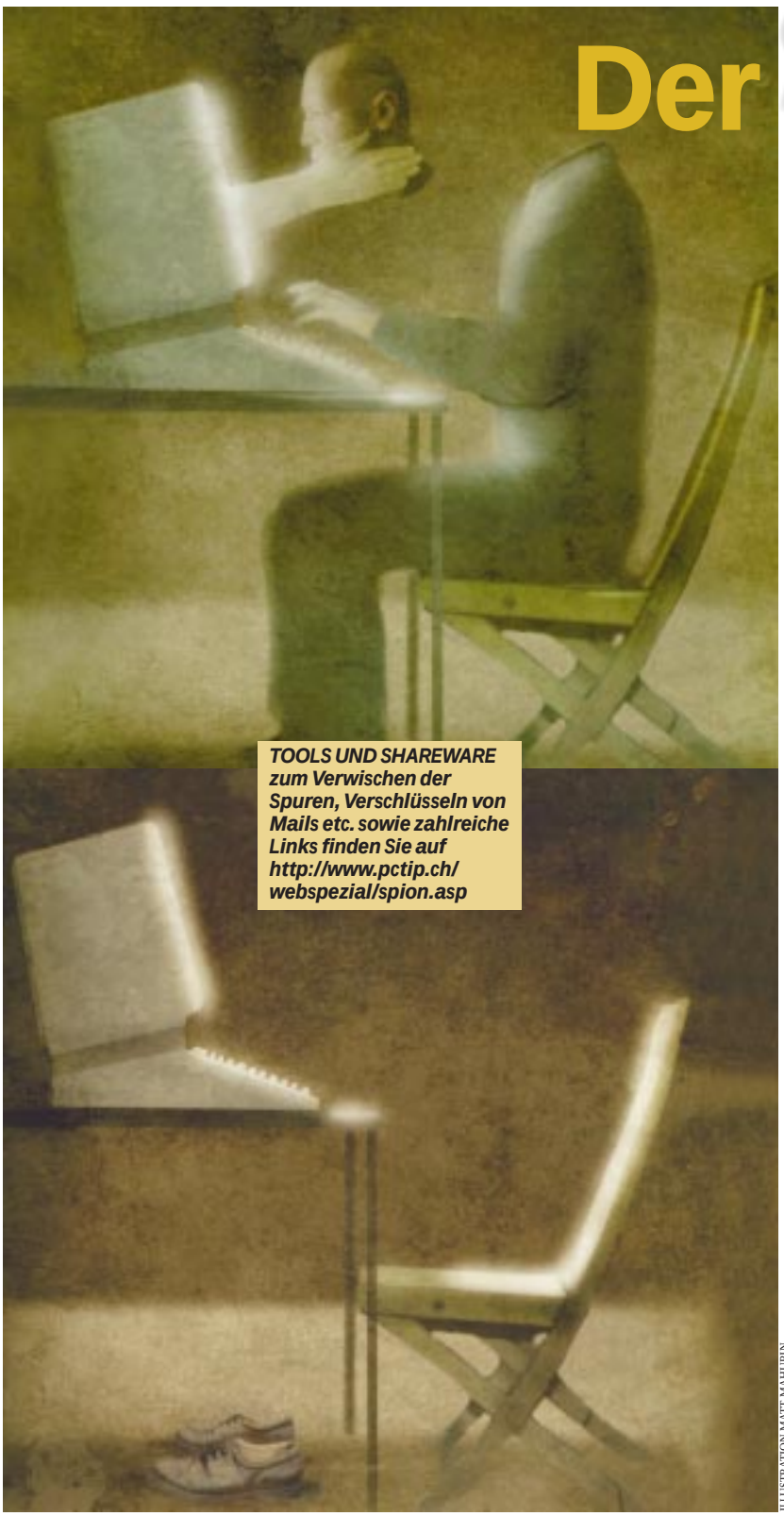

Der Spion s

Wenig Internet-Know-how ist nötig, um wildfremde Menschen auszuspionieren. Das grösste Sicherheitsrisiko im Cyberspace sind dessen Bewohner selbst.

