Serie

Sicherheit

10/99 Risiko Festplatte
Spionage und Sabotage am Mac

12/99 Unfall, Ungeschick, Ungeziefer
Festplattencrashs, versehentliches Löschen, Virenbefall und andere Kalamitäten

Tatort Internet

Das Internet ist kein so gefährliches Pflaster, wie viele glauben. Aber nur wer die Risiken kennt, kann sich sicher durch den Cyberspace bewegen. Im zweiten Teil unserer Serie über Sicherheit am Mac räumen wir mit den Mythen um das Internet auf.

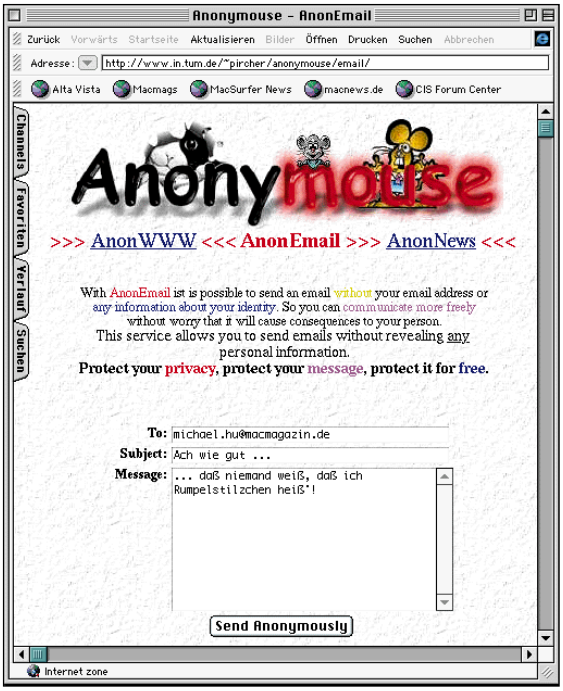
Auf CD-ROM: OTSessionWatcher, Freeware PGP 6.5.1, Demo von SafeMail 2.0.1, ältere Artikel aus Mac MAGAZIN

Im Internet weiß niemand, daß du ein Hund bist", hat Nicholas Negroponte, Gründer des MIT Media Lab, einmal gesagt. Die naive Annahme von der Anonymität des Surfers ist allerdings den vielen Mythen zuzurechnen, die das Internet umgeben. Ebenso leichtfertig ist freilich die – selbst von ansonsten seriösen Medien verbreitete – Darstellung, der Internet-Zugang eröffne kriminellen Hackern den ungehinderten Zugang zu sämtlichen Daten, E-Mails oder gar dem Bankkonto des Surfers. Tatsächlich kann sich niemand im Internet bewegen, ohne dabei eine Datenspur zu hinterlassen. Und wie auf dem unbekannten Terrain einer fremden Stadt helfen nur zuverlässige Informationen, die vorhandenen Risiken richtig einzuschätzen und sich vor den Gefahren wirksam zu schützen.

Um zu beweisen, daß die bei der Datenübertragung oder dem Zugriff auf Webserver oder Homepages lauernden Risiken durchaus in den Griff zu bekommen sind, wollen wir erklären, was dabei vor sich geht. Der erste Teil soll davon handeln, was der Surfer automatisch von sich verrät und was Dritte mit diesem Wissen anfangen können. Der zweite Teil beschäftigt sich damit, was Unbefugte – Hacker unter Umständen – hinterrücks über Ihre Daten in Erfahrung bringen können, und schließlich folgt ein Abschnitt über den sicheren Versand von E-Mails.

Spuren im Netz

Als Internetnutzer ist Ihnen die Oberfläche des weltweiten Netzwerks ja vertraut: Ein Klick mit der Maus öffnet eine Webseite, ein weiterer fragt die vorliegende E-Mail ab, und mit einem dritten schicken Sie eine Nachricht an eine Newsgroup ab. Verborgen unter der polierten Oberfläche tauscht Ihre Software Datenpakete mit nicht immer offensichtlichem Inhalt mit verschiedenen Servern aus. Der Zugriff auf eine Webseite beispielsweise erfordert die Übertragung von HTML-Dateien und Grafikdokumenten. Allein damit ist es allerdings nicht getan. Wenn Sie nachvollziehen wollen, wie der Datenaustausch im Internet wirklich funktioniert, müssen Sie eine Software wie etwa OTSessionWatcher einsetzen (Shareware, 35 Dollar, auf der Heft-CD), die auch die in diesem Artikel gezeigten Beispiele aufzeichnete. Auf den ersten Blick mögen diese Ihnen vielleicht wie Buchstabensalat erscheinen, was sie allerdings nicht sind.



Mit dem Anonymouse-Dienst können Sie E-Mails anonym verschicken und unerkannt durchs Web surfen.

```
Send data (359 bytes).
GET / HTTP/1.1
Host: www.macmagazin.de
Accept-Language: de
Referer:
http://www.macup.com/cgi-
bin/ssi/home.shtml
User-Agent: Mozilla/4.0 (compa-
tible; MSIE 4.01; Mac_PowerPC)
UA-OS: MacOS
UA-CPU: PPC
```

IP-Nummer. Beispiel 1 zeigt ein Datenpaket, mit dem ein Browser eine Webseite anfordert, im vorliegenden Fall unsere Startseite www.macmagazin.de. Der Browser verrät damit noch mehr als nur das Interesse des Anwenders an dieser Seite: Zunächst einmal wird mit allen Daten die IP-Nummer des Absenders übertragen, anhand derer der Surfer später prinzipiell identifiziert werden kann; doch dazu unten noch mehr. Die Abfrage der HTML-Seite verrät dem Webserver zusätzlich, daß der Anwender die Seiten in deutscher Sprache bevorzugt (Accept-Language), den Microsoft Internet Explorer in Version 4.01 für Power-Macs benutzt (User-Agent), diese Abfrage von einem Power-Mac (UA-CPU) unter Mac OS (UA-OS) abschickt und auf die abgefragte Seite von www.macup.com, also der Website unseres Schwestermagazins MACup, verwiesen wurde (Referer).

Webserver können diese Zusatzinformationen ignorieren, protokollieren sie aber zumindest im Logfile mit, was dann statistische Auswertungen erlaubt. Auf diese Weise können wir zum Beispiel herausfinden, welchen Browser unsere Leser bevorzugen (Netscapes Navigator) und wieviele Windows-Anwender auf unser Online-Angebot zugreifen. Ein Webserver kann diese Informationen aber auch dazu verwenden, eine auf den jeweiligen Benutzer zugeschnittene Version der abgefragten Seite zu erzeugen. So läßt sich auch erklären, warum deutsche Surfer zum Beispiel auch auf US-Sites auffallend häufig auf deutsche Werbebanner stoßen, ein Browserhersteller zum Update auf die neueste Version aufmerksam macht oder zum Umstieg auf sein Produkt auffordern kann und ähnliches mehr.

Die Referer-Angabe kann beispielsweise für die Abrechnung von Provisionen benutzt werden (wer auf die Bestellseite eines Versenders verweist, bekommt eine Provision für jede daraufhin getätigte Bestellung) oder aber den Zugriff auf eine Seite beschränken: Einer Downloadseite könnte dazu eine Seite mit den Lizenzbestimmungen vorgeschaltet sein, wobei der Server den Zugriff nur dann akzeptiert, wenn man von der Seite mit dem Kleingedruckten dorthin verwiesen wurde. Die Anwender des neuen Webbrowsers iCab (in Version 1.7 auf unserer CD zu finden) haben übrigens die Möglichkeit, die Übermittlung des „Referer“ grundsätzlich zu unterbinden.

> Jeder Surfer hinterläßt eine Datenspur im Internet

Eindeutige Identifizierung. Prinzipiell kann der Server all diese Angaben speichern, um ein Benutzerprofil anzulegen, das bei allen weiteren Besuchen des Surfers aktualisiert und erweitert wird. Dafür müßte der Websurfer allerdings eindeutig identifiziert werden, wofür die IP-Nummer meist nicht ausreicht. In Firmennetzwerken, die über einen Router und eine Standleitung an das Internet angebunden sind, besitzt meist jeder Rechner eine feste IP-Nummer, welche recht mühelos Rückschlüsse auf den Internetprovider und die Firma zuläßt. Der Anwender ist damit allerdings kaum eindeutig zu identifizieren, denn nicht immer nutzt nur ein Mitarbeiter (und stets derselbe) eine bestimmte Maschine. Wer sich per Telefonleitung bei seinem Provider einwählt, bekommt ohnehin dynamisch eine freie IP-Nummer aus einem Pool zugeteilt, so daß sich hinter derselben Nummer Tausende von Nutzern verbergen können.

Zur eindeutigen Identifizierung eines Nutzers durch den Server oder auch einen Hacker taugt die IP-Nummer also nicht, weshalb zum Anlegen von Benutzerprofilen die sogenannten Cookies eingesetzt werden (siehe unten). Auf der anderen Seite stehen die Daten, anhand derer gerade Nutzer einer Einwahlverbindung dingfest gemacht werden können, durchaus zur Verfügung: Internetprovider sind gesetzlich dazu verpflichtet, die dynamische Zuteilung von IP-Nummern an ihre Kunden zu protokollieren, und müssen bei entsprechenden Anfragen der Strafverfolgungsbehörden, der Verfassungsschutzämter, des MAD und des BND Auskunft darüber erteilen, wer zu einem bestimmten Zeitpunkt unter einer bestimmten IP-Nummer im Internet unterwegs war.

Eine Ausnahme bilden hierbei die Internet-by-call-Anbieter, die die Identität ihrer Kunden nicht kennen können, sofern sie nicht irgendeine Form der Anmeldung erfordern. Ebenso wie ein Erpresser seine Geldübergabeverhandlungen nicht vom heimischen Telefonanschluß, sondern von einer Telefonzelle aus führt, wird Internet-Kriminalität vom Betrug bis zur Verbreitung von Kinderpornografie wohl künftig über Internet-by-call abgewickelt werden. Wie lange diese rechtliche Grauzone noch fortbestehen wird, bleibt abzuwarten.

Spam-Mail, Remailer. Was für die mögliche Enttarnung des Websurfers mit Hilfe seiner IP-Nummer gilt, läßt sich analog auf die Nutzung anderer Dienste wie FTP, News oder E-Mail übertragen. Das TCP/IP-Protokoll des Internet überträgt sämtliche Daten ➔

in kleinen Paketen, die Sender und Empfänger über ihre IP-Nummer identifizieren. Auch wer E-Mails und Nachrichten an Newsgroups abschickt oder sich Dateien von FTP-Servern herunterlädt, hinterläßt eine Datenspur, die ihn über seine IP-Nummer identifiziert. Falls Sie allerdings mit Hilfe der Informationen im Header den Ursprung unerwünschter Werbemails (Spam) herauszufinden versuchen, dann werden Sie kaum den Spammer dingfest machen können. Soweit Spam-Mails nicht von Schnupper-Accounts oder kostenfreien Maildiensten wie etwa Hotmail verschickt werden, bemühen Spammer sich in der Regel, die Herkunft ihrer Mails zu verschleiern. Wie schon in den frühen Tagen des Internets üblich, erlauben zudem die Betreiber einiger Mailserver immer noch jedem, Mails von ihrem Server abzuschicken. Und diese Gutmütigkeit wird nunmehr häufig dazu genutzt, den Spam-Mails eine unverdächtige und irreführende Herkunft zu verleihen.

Mit einer ähnlichen Methode arbeiten anonyme Remailer, die ihre Mails mit einer neuen, anonymisierten Adresse an den Empfänger weiterleiten, so daß dieser die Möglichkeit zum Antworten hat. Weder der Phantasiename des nun anonymen Absenders noch die IP-Nummer erlauben es dem Empfänger, zu erkennen, woher die Mail kommt – nur der Remailer selbst läßt sich als Absender ermitteln. Wenn der Empfänger nun aber eine Antwort schickt, gelangt sie zu dem Remailer, der sie an den tatsächlichen Absender der ursprünglichen Mail weiterleitet. Gleichzeitig ist damit auch die Schwachstelle der Remailer bezeichnet. Denn um Antworten weiterleiten zu können, muß er für jedes verwendete Pseudonym den zugehörigen Klarnamen speichern. In einem konkreten Fall aus dem Jahre 1995 konnte die Scientology-Sekte gerichtlich durchsetzen, daß der finnische Remailer anon.penet.fi die Herkunft einer Mail offenlegen mußte, die angeblich die Rechte von Scientology verletzte.

Einen verbesserten Schutz der Anonymität erreichen Zweifler durch die Verwendung mehrerer hintereinandergeschalteter Remailer, so daß der Zugriff auf die Daten eines Remailers lediglich die Adresse eines weiteren zutage fördert. Unter der Adresse www.in.tum.de/~pircher/anonymicer/ finden Sie ein Angebot, um nicht nur E-Mails anonymisiert zu verschicken, sondern auch auf Newsgroups und HTML-Seiten zugreifen zu können, ohne eine identifizierende Datenspur zurückzulassen.

Cookies

Wie bereits geschildert, ist die IP-Nummer generell nicht geeignet, den Besucher einer Website wiederzuerkennen. Lediglich den Strafverfolgungsbehörden stehen die dazu nötigen Daten zur Verfügung. Nicht nur die Identität des Surfers, sein Name und seine Postanschrift bleiben unbekannt. In der Tat läßt sich via IP-Nummer nicht einmal eruieren, ob der Besucher dieselbe Site schon früher einmal besucht hat, da ihm beim letzten Besuch eine andere Nummer zugeteilt gewesen sein könnte. Eine solche Identifizierung können wiederum „Cookies“ übernehmen. Cookies sind kleine Datenpakete, welche ein Webserver, vermittelt durch den Browser, auf der Festplatte des Surfers speichern kann. Die stillschweigende Einführung des Cookie-Mechanismus vor einigen Jahren schürte die Angst vor den kleinen Krümelmonstern, und die geheimniskrämerische Art, mit der Browser und Server in stiller Kumpanei Cookies austauschten, ohne den Anwender zu informieren, trug nicht gerade dazu bei, diese Ängste zu zerstreuen. Heutzutage bieten alle Browser die Möglichkeit, das Speichern von Cookies mehr oder weniger selektiv zu unterbinden. Da allerdings die Funktionsweise von Cookies nach wie vor nicht allgemein bekannt ist, schalten viele Anwender Cookies einfach ab, was seinerseits zu Problemen führen kann.

Wenn Ihnen ein Cookie suspekt erscheint, können Sie ihn in iCab einfach löschen.

Idee des Cookie-Konzepts. Wenn der Surfer von Besuch zu Besuch einer Website nicht wiederzuerkennen ist, muß der Browser dem Server auf die Sprünge helfen. Der Server schickt dem Browser ein Datenpaket, das dieser auf der Festplatte des Surfers deponiert. Dieses Datenpaket kann Angaben enthalten, die der Surfer bereits über sich gemacht hat, oder einfach nur eine Art Kundennummer, unter der der Server diese in seiner eigenen Datenbank ablegt. Da der Cookie nur Daten beinhalten kann, die der Surfer ohnehin preisgegeben hat, und letzterer sie (im Gesamtumfang von 4 Kilobyte, was freilich selten ausgenutzt wird) auf seiner Festplatte speichert, bleibt der Datenschutz gewährleistet: Auf der Festplatte des Anwenders sind die Daten so sicher oder unsicher wie alle anderen auch. Die Abbildung unten zeigt, wie ein Server mehrere Cookies an den Browser schickt: Die eigentlichen Nutzdaten sind kodiert, was einen gewissen Schutz vor dem Angriff durch trojanische Pferde bietet.

```
Receive data (765 bytes).
HTTP/1.0 302 Found
Set-Cookie: valueclickref_h001
0874_3=a0012963_936289837.49458
4_11;domain=.valueclick.com;
path=/
Set-Cookie: b_s=a0012963&1;
domain=.valueclick.com; path=/;
expires=Mon,01-Nov-1999
16:30:37 GMT
Set-Cookie: c_p=00&1&01&1;
domain=.valueclick.com; path=/;
expires=Tue,29-Feb-2000
16:30:37 GMT
Location: http://stclst01.value
click.com/ad.s/a0012963.gif
```

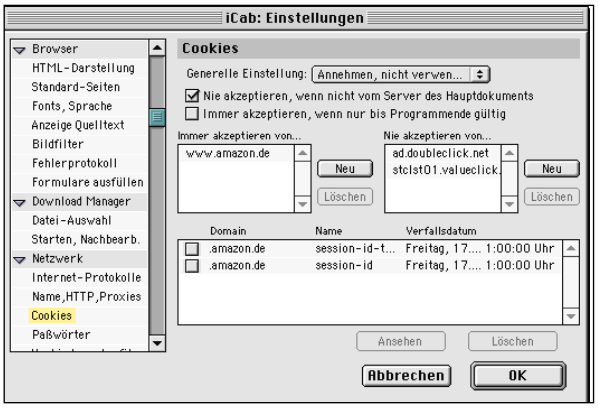
Ob der Browser diese Cookies allerdings tatsächlich speichert, hängt von den Voreinstellungen ab und ist für den Server nicht unmittelbar zu überprüfen. Beim dem nächsten Aufruf einer Seite des Servers schickt der Browser die von diesem Server gespeicherten Cookies an ihn zurück, wie in der Abbildung auf der nachfolgenden Seite zu sehen ist. Anhand dieser Daten kann der Server nunmehr den Besucher wiedererkennen, diesen vielleicht mit Namen begrüßen oder seinen privaten Bereich auf einer Portal-Site öffnen.

```
Send data (481 bytes).
Host: www2.valueclick.com
Accept-Language: de
Referer: http://www.cookiecen
tral.com/mim03.htm
User-Agent: Mozilla/4.0 (compa-
tible; MSIE 4.01; Mac_PowerPC)
UA-OS: MacOS
UA-CPU: PPC
Cookie: valueclickref_h0010874_
3=a0012963_936289837.494584_11;
b_s=a0012963&1; c_p=00&1&01&1
Receive data (765 bytes).
HTTP/1.0 302 Found
Set-Cookie: valueclickref_h0010
874_3=a0012964_936290137.070641
_11; domain=.valueclick.com;
 path=/
Set-Cookie: b_s=a0012964&1; do-
main=.valueclick.com; path=/;
expires=Mon, 01-Nov-1999 16:35:
37 GMT
Set-Cookie: c_p=00&1&01&1; do-
main=.valueclick.com; path=/;
expires=Tue, 29-Feb-2000 16:35:
37 GMT
Location: http://stclst01.value
click.com/ad.s/a0012964.gif
```

(Fast) Unbegründete Angst. Da ein Cookie nicht vom Server abgefragt, sondern vom Browser unaufgefordert und nur von diesem kontrolliert herausgegeben wird, ist ein Zugriff eines Servers auf die von einem anderen gespeicherten Cookies nicht möglich. Die Sorge, daß verschiedene Server über gespeicherte Cookies Daten über einen Anwender austauschen könnten und so ein Bewegungsprofil im Internet erstellen, ist daher unbegründet – allerdings mit einer kleinen Einschränkung: Cookies können nicht allein beim Zugriff auf eine HTML-Seite gesetzt werden, sondern bei jedem Zugriff, beispielsweise auch auf Bilder, Töne oder Filme. Häufig sind es Werbebanner, die den Browser zum Speichern eines Cookies auffordern, während die Webseite als solche gar keine Cookies verwendet.

Werbebanner liegen nicht immer auf dem Server, auf dessen Seiten sie plaziert sind, sondern häufig auch auf dem Server des werbenden Unternehmens beziehungsweise einer Agentur wie DoubleClick.net oder ValueClick.com, die für verschiedene Kunden Werbebanner schalten. Diese beiden Agenturen sind für einen Großteil aller Werbebanner im WWW verantwortlich. Da jeder Zugriff auf ein zum Beispiel von DoubleClick.net geschaltetes Banner einen Zugriff auf deren Server darstellt, unabhängig davon, auf welcher Webseite das Banner erscheint und für welchen Kunden es wirbt, werden ebenfalls die von anderen DoubleClick.net-Bannern gesetzten Cookies übermittelt. Eine solche Agentur ist auf diese Weise grundsätzlich in der Lage, den Weg des Surfers über all jene Websites zu verfolgen, die ihre Werbebanner zeigen.

Online-Werber nutzen die so gewonnenen Informationen aus, um ihre Werbung mit geringeren Streuverlusten an ihre Zielgruppen heranzubringen. Da erst bei Zugriff auf die Seite bestimmt wird, welches Banner auf der Seite erscheinen soll, können die Firmen ihre Werbung auf das vermutete Interessenprofil des Surfers abstimmen. Falls Sie es den Werbern nicht ganz so einfach machen wollen, sollten Sie die von Werbebannern gesetzten Cookies zurückweisen. Die Konfigurationsmöglichkeiten älterer Browser hatten sich darauf beschränkt, Cookies entweder pauschal abzulehnen, sie ebenso pauschal zu akzeptieren oder allenfalls den Anwender von Fall zu Fall entscheiden zu lassen, was lästig und zeitraubend war. Aktuelle Browserversionen hingegen gestatten auf recht ausgefeilte Weise, die Cookies im Zaum zu halten: Der Internet Explorer erlaubt es, auf Server-Basis festzulegen, ob Cookies abgelegt werden dürfen, so daß Sie, wenn Sie wollen, DoubleClick.net und ValueClick.com ein für alle Mal den Zugang zu Ihrer Festplatte verwehren können. Mit Netscapes Navigator dagegen können Sie alle Cookies ablehnen, die von einem anderen Server stammen als die gerade besuchte Site, womit die Banner-Agenturen ebenfalls ausgeschlossen wären. iCab wiederum erlaubt beide Varianten und läßt Sie darüber hinaus gesetzte Cookies inspizieren und löschen. Sie können übrigens sicher sein, daß Sie nach einem Besuch unserer Website www.macmagazin.de keinen weiteren Cookie auf Ihrer Festplatte finden werden. Dies gilt auch für unser Schwestermagazin MACup (www.macup.de).



iCab bietet die ausgefeiltesten Optionen zur Filterung und Verwaltung von Cookies, die Sie auch einzeln inspizieren können.

Nicht ganz ohne. Sie könnten versucht sein, Cookies nun generell zurückzuweisen, aber damit würden Sie sich zusätzliche Probleme schaffen. Cookies sind, ihrem schlechten Ruf zum Trotz, durchaus nützlich: Wenn beispielsweise Ihr Browser während einer Online-Bestellung abstürzt, werden Sie nach einem Neustart des Programms die zuvor georderten Waren noch im virtuellen Einkaufswagen vorfinden, da Sie als Besucher der Website anhand des zuvor gesetzten Cookies wiedererkannt werden. Portal-Sites und andere Angebote im WWW, die Sie an Ihre Bedürfnisse anpassen können, speichern derartige Voreinstellungen gewöhnlich in Cookies und stellen daher ihre Zusammenarbeit ein, wenn Sie sie ausschalten. Selbst im ungünstigsten Fall können Cookies keinen Schaden anrichten. Aber passen Sie gut auf sie auf: Manche Cookies enthalten Zugangsdaten für personalisierte Websites, und wer diese klaut, könnte damit vielleicht Ihren Terminkalender auf einer Portal-Site einsehen.

Die potentielle Gefahr droht hierbei nicht aus dem Internet, sondern vielmehr von jedem, der Zugang zu Ihrem Rechner hat (siehe Folge 1, Mac MAGAZIN 10/99).

Übertragungssicherheit

Wenn wir auf einen Server im WWW zugreifen, mag es den Anschein haben, als kommunizierten wir über eine Punkt-zu-Punkt-Verbindung – vergleichbar etwa mit einer Telefonverbindung zwischen zwei Teilnehmern. Das Internet funktioniert allerdings nicht so, und der Austausch von Daten zwischen zwei Computern ist komplizierter. Unter dem Aspekt des Datenschutzes stellen sich drei Fragen:

- Können die zwischen Ihnen und einem Server ausgetauschten Daten von irgendwoher abgehört werden?
- Ist der Server wirklich der, für den Sie ihn halten?
- Kann jemand Ihre Identität im Internet annehmen und in Ihrem Namen und auf Ihre Kosten beispielsweise finanzielle Transaktionen tätigen?

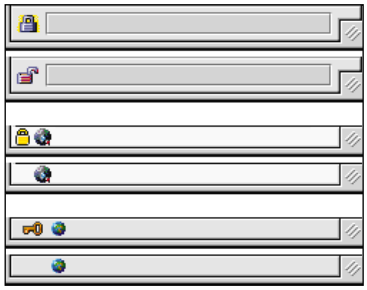
Entgegen der verbreiteten Vorstellung ist das Internet ein sichereres Medium als etwa Telefon- oder Faxverbindungen, die im Fall von Interkontinentalverbindungen routinemäßig von den Geheimdiensten abgehört werden. Die Datenübertragung im Internet erfolgt nicht als stetiger Daten- ➔

strom von Punkt zu Punkt, sondern in Form von kleinen Päckchen, die, jeweils mit den IP-Nummern von Absender und Empfänger gekennzeichnet, unabhängig voneinander auf die Reise durch das weltweite Datennetz geschickt werden. Welchen Weg ein Datenpaket zwischen Absender und Empfänger nimmt, ist kaum vorherzusagen und kann sich von Mal zu Mal ändern.

Verschlüsselung. Wer eine bestimmte Übertragung aufzeichnen möchte, müßte dazu alle zugehörigen Pakete auf ihren diversen Pfaden aufspüren und in der richtigen Reihenfolge zusammensetzen. Dies wäre aber selbst dann schwierig, wenn sich jemand Zugang zu einigen Knotenpunkten im Internet verschafft hätte. In ihrem lokalen Netzwerk und beim Provider werden die Datenpakete noch auf einem festen Pfad weitergeleitet und sind daher am gefährdetsten. Im Internet selbst hingegen sorgt dessen Übertragungsmodus für eine gewisse Sicherheit, die schon durch relativ einfache Verschlüsselungsverfahren auf ein für alle praktischen Belange ausreichendes Maß gebracht werden kann. Ein irgendwo eingeschleustes Programm könnte beispielsweise IP-Pakete nach Kreditkartennummern durchsuchen, die ja einem bestimmten Muster folgen. Falls diese jedoch verschlüsselt übertragen werden, etwa mit einer 40-Bit-Verschlüsselung nach dem Standard SSL (Secure Socket Layer, siehe unten), dann gibt es kein wiedererkennbares Muster mehr, und die Masse der Datenströme im Internet garantiert dafür, daß ein solcher Fischzug scheitern muß.

Finanzielle Transaktionen im Internet gelten vielfach als gefahrenträchtig, aber wer seine Online-Einkäufe mit der Kreditkarte bezahlt, ist keineswegs Freiwild für Hacker, die angeblich die Übertragung von Kreditkartendaten problemlos abhören und sie für eigene Einkäufe nutzen könnten. Immerhin genügt es ja tatsächlich meist, Vor- und Zuname, Kreditkartennummer und Ablaufdatum anzugeben; eine Unterschrift ist nicht erforderlich und könnte nicht überprüft werden. Wie aber die Erfahrung zeigt, wird die Unterschrift auch außerhalb des Cyberspace kaum je kontrolliert, und wer seine Karte einem Restaurantkellner anvertraut, stellt ihm damit mehr Informationen für einen Mißbrauch zur Verfügung, als es der Surfer im Internet könnte. Die Gefahr ist real, aber sie ist im Internet nicht größer als in der wirklichen Welt.

SSL und SET. Zur Minimierung der vorhandenen Gefahr sollten Sie darauf achten, daß die von Ihnen gewählten Online-Anbieter das SSL-Protokoll nutzen. Ob die aktuelle Webseite in diesem Sinne sicher ist, erkennen Sie am Schlüssel- oder Schloßsymbol in der linken unteren Ecke Ihres Browserfensters. Nur wenn der Schlüssel ganz respektive das Vorhängeschloß geschlossen ist, handelt es sich um eine sichere Seite. Das SSL-Protokoll kodiert die übertragenen Daten mit einem 40-Bit-Schlüssel, welcher die amerikanischen Exportrestriktionen gegen starke Verschlüsselungsprogramme respektiert. Da aber ein Hacker kaum, wie bereits gesagt, in der Lage wäre, gezielt an alle Datenpakete einer Übermittlung zu gelangen, um diese zu entschlüsseln, und es ihm zudem durch die Verschlüsselung verwehrt ist, in allen Paketen nach Mustern von zum Beispiel Kreditkartennummern zu suchen, kann das SSL-Protokoll durchaus als ausreichend sicher gelten. SSL sorgt somit zum einen für eine sichere Übertragung der Daten, garantiert zudem aber auch die Authentizität des Servers.



Browser unterscheiden unterschiedlich zwischen sicheren (SSL) und unsicheren Verbindungen (von oben: Navigator, Internet Explorer, iCab).

Einen noch höheren Sicherheitsstandard gewährleistet ein Verfahren namens SET („Secure Electronic Transaction“), das zur Zeit aber noch seltener als der SSL-Standard angewandt wird. Für Onlinebanking werden zudem vielfach – zusätzlich oder anstatt einer Verschlüsselung – einmalig verwendete Transaktionsnummern (TANs) eingesetzt (einen weiteren Artikel zu diesem Verfahren aus Mac MAGAZIN 8/99 finden Sie auf der Cover-CD vor).

Täuschungsversuche. Neben dem Abhören Ihrer Daten droht zumindest theoretisch eine weitere Gefahr: Der Server eines Angreifers könnte sich als ein anderer ausgeben und Sie damit veranlassen, sensitive Informationen preiszugeben. Beim sogenannten Man-in-the-middle-Angriff schaltet sich ein Computer in die Verbindung zwischen Ihnen und einem Server, beispielsweise dem Ihrer Bank ein. Der „Mann in der Mitte“ fängt nun Ihre Datenpakete ab und schickt sie in modifizierter Form an den eigentlich angesprochenen Server weiter. Zum Beispiel könnte jemand eine Überweisung, die Sie gerade veranlassen, auf sein eigenes Konto umleiten. Gegenüber dem Server gibt sich der Computer des Angreifers als Sie aus und leitet die entsprechenden Datenpakete, notfalls modifiziert, an Ihren Computer weiter. Tatsächlich scheint es aber noch keinen erfolgreichen Man-in-the-middle-Angriff gegeben zu haben, wofür vor allem die Netzwerkstruktur des Internets verantwortlich ist, die es so gut wie unmöglich macht, alle Datenpakete aufzufischen. Der Angreifer müßte schon beim Provider oder in Ihrem lokalen Netz sitzen, um eine echte Chance zu haben.

Dasselbe gilt für das „IP-Hijacking“ einer Verbindung, bei der ein Angreifer Ihre Verbindung zu beispielsweise Ihrer Bank übernimmt, nachdem Sie sich durch Übermittlung einer TAN autorisiert haben. Danach könnte er in Ihrem Namen beliebig schalten und walten. Allerdings müßte in diesem Fall ein solcher Verbindungsentführer schon ganz in ihrer Nähe sitzen, um diesen Trick erfolgreich anwenden zu können.

Etwas aussichtsreicher erscheint schon die Methode des DNS-Spoofing, welches auf dem Verfahren beruht, einen Servernamen wie www.macmagazin.de in eine IP-Nummer, also hier 195.222.199.9 zu übersetzen, wie es bei jedem Zugriff auf eine URL geschieht. Wenn der Domain Name Server (DNS) Ihres Providers den angefragten Servernamen nicht kennt, leitet er die Anfrage an einen anderen DNS weiter. Genau an dieser Stelle versucht ein Angreifer mit dem DNS-Spoofing anzusetzen. Hierzu richtet er zunächst einen Webserver ein, dessen Angebot dem eines anderen – sagen wir, www.apple.de – weitestgehend gleicht, nur daß beispielsweise einige Downloads trojanische Pferde sind. Der Angreifer schickt nun eine Anfrage nach der IP-Nummer von www.apple.de an den DNS Ihres Providers, der seinerseits (falls er die IP-Nummer nicht in seinem Cache verfügbar hat, denn nur in diesem Falle funktioniert dieser Trick) bei einem zweiten DNS anfragt. Der Angreifer schickt nun sofort ein Paket an Ihren DNS, das sich als Antwort des zweiten DNS ausgibt. Die

IP-Nummer des Angreifers wird dabei als diejenige von www.apple.de anzeigt. An der Antwort Ihres DNS erkennt der Angreifer nunmehr, ob sein Trick tatsächlich geglückt ist, denn in diesem Fall wird dies seine eigene IP-Nummer sein. Von diesem Moment an werden alle Zugriffe aus dem Netz Ihres Providers auf www.apple.de auf den Server des Angreifers umgeleitet – und dies geschieht so lange, bis die falsche Zuordnung aus dem Cache Ihres Domain Name Servers gelöscht wird.

DNS-Spoofing würde theoretisch funktionieren, allerdings setzt es ein präzises Timing voraus. Da der Angriff immer nur einem bestimmten Provider gilt und Sie in einem eng begrenzten Zeitfenster auf einen bestimmten Server zugreifen müssen, um dem Betrug zum Opfer zu fallen, ist die Gefahr letztlich gering. Wenn Sie ganz sichergehen wollen, dann sollten Sie in Ihren Bookmarks den symbolischen Namen sicherheitsrelevanter Server durch die IP-Nummer ersetzen, denn diese nicht weiter manipuliert werden.

E-Mail

Elektronische Post wird oft mit einer Postkarte verglichen, deren Inhalt jeder, zum Beispiel der Postbote, lesen könne. Tatsächlich gilt für E-Mail dasselbe wie für andere Formen des Datenaustauschs im Internet: E-Mails werden zwar im Klartext durch das Internet befördert, werden dabei allerdings in kleine Datenpakete zerlegt und auf nicht leicht nachvollziehbaren Wegen versandt. Ein Hacker, der nicht gerade in ihrem lokalen Netz sitzt oder Zugang zum Mailserver des Providers hat, wird schwerlich in Ihren Mails lesen können. Sie können die Sicherheit Ihrer Mails gegen unerwünschte Mitleser aber noch erhöhen, indem Sie Ihre Texte mit einer Software wie PGP oder SafeMail verschlüsseln (PGP als Freeware und SafeMail als Demoversion liegen auf der CD, ebenso wie eine Anleitung zur Verschlüsselung mit PGP aus Mac MAGAZIN 11/98).

Das größte Risiko für die Sicherheit Ihrer E-Mails sind allerdings Sie selbst: Wenn Sie etwa Ihr E-Mail-Programm das Paßwort für die Mailabfrage bei Ihrem POP3-Server speichern lassen – schließlich ist es so bequemer, und vielleicht haben Sie das Paßwort ohnehin längst vergessen – dann kann jeder, der Zugang zu Ihrem Computer hat, Ihre Mails abfragen oder in Ihrem Namen Mails verschicken. Es würde zudem sogar bereits genügen, die Voreinstellungen Ihres Mail-Clients zu kopieren, um künftig von einem jeden beliebigen Rechner aus auf Ihre E-Mail zugreifen zu können. Auch die bereits empfangene oder abgeschickte Mail liegt meist unverschlüsselt und ungesichert auf Ihrer Festplatte. Wie Sie die vor unbefugtem Zugriff schützen können, haben wir im vorangegangenen Heft erklärt. *MJH*

Mit der Kreditkarte im Internet

Welches Risiko gehen Sie bei Kreditkartentransaktionen im Internet ein? Wir befragten dazu Etta Schulze und Margit Schneider von der Firma EURO Kartensysteme (EuroCard, Eurocheque).

Mac MAGAZIN: *Welche Empfehlung geben Sie Kreditkarteninhabern, die im Internet mit ihrer Karte bezahlen wollen?*
EURO Kartensysteme: Wir empfehlen für Zahlungen im Internet den Einsatz der Kreditkarte bei Anbietern, die den Sicherheitsstandard SET anwenden. Man erkennt das an dem SET-Zeichen auf der Homepage des Händlers oder des Dienstleisters. Wenn SET noch nicht eingesetzt wird, dann empfehlen wir, die Kreditkartendaten mit SSL-Verschlüsselung zu versenden.

MM: *Welche Empfehlungen geben Sie den Online-Anbietern, die die EuroCard akzeptieren?*
EK: Händlern und Dienstleistern, die im Internet anbieten, empfehlen wir ebenfalls, den SET-Standard zu nutzen. Beim Aufbau der Website sollte der Internethändler darauf achten, daß er neben den Kartendaten auch die Anschrift des Karteninhabers und die Lieferanschrift aufnehmen kann, falls diese voneinander abweichen. Beim Angebot immaterieller Güter sollte die E-Mail-Adresse des Bestellers abgefragt werden, so daß eine Rückverfolgung möglich ist.

MM: *Welche Regeln sollte ein Kreditkartenzahler einhalten, um sich nicht Fahrlässigkeit bei Onlinegeschäften vorwerfen lassen zu müssen?*
EK: Alle Karteninhaber sind verpflichtet, ihrer Sorgfaltspflicht nachzukommen. Sollte ein Mißbrauch darauf beruhen, daß beispielsweise die Kreditkarte an Dritte weitergegeben oder im Handschuhfach eines Autos deponiert und dann gestohlen wurde, dann handelte der Karteninhaber fahrlässig und haftet für den daraus entstandenen Schaden. Darüber hinaus sollten Kreditkarteninhaber einige weitere Tips beachten:

- Gehen Sie sorgfältig mit Ihren Kartendaten um. Das Internet ist ein offenes Netz, und Kreditkartennummern können einmal in falsche Hände gelangen. Achten Sie auf die Verschlüsselung der Kartendaten (SET oder SSL). Geben Sie nicht voreilig die Kartennummer ein, bevor Sie die Bedingungen gelesen haben. (Gehen Sie ein Abonnement ein oder treten Sie einem Club bei? Wie sehen die Abrechnungsmodalitäten und Kündigungsfristen aus?)
- Drucken Sie sich die Allgemeinen Geschäftsbedingungen, Kunden- und Vertragsbedingungen aus, ebenso die Bestellung selbst als Erinnerungsstütze, was Sie wo bestellt haben.
- Vergleichen Sie die Umsätze auf der Kreditkartenabrechnung mit dem Bestellformular. Zahlreiche Anbieter rechnen über spezielle Abrechnungszentren ab, das heißt, die Namen auf der Kreditkartenabrechnung stimmen nicht mit denen auf der Bestellung überein; seriöse Internetanbieter nennen diese Zentren in der Regel in ihren Allgemeinen Geschäftsbedingungen oder auf dem Bestellformular.

Margit Schneider, Manager Security & Risk bei EURO Kartensysteme

MM: *Welche Maßnahmen kann ein Karteninhaber veranlassen, um eine nicht von ihm autorisierte Transaktion zu reklamieren? Wie hoch ist das finanzielle Risiko, das jemand eingeht, der online mit der Kreditkarte bezahlt?*
EK: Der Karteninhaber wendet sich in einem solchen Fall an das die Karte ausgebende Institut. Der Kundenberater füllt mit ihm ein Reklamationsformular aus; darin wird unter anderem nach dem reklamierten Umsatz und dem Reklamationsgrund gefragt. Letzterer sollte möglichst detailliert und ausführlich dargestellt werden. Dem Reklamationsschreiben müssen sämtliche wichtigen Unterlagen wie Kopien von Belegen beigefügt werden. Das Institut wird den Kontakt zum Händler oder Dienstleister aufnehmen, um den Sachverhalt zu klären.

Grundsätzlich gilt: Der Kreditkarteninhaber haftet ausschließlich für diejenigen Transaktionen, die er auch tatsächlich getätigt hat. Der Herausgeber einer Kreditkarte ist gegenüber dem Inhaber der Karte beweispflichtig, daß bestimmte Umsätze getätigt worden sind. ■