um den Besuchern eine Kontaktmöglichkeit anzubieten. Ausserdem gibt es im WWW «Telefonbücher» für E-Mail-Adressen. Es handelt sich dabei um spezielle Dienstleistungen, die das Suchen nach E-Mail-Adressen aufgrund des Namens einer Person erlauben.

Die *Diskussionsforen* im Internet – die so genannten *Newsgroups* – sind ebenfalls nützlich für Spammer. Es existieren tausende von Newsgroups. Jede Newsgroup deckt ein bestimmtes Thema ab. Beliebige Internet-Benutzer können in einer Newsgroup mitlesen oder eigene Artikel veröffentlichen. Jeder Artikel ist üblicherweise mit der E-Mail-Adresse des Absenders versehen. Davon können Spammer doppelt profitieren: In den Newsgroups gelangen sie an die begehrten Adressen. Zudem gibt ihnen das Thema der Newsgroup wertvolle Hinweise auf die Interessen der jeweiligen Person. Diese Information lässt sich für gezieltere Werbung ausnützen.

April, April, jahrein, jahraus – Pseudoviren

Ein *Pseudovirus* ist eine Falschmeldung. Im englischen Sprachraum spricht man von einem *Hoax*. Die «Good Times»-Warnung, mit der Alice konfrontiert war, ist ein typisches Beispiel für ein Pseudovirus. Es gibt kein echtes Virus namens «Good Times».

Viele Pseudoviren funktionieren wie Kettenbriefe. Sie legen den Lesern nahe, die Warnung an ihre Bekannten zu verschicken, um auch sie vor Schaden zu bewahren. Insofern kann die Warnmeldung selbst als ein Virus angesehen werden. Pseudoviren richten Schaden an, indem sie die Zeit der Leser sowie technische Ressourcen für die Bearbeitung und Übermittlung verschwenden.

Vielen Internet-Anwendern fehlen das nötige technische Hintergrundwissen sowie die Erfahrung, um zwischen echten Virenmeldungen und Falschmeldungen zu unterscheiden. Zumal die Falschmeldungen häufig mit plausibel anmutenden Fachausdrücken gespickt sind.

So wie das folgende Beispiel:

> You have been selected for an extensive port and virus implementation scan by SARC, a division of Symantec Inc. During the next few days your system will be aggressively attacked by various new multimorphic, stealthmode Internet virus programmes. Any system damage or data loss sustained during these attacks can be reported to our e-mail response team.
>
> Please use your e-mail client and other programs like IRC or ICQ frequently to support influx of our destructive payloads. Already a payload has been attached and executed by your mail client to ensure satisfying results upon reading this message.
>
> Thank you for your cooperation during this important research phase.
> Symantec AntiVirus Research Center (SARC)

In diesem Fall ist die E-Mail sogar von einem angesehenen Produzenten von Antivirensoftware unterschrieben. Allerdings hat der Hersteller nichts mit dieser Meldung zu tun, sie wurde von einer anderen Person verfasst.

Inhaltskontrolle

Alice und ihre Tochter Virginia besuchen Bob in seinem Plattenladen. Während sich Alice und Bob miteinander unterhalten, stöbert Virginia in den CDs. Sie findet ein spannendes Album, das sie gerne behalten möchte. Alice aber hat Bedenken in Bezug auf die Songtexte. Sie hat zwei Möglichkeiten zur Inhaltskontrolle.

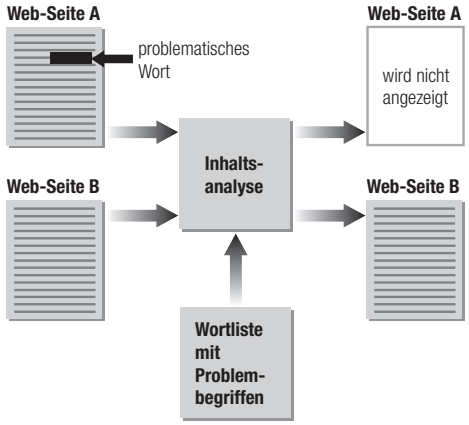
- *Taxierung*: Alice prüft, ob eine Warnung wie «Parental Advisory – Explicit Lyrics» auf der CD angebracht ist.
- *Inhaltsanalyse*: Alice blättert durch das beigelegte Booklet mit den Songtexten, oder sie hört sich einige der Stücke an.

Diese beiden Techniken der Inhaltskontrolle kommen auch im Internet in Form von *Filtersoftware* zur Anwendung. Eine Filtersoftware überwacht die Downloads aus dem Internet und entscheidet aufgrund

gewisser Kriterien, welche Dokumente dem Benutzer angezeigt werden und welche nicht. Filterprogramme sind eine technische Möglichkeit, sich selbst oder andere Personen vor problematischen Inhalten aus dem Internet zu schützen. Zum Beispiel werden gemeinhin gewisse Themen wie Pornografie oder die Darstellung übermässiger Gewalt für sehr junge Personen als ungeeignet erachtet. Manche Firmen setzen Techniken zur Inhaltskontrolle ein, um für ihre Angestellten alles zu sperren, was für die Arbeit nicht benötigt wird.

Inhaltsanalyse

Bei dieser Technik trifft ein Programm bei jedem neuen Dokument die Entscheidung darüber, ob es angezeigt werden soll oder nicht. Das Programm stützt sich auf eine Sammlung von problematischen Begriffen. Jedes Dokument wird analysiert. Falls heikle Begriffe in einer bestimmten Kombination und Menge im Dokument auftauchen, wird es verworfen. Andernfalls wird das Dokument angezeigt.



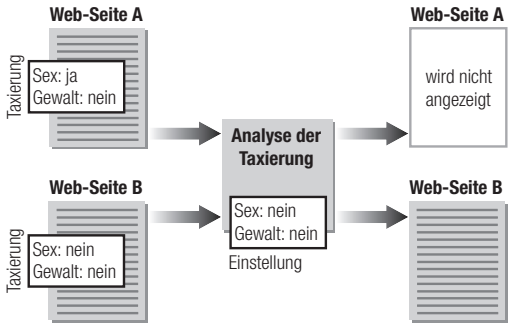
Das Problem bei dieser Technik: Es kann vorkommen, dass auch unproblematische Dokumente ausgeschlossen werden. Beispielsweise wird ein medizinisches Dokument über Geschlechtskrankheiten unter Umständen fälschlicherweise gesperrt. Zudem können mit Hilfe

der Inhaltsanalyse keine Bilder, Tondokumente oder Videosequenzen beurteilt werden.

Taxierung

Bei dieser Technik wird für jedes Dokument eine Taxierung festgelegt und zur Verfügung gestellt. Die Bewertung des Dokumentinhalts wird häufig von Menschenhand durchgeführt. Es gibt Firmen, die sich auf dieses Geschäft spezialisieren.

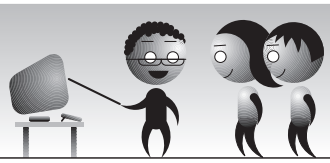
Beim Browsen im Internet sorgt ein Programm dafür, dass für jedes anzuzeigende Dokument die zugehörige Taxierung geprüft wird. Das Programm entscheidet anhand der Taxierung, ob das Dokument angezeigt werden darf.



Der Vorteil manueller Taxierung liegt auf der Hand: Menschen können nicht nur Texte, sondern auch Bilder, Tondateien oder Videosequenzen taxieren. Diesbezüglich ist Taxierung der Inhaltsanalyse überlegen.

Wie aber soll mit Dokumenten umgegangen werden, für die keine Taxierung existiert? Die meisten Programme sperren solche Dokumente. Noch heikler sind Dokumente, die nach der Taxierung verändert werden. Alle geänderten Dokumente müssen erneut taxiert werden. Probleme dieser Art treten bei der Inhaltsanalyse nicht auf.

Praxis



Schutz vor Spamming

Die wichtigste Massnahme im Zusammenhang mit Spamming lautet: ignorieren! Auf keinen Fall sollte auf Spam-Mails mit einer Beschwerde beim Absender reagiert werden. Drei Gründe:

- Oft ist die Absenderadresse schon kurz nach dem Versand der Spam-Mails nicht mehr gültig. Viele Spammer richten eigens für das Verschicken ihrer Spammings ein E-Mail-Konto ein, das anschliessend geschlossen wird. Jede Antwort hat lediglich eine Fehlermeldung zur Folge.
- Spammer benutzen oft gefälschte Absenderadressen. In diesem Fall landen die Beschwerden am falschen Ort – das Spamming richtet noch mehr indirekten Schaden an.
- Sollte die Absenderadresse ausnahmsweise gültig sein, ist das Beantworten trotzdem nicht zu empfehlen. Dadurch wird nur bestätigt, dass die eigene E-Mail-Adresse intakt ist. Die Adresse gewinnt für die Spammer an Wert.

Fazit: Für Internet-Anwender ist es am schnellsten, billigsten und bequemsten, Spam-Mails per Knopfdruck zu löschen und ansonsten zu ignorieren.

Gefälschte E-Mails

Mallet möchte eine E-Mail unter falschem Namen verschicken. Das ist kein Problem, denn in den meisten E-Mail-Programmen gibt der Benutzer seinen Namen sowie seine E-Mail-Adresse selber ein. Mallet

kann in den Einstellungen zum Beispiel den Namen «Bob» und die Adresse `bob@sonicdreams.com` eintragen.

Erfreulicherweise funktioniert diese sehr simple Art der Fälschung längst nicht immer. Die für den Mail-Transport verantwortlichen Mail-Server im Internet können nämlich die Adressen prüfen. Meistens wird die Domain geprüft. Die Domain ist der Adressteil hinter dem «@»-Zeichen, zum Beispiel `sonicdreams.com`. Eine E-Mail wird nur dann akzeptiert, wenn die Domain der Absenderadresse mit der Domain des Mail-Servers übereinstimmt. Im Beispiel: Mallets Internet-Provider HappyNet unterhält einen Mail-Server in der Domain `happynet.com`. Der Mail-Server sollte folglich keine E-Mails einer Absenderadresse aus der Domain `sonicdreams.com` akzeptieren.

Aber es existieren weitere, trickreichere Fälschungsverfahren. Beispielsweise können manche Mail-Server direkt angesprochen werden, um ihnen neben einer falschen E-Mail-Adresse auch einen gefälschten Ursprungsort vorzutäuschen. Dieses Vortäuschen wird in der Fachsprache *Spoofing* genannt. Ob Spoofing möglich ist, hängt entscheidend von der Konfiguration eines Mail-Servers ab.

Absenderadressen prüfen

Alice erhält eine E-Mail, an deren Echtheit sie zweifelt. Wie kann sie prüfen, ob die Absenderadresse gefälscht wurde? Sie schreibt zurück und fragt nach. E-Mails abzufangen ist ungleich schwieriger, als sie zu fälschen. Die Rückfrage wird mit grosser Wahrscheinlichkeit am richtigen Ort landen. Oder es wird eine Fehlermeldung ausgelöst, falls die Absenderadresse nicht existiert. So oder so – die Fälschung ist entlarvt.

Eine E-Mail besteht aus zwei Teilen – der eigentlichen Nachricht sowie Zusatzinformationen wie Absender, Empfänger oder Zeitpunkt des Verschickens. Der Teil der E-Mail mit den Zusatzinformationen heisst *Kopf* oder *Header*. Im Header ist auch der Weg aufgezeichnet, den die E-Mail im Internet zurückgelegt hat. Es handelt sich dabei um eine Liste von Host-Namen oder IP-Adressen der beteiligten Mail-Server. Diese Liste lässt Rückschlüsse auf den tatsächlichen Absender zu.

Alice kann sich den Header einer E-Mail in ihrem Mail-Programm anzeigen lassen. Das folgende Beispiel zeigt eine E-Mail, die Mallet im Namen von Bob geschrieben hat:

```
Received: from mail.happynet.com [23.24.25.1])
    by mail.wondersurf.com (8.8.8/8.8.8) with ESMTP id QAA24742;
    Fri, 4 Feb 2000 16:26:44 +0100 (MET)
Received: from mallet.happynet.com [123.023.76.66])
    by mail.happynet.com (8.8.8/8.8.8) with ESMTP id QAA14795
    Fri, 4 Feb 2000 16:26:42 +0100 (MET)
Date: Fri, 4 Feb 2000 16:26:41 +0100 (MET)
To: alice@wondersurf.com
From: bob@sonicdreams.com
Subject: Ich mach Schluss
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain

Hallo Alice

Ich habe mich nach reiflicher Überlegung dazu entschlossen, Schluss zu ma-
chen. Es tut mir leid für dich, aber ich kann meine Gefühle für Melissa nicht
länger verleugnen.

Bob

P.S. Gestern hab ich Mallet getroffen. Er ist gar kein so schlechter Typ, wie
wir immer gedacht haben. Mach doch mal mit ihm ab!
```

Die «From»-Zeile zeigt, dass die Mail vermeintlich von Bobs E-Mail-Adresse `bob@sonicdreams.com` stammt. Doch diese Angabe stimmt nicht mit dem Weg überein, den die E-Mail im Internet genommen hat. Aufgrund der «Received»-Zeilen im Header wurde die Mail von einem Rechner namens `mallet.happynet.com` zum Mail-Server von HappyNet (`mail.happynet.com`) und anschliessend zum Mail-Server bei Alices Provider WonderSurf geschickt. Offenbar besitzt Mallet einen Computer, der ständig am Netz hängt und über einen eigenen Namen verfügt. Damit ist die Fälschung aufgedeckt. Eine Mail des «echten» Bob würde vom einem Rechner bei SonicDreams stammen und über Bobs Provider geliefert.

Mallet könnte allerdings geschickter vorgehen, indem er seinem Rechner einen anderen Namen gibt und versucht, die E-Mail via Bobs Internet-Provider zu verschicken. In solchen Fällen genügt die einfache Untersuchung anhand der Rechnernamen nicht. Stattdessen müsste Alice die IP-Adressen der beteiligten Rechner überprüfen. Bei wichtigen E-Mails wie Verträgen oder anderen Angeboten verlässt sie sich deshalb besser auf die Authentifizierung des Absenders mittels Zertifikaten und digitaler Unterschriften.

Inhaltskontrolle an verschiedenen Orten

Filterprogramme zur Inhaltskontrolle können auf unterschiedlichen Ebenen eingesetzt werden:

- *Web-Angebote*

  Im Internet existieren verschiedene Angebote, die das Filtern von Dokumenten gleich selber übernehmen. Es handelt sich dabei häufig um Informationsdienste wie Internet-Kataloge oder Suchdienste. Manche Dienste ermöglichen das Aktivieren eines Filters zur Inhaltskontrolle. Andere Dienste stellen ihr Angebot für verschiedene Zielgruppen zur Verfügung – zum Beispiel speziell für Kinder.

- *Internet-Provider*

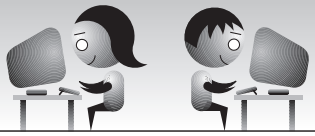
  Manche Internet-Provider bieten ebenfalls Möglichkeiten zur Inhaltskontrolle an. So kann beispielsweise ein Proxy-Server Filterfunktionen übernehmen.

  Einige Internet-Provider betreiben eine spezielle Art der Inhaltskontrolle. Sie machen auf den eigenen Web-Servern keine Web-Seiten mit problematischen Inhalten zugänglich. In bestimmten Ländern ist diese Art der Inhaltskontrolle sogar von staatlichen Behörden vorgeschrieben. Das Vorgehen ist umstritten, weil es von vielen Personen als Zensur angesehen wird.

- *Privat-PC*

  Die meisten Systeme arbeiten auf dem eigenen Rechner, überwachen die Internet-Verbindung und blockieren heikle Dokumente aufgrund von konfigurierbaren Vorgaben. In der Regel hat ein Benutzer über Systeme dieser Art die beste Kontrolle. Andererseits besteht die Gefahr, dass ein versierter Benutzer das Kontrollsystem durch Eingriffe in das Betriebssystem deaktivieren kann.

Anwendung



Leider gibt es im Internet keine «Stopp Werbung»-Kleber. Zwar bemühen sich die Internet-Provider, unerwünschte Massensendungen nicht an die Kunden auszuliefern. Trotzdem schlüpfen immer wieder Werbesendungen durch die Maschen.

Es lohnt sich für Alice nicht, sich zu ärgern. Die einfachste Massnahme gegen Spamming ist es, die Mails sofort zu löschen. Alice macht auf keinen Fall den Fehler, auf eine Spam-Mail zu antworten.

E-Mails zu fälschen ist nicht allzu schwierig. Seit Alice das weiss, überprüft sie bei wichtigen E-Mails den Absender. Im Idealfall sind die E-Mails digital unterschrieben. Dann kann Alice die Echtheit anhand des Zertifikats überprüfen. In den übrigen Fällen ruft oder schreibt Alice zuerst zurück und fragt beim mutmasslichen Absender nach. Genauso macht es Alice schliesslich seit langem bei Briefen oder Faxmeldungen mit brisantem Inhalt.

Im Zusammenhang mit Pseudoviren und Kettenbriefen hat sich Alice die folgenden Verhaltensregeln gemerkt:

- Alice tritt jeder E-Mail-Nachricht dieser Art mit viel Misstrauen gegenüber. Sie versucht abzuschätzen, wie plausibel die Meldung erscheint. Wer ist der Absender? Ist eine offizielle Behörde zitiert? Gibt es auf der Web-Site dieser Behörde entsprechende Informationen?
- Im WWW existieren verschiedene Web-Seiten, die ausführliche Listen mit den bekannten Falschmeldungen unterhalten. Alice schaut auf einer dieser Listen nach. Falls die Nachricht dort vermerkt ist, kann sie getrost ignoriert werden.
- Im Zweifelsfall ignoriert Alice die Warnmeldung. Erfahrungsgemäss kommt es äusserst selten vor, dass auf diesem Weg vor Viren oder anderen Problemen und Ereignissen gewarnt wird.

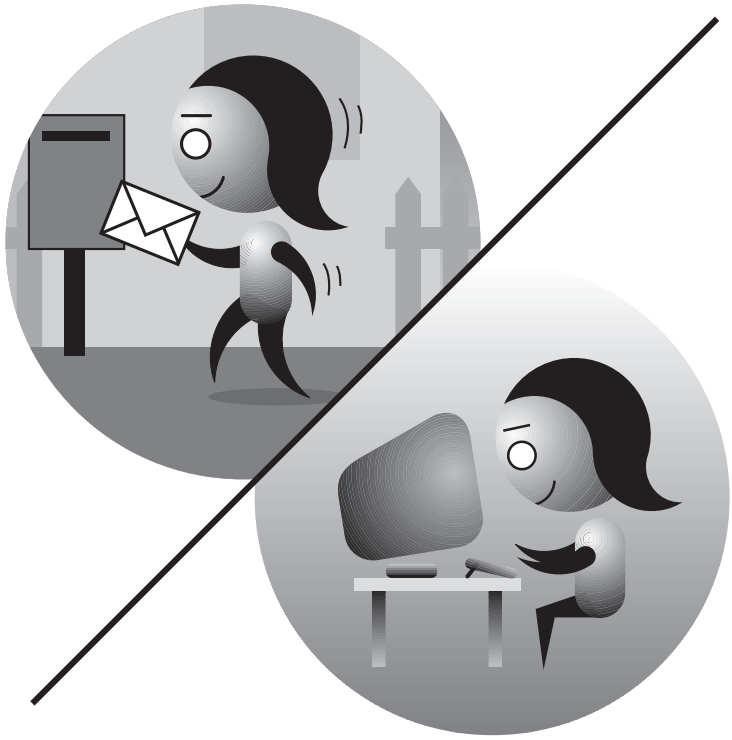
Nun kann Alice über Meldungen wie die folgende nur noch lachen:

> Subject: Internet Cleanup Day
>
> As many of you know, each year the Internet must be shut down for 24 hours in order to allow us to clean it. The cleaning process, which eliminates dead e-mail and inactive ftp, www and gopher sites, allows for a better working and faster Internet. This year, the cleaning process will take place on February 28.
>
> In order to protect your valuable data from deletion we ask that you do the following: (1) Disconnect all terminals from their Internet connections. (2) Shut down all Internet servers, or disconnect them from the Internet. (3) Disconnect all disks from any connections to the Internet. (4) Refrain from connecting any computer to the Internet in any way.
>
> We understand the inconvenience that this may cause some Internet users, and we apologize. However, we are certain that any inconveniences will be more than made up for by the increased speed and efficiency of the Internet, once it has been cleared of electronic flotsam and jetsam.
>
> We thank you for your cooperation.

Und wie hält es Alice mit der Inhaltskontrolle? Wie schützt sie ihre Tochter Virginia vor heiklen Web-Seiten? Alice gibt sich keinen Illusionen hin: Auch bei der Altpapiersammlung in der Schule kommt Virginia mit zweifelhaften Erzeugnissen in Kontakt. Auf den Dutzenden von Fernsehkanälen wird ebenfalls keine heile Welt präsentiert. Alice hat längst erkannt: Gesellschaftliche Probleme lassen sich nur selten mit technischen Massnahmen lösen. Anstatt sich auf den trügerischen Schutz von Filtersoftware zu verlassen, vertraut Alice in der Erziehung lieber auf ein intaktes soziales Umfeld. Sie nimmt sich die Zeit, hin und wieder mit Virginia gemeinsam im Internet zu surfen. Genauso wie sie oft zusammen mit Virginia vor dem Fernseher sitzt und gewisse Sendungen diskutiert.

Kapitel 9

Sicherheit im Alltag – Sicherheit im Internet



Kaum jemand ist so unvorsichtig und lässt die Türen zu seiner Wohnung Tag und Nacht offen oder deponiert den Schlüssel gut sichtbar neben der Eingangstüre. Nur wenige Leute bewahren ihr gesamtes Vermögen vermeintlich gut versteckt unter der Matratze auf, und niemand überlässt seine Kreditkarte samt PIN-Code leihweise einem Unbekannten. Intime Telefongespräche wickelt man kaum via Handy während der Stosszeit im überfüllten Bus ab. Beim Kauf oder Verkauf eines Hauses zieht man üblicherweise einen amtlichen Notar bei, der die Rechtmässigkeit des Geschäftes überwacht. Bei grösseren Bankgeschäften verlangen die meisten Banken einen Identitätsnachweis. Viele Firmen kontrollieren, wer das Firmengelände betritt oder verlässt. Und wer an einem Wettbewerb «Der schrägste Gartenzwerg» teilnimmt, muss davon ausgehen, dass er künftig regelmässig mit Werbung rund um Gartenbau und -pflege bedient wird. Kindern wird beigebracht, dass man von fremden Leuten keine Süssigkeiten entgegennehmen darf, und verantwortungsbewusste Eltern kaufen ihren Sprösslingen nicht jeden beliebigen Videofilm.

Daneben gibt es die übervorsichtigen Leute: Die Haustüre wird dreifach gesichert. Niemand, aber wirklich gar niemand besitzt einen zweiten Schlüssel. Alle Fenster sind vergittert, und die Wohnung, die Garage und das Auto werden mittels Alarmanlage überwacht. Wertvolle Gegenstände werden im Tresor einer Bank aufbewahrt, in der Wohnung stehen nur Billigmöbel. Eingehende Briefpost wird durchleuchtet und auf mögliche Briefbomben untersucht. Die Telefonnummer ist geheim und taucht in keinem Verzeichnis auf. Das Haus wird nur verlassen, wenn es wirklich nicht anders geht. Die Kinder werden mit dem Auto zur Schule gebracht und abgeholt, und es ist ihnen strengstens untersagt, irgendetwas aus dem Familienleben in der Schule zu erzählen. Am Bancomaten werden nur kleine Beiträge abgehoben, sofort das Passwort geändert und die Nummern der Banknoten notiert. Von den einzelnen Teilen des Geschirrs wird immer gleich ein Reserveexemplar gekauft: Jedes Stück ist in zweifacher Ausführung vorhanden. Und jede Zugsauskunft wird durch nochmalige Anfrage bei einem anderen Bahnhof überprüft.

Man kann sich das Leben von solchen Leuten gut vorstellen: Wenn eine Wasserleitung bricht, besitzt kein Nachbar einen Schlüssel. Dau-

ernde Fehlalarme und die vergitterten Fenster mindern die Lebensqualität gewaltig. Das tägliche Leben ist geprägt von Paranoia. Der Spass bleibt auf der Strecke.

Weder übertriebene Vorsicht noch fahrlässige Sorglosigkeit sind im Alltag angebracht. In Sachen Sicherheit gilt es, einen vernünftigen Mittelweg zu finden. Das Wissen um mögliche Gefahren und die Einschätzung der Risiken sind Voraussetzung für eine angebrachte Verhaltensweise. Deshalb wird regelmässig auf die im Alltag lauernden Gefahren hingewiesen oder sicherheitsrelevante Aufklärung betrieben: Unfallverhütungskampagnen, Ratschläge der Polizei zu Diebstahl und anderen Gefahren, Informationen von Banken bezüglich Zahlungsverkehr und Geldbezug an Bankautomaten, Hinweise auf mögliche Nebenwirkungen von Medikamenten. Stete Sensibilisierung und das Bewusstmachen der im Alltag lauernden Gefahren und Risiken sind ein wichtiges Element unserer Gesellschaft. Mit Panikmache und dem Schüren übertriebener Angst hat diese Prävention nichts zu tun.

Genauso verhält es sich mit der Sicherheit im Internet. Das Internet sollte nicht ohne ein Bewusstsein um die potenziellen Gefahren, Risiken und Probleme genutzt werden. Trotzdem ist das Internet keine Räuberhöhle, wo hinter jeder Ecke ein Bösewicht lauert. Im Internet soll man sich deshalb wie im Alltag verhalten: mit der nötigen Portion Vorsicht, ohne dabei einem übertriebenen Sicherheitsdenken zu verfallen.

Der einzige Unterschied bezüglich Sicherheit im Internet und im Alltag: Im Alltag sind wir uns der meisten Gefahren bewusst und haben uns zweckmässige Verhaltensweisen angeeignet. Das Internet ist ein neues Medium, in dem wir uns vorerst ohne grossen Erfahrungshintergrund bewegen. Ein Bewusstsein rund um sicherheitsrelevante Aspekte im Internet fehlt noch in breiten Bevölkerungskreisen. Hier sind viel Aufklärungsarbeit und Ausbildung nötig! Wenn dieses Buch die Leserin und den Leser für Sicherheitsfragen im Zusammenhang mit dem Internet sensibilisiert hat, ist damit ein Schritt in Richtung kompetente und verantwortungsbewusste Nutzung der neuen Informations- und Kommunikationstechnologien gemacht.

Stichwortverzeichnis