von Bruno Habegger

Zukünftig muss man sich selbst vor dem Seifenspender über dem Waschbecken in der Toilette in acht nehmen, um sich Peinlichkeiten zu ersparen. Eine US-Firma hat vor kurzem einen Seifenspender in die Testphase geschickt, der mittels Sensoren feststellt, ob man Gebrauch von ihm machte und die Toilette mit sauberen Händen verlässt. Nur noch eine Frage der Zeit, bis der Lokus ans Internet angeschlossen wird und den Chef per E-Mail auf die Missetat aufmerksam macht. Die dazu nötige Technologie hat Sun vorgestellt: Sie heisst Jini, regelt den Datenaustausch verschiedenartigster Geräte in einem Netzwerk und basiert auf Java.

Ruedi Meister*, ich mag ihn nicht. Keine Ahnung, weshalb. Vielleicht, weil er in der Newsgroup ch.general immer eine grosse Klappe führt. Mal sehen, der kann was erleben! Leider weiss ich nicht, wo er wohnt. Macht nichts. Die Meta-Suchmaschine der Uni Hannover Mesa kennt ihn sicherlich: http://mesa.rrzn.uni-hannover.de/ benötigt nur Vor- und Nachname, durchforstet danach – wenn es sein muss minutenlang – mehrere E-Mail-Verzeichnisse. Bingo! Schon nach kurzer Zeit spuckt die Suchmaschine seine E-Mail-Adresse aus. Ich habe noch mehr Glück: Mesa kennt sogar seine Adresse. Mein Mann wohnt in der Nähe von Bern in einem kleinen Dorf. Twix-Tel verrät seine Telefonnummer. Ruedi ist unvorsichtig: Sogar seine Natel-Nummer lagert auf der CD-ROM.
*** Name geändert**

Big boss is washing you in der schönen, neuen Welt. Immer weiter wuchern die Daten-Netzwerke, immer mehr Anwendungen laufen

***TOOLS UND SHAREWARE** zum Verwischen der Spuren, Verschlüsseln von Mails etc. sowie zahlreiche Links finden Sie auf http://www.pctip.ch/webspezial/spion.asp*

ILLUSTRATION MATT MAHURIN

1 surft gleich nebenan

über Netzwerke, immer mehr Firmen schliessen ihre Computer gegen innen zusammen und koppeln ihr Netzwerk gegen aussen ans weltweite Internet. Auch die Zahl der ans Internet angeschlossenen Haushalte wächst. Bis zum Jahr 2003 sollen laut Datamonitor ein Drittel aller Haushalte in Europa am Netz hängen. Die Technologie geht mit Siebenmeilenstiefeln voran – die Anwender benehmen sich allerdings immer noch, als würde es genügen, die wichtigen Dokumente im Schreibtisch einzuschliessen und den Schlüssel auf sich zu tragen. Doch heutzutage benötigen Einbrecher statt Dietrich und Taschenlampe nur einen PC und ein Modem.

Er hat Glück, eigentlich bin ich ein netter Kerl. Und kriminell auch nicht. Aber ich könnte ihm schon jetzt übel mitspielen, beispielsweise bei verschiedenen Shopping-Sites in seinem Namen Waren bestellen – gewissermassen eine Shop-Bomb basteln. Die meisten Versandhäuser handeln nachlässig, lassen sich die Bestellung nicht rückbestätigen. Nicht besonders schlimm für Ruedi: Er kann die unbekannte Post refüsieren. Weit unangenehmere Folgen könnte es für ihn haben, wenn er das Passwort für seine Combox-Nummer nicht geändert hat. Meist sinds die letzten vier Ziffern der Natel-Nummer, oft aber auch einprägsame Folgen wie 0000 oder 1234. Ich könnte protokollieren, wer ihn anruft. Einfach so. Ich bin schliesslich ein Voyeur. Vielleicht ist er verheiratet und hat daneben eine Freundin? Ich könnte sein Liebesleben ruinieren. Ärger bringt auch die kurzzeitige Umleitung seiner Post. Vielleicht ist, bis er sein Unglück bemerkt, die Abrechnung seiner Kreditkartenfirma darunter? Ein Anruf bei der Post und eine geschickte Ausrede, warum man jetzt gerade kein Umleitungsformular ausfüllen und unterschreiben kann, genügt.

Um das Sicherheitsbewusstsein von Anwendern und Verantwortlichen für die Netzwerke steht es nicht besonders gut. In den vernetzten USA sorgen sich die Firmen laut einer Umfrage des International Network Service INS um die Sicherheit, doch haben nur 36 Prozent der befragten Unternehmer Tools im Einsatz, die Eindringlinge aufspüren und dingfest machen. Die deutsche Orbit, spezialisiert auf Netzwerke, hat in einer Umfrage unter 100 mittleren und grossen Unternehmen in Deutschland, ermittelt, dass 80 Prozent davon nur schlecht auf die Gefahren aus dem Internet vorbereitet sind. «Noch nie waren in den Firmennetzen so viele und so wertvolle Informationen gespeichert wie heute. Und noch nie war es für Aussenstehende und Unbefugte so leicht, an diese Informationen zu gelangen», so Orbit-Geschäftsführer Toni Schnürer. Und mehr als die Hälfte der befragten Unternehmen verschlüsselt ihre Daten nicht, hält gar eine Authentifizierung der Anwender für überflüssig.

Jetzt bin ich neugierig geworden. Was treibt R. M. so im Internet? Ich weiss schon, er bewegt sich im Usenet. Deshalb checke ich bei http://www.dejanews.com/, welche Spuren er hinterlassen hat. Schock! Der Mann nimmt Drogen! Wie ich das in Erfahrung gebracht habe? Ganz einfach: Ich gebe seine E-Mail-Adresse in Power Search ein und erhalte seine Postings in allen Newsgruppen. Ich rufe eine Message auf und klicke auf Author Profile und erhalte eine saubere Aufstellung der Newsgruppen, für die er sich jemals interessiert hat. Und voilà: In einer Newsgroup über Drogen schlägt er seine Erfahrungen breit. Ich könnte nun herausfinden, wo er arbeitet. Vielleicht verrät die Homepage seiner Firma mehr Details über ihn? Oder das Internet nach Stelleninseraten abgrasen, in denen er sich anpreist und seinen Chef per E-Mail informieren? Mit seiner Kreditkarten-Nummer könnte ich die zahlungspflichtigen Datenbanken abfragen, die Nummer seines Autos abchecken oder nachklicken, ob Betreibungen gegen ihn laufen.

Wenn schon die Firmen nachlässig sind, wie sollten sich da die privaten Anwender an die einfachsten Sicherheitsregeln halten? Sie wähnen sich im Schutz der Masse – was sollte ein Hacker bei ihnen schon zu suchen haben? Die meisten von ihnen gehen deshalb sozusagen mit «ungewaschenen» Händen ins Netz. Sie speichern ihre Passwörter auf der Festplatte ab – bequemlichkeitshalber – oder ändern fahrlässig die Standard-Vorgaben der Internet-Provider für den Zugang nicht. Kennt man die E-Mail-Adresse eines Surfers und weiss um die Gepflogenheiten des Providers, lässt sich auf das Kennwort schliessen – die halbe Miete für das Surfen auf fremde Kosten. Bei vielen Internet-Providern ist der vordere Teil der E-Mail-Adresse gleichzeitig auch das Kennwort. Und das Passwort herauszufinden ist mit frei erhältlicher Software, die automatisch eine Wortliste abarbeitet, nicht weiter schwierig. Viele Anwender vergeben nämlich leicht zu erratende Passwörter, Wörter wie Traktor, Gott oder Sex. Technisch anspruchsvollere Programme spionieren bei stehender Internet-Verbindung die Daten auf der Festplatte aus – unbemerkt vom fröhlichen Surfer. Mit den gefundenen Passwörtern lässt sich noch viel mehr anstellen, beispielsweise die private E-Mail-Post lesen. ▶

Personenschutz I

Diskrete Surferinnen und Surfer bewahren ihre Privatsphäre, denn sie...

tippen Adresse und Telefonnummer so wenig wie möglich ein. Und wenn, nur auf Homepages bekannter Firmen.

checken als erstes auf der Homepage ab, wie die Firma mit ihren Daten umgeht («Privacy Policy»). Es sollte explizit erklärt werden, dass die Daten des Surfers nicht weiter verkauft werden.

bewegen sich nicht in schmuddeligen, unbekannten Ecken des Internet. Das tun sie ja auch in der Realität nicht.

stellen die Sicherheitseinstellungen im Browser auf hoch (im Internet Explorer 4 unter Systemsteuerung/Internet/Sicherheit), deaktivieren Active-X und Javascript, schalten beides nur selektiv (beim Internet Explorer möglich) auf vertrauenswürdigen Sites ein und lassen vor Cookies warnen (unter Erweitert/ Sicherheit).

verraten im Usenet keine privaten Dinge, geben keine Anhaltspunkte über Wohnort und mehr.

verhindern die Archivierung ihrer Newsgruppen-Artikel mit «x-no-archive: yes» als erste Zeile im Text.

verzichten auf relativ unsichere Chat-Tools wie ICQ.

sind sich auch in Chat-Rooms bewusst, dass mindestens dessen technischer Betreuer ihre Identität ermitteln kann.

Fortsetzung Seite 23

Sicherheit im Internet

▶ Die Adresse des Mailservers ist bekannt – und oft sind Pass- und Kennwort identisch mit jenen für den Internet-Zugang.

Eine ganze Menge könnte ich jetzt über den Menschen Ruedi Meister erfahren. Vielleicht ist ja so dumm und postet auch in zwielichtigen Newsgroups mit sexuellen Inhalten? Sein ganzes Leben könnte ich in den Griff kriegen, seine E-Mails lesen, ihn terrorisieren, seinen Rechner während der Internet-Verbindung blockieren oder zum Abstürzen bringen – auch dafür sind zahlreiche mehr oder weniger leicht bedienbare Tools im Internet erhältlich.

So gibt der unbedachte Surfer sein Privatleben im Netz preis. Und er gibt dem noch weiter Vorschub: In Newsgruppen und Chatrooms verrät er seine sexuellen Vorlieben, seine Hobbys, seine Pläne und ahnt nicht, dass jedes Wort archiviert wird und jederzeit einsehbar ist. Er tippt seine Adresse und Telefonnummer in Formulare, einfach so, aus Neugierde, um eine bestimmte Datei, Freeware oder ein unzüchtiges Bild herunterzuladen. Noch schlimmer: Er gibt seine Kreditkarten-Nummer auf ungesicherten Homepages preis – oder überlässt sie Betreibern zwielichtiger Websites in den USA oder in Asien, Typen, denen er in der Realität nicht mal die Hand schütteln würde.

Aber ich bin ja wie schon gesagt ein netter Mensch. Und Ruedi Meister ist mir im Grunde genommen eigentlich egal. Jeder kann tun und lassen, was er oder sie will – das habe ich im Cyberspace gelernt. Und ich möchte Ruedi nicht unterschätzen. Schliesslich hinterlasse auch ich meine Spuren im Cyberspace, die er zurückverfolgen könnte. Dann müsste ich mich vor dem Richter für mein schändliches Treiben verantworten und Busse tun.

Die Einsamkeit vor dem Computermonitor, die räumliche und körperliche Distanz zu den anderen Surfern verführt zum Irrglauben, man sei anonym im Netz. Zwar sind einzelne, private Surfer wohl kaum ein lohnendes Ziel für Hacker und Cracker. Aber: Sobald mehrere Computer miteinander verbunden werden, an denen Menschen arbeiten, löst sich technisch gesehen die Privatsphäre auf. Jeder Rechner erhält während einer Internet-Sitzung eine bestimmte IP-Nummer, die, einmal bekannt, Böswilligen gezielte Attacken und Abfragen erlaubt. (Hinweis: Die IP-Nummer eines Web-Servers www.name.ch erhalten Sie ganz einfach: Öffnen Sie ein DOS-Fenster und geben Sie «ping www.name.ch» ein. Gutartige Mitmenschen nutzen diese Funktion nur, um eine fehlerhafte Internet-Verbindung zu überprüfen. Dasselbe gilt für den Befehl «tracert www.name.ch», der den Weg durch den Internet-Dschungel bis zum Zielrechner verfolgt.)

Die Festplatte verrät ihren «Beschreiber», genau wie der Seifenspender Waschfaule an den Pranger stellt. Anwender müssen deshalb lernen, sich im Netz diskret zu bewegen, vorsichtiger als in der Realität, in der die Menschen immer offenbarungswütiger werden. Vielleicht unter anderem auch deshalb, weil der Auftritt in einer Talkshow immer noch anonymer als das Surfen im Internet ist.

Personenschutz II

Diskrete Surferinnen und Surfer bewahren ihre Privatsphäre, denn sie...

installieren immer die neusten Sicherheits-Updates für ihren Browser.

öffnen keine E-Mail-Anhänge unbekannter Herkunft.

tippen die Nummer ihrer Kreditkarte nur auf gesicherten Sites vertrauenswürdiger Händler ein. Auf das kleine Symbol des Schlüssels oder des geschlossenen Vorhängeschloss im Browser achten!

denken daran, dass E-Mails wie Postkarten sind – jeder kann sie lesen. Wichtige und private Informationen verschlüsseln sie deshalb mit Software wie Pretty Good Privacy.

wickeln ihren E-Mail-Verkehr über anonyme Remailer wie Hotmail oder GMX ab.

installieren im Büro kein Modem ohne Bewilligung. Über solche Modems kann ins Netzwerk eingebrochen werden.

belassen wichtige Dokumente (Geschäftsberichte etc.) nicht auf ihrer lokalen Festplatte, sondern auf einem gesicherten Server.

speichern nie Passwörter ab und ändern sie regelmässig. Passwörter müssen kompliziert aufgebaut sein, am besten mit Zahlen und Buchstaben.

löschen regelmässig den lokalen Cache-Speicher (die temporären Dateien im Internet Explorer).

Wahre Geschichten von falschen Surffreunden

Hacker dringen auf Websites und knacken Netze

Immer wieder werden Homepages gehackt – die Eindringlinge ersetzen Bilder und hinterlassen Parolen. Eine Sammlung findet sich auf http://www.2600.com/.

FOTOILLUSTRATION WILLIAM DUKE

Spektakulärste Aktion in der Schweiz war der Angriff auf einen Aargauer Internet-Provider. Ein serbischer Hacker verunstaltete die beim Provider lagernde Homepage einer Kosovo-Zeitschrift. Danach verlangte er beim Provider die Löschung der Site und drohte mit der Zerstörung des Computers des Providers. Um der Drohung Nachdruck zu verschaffen, löste er bei einem PC des Providers einen Festplatten-Crash aus.

«Alle, die am Internet hängen, also auch Provider, benötigen ein umfassendes Sicherheitskonzept, das regelmässig überprüft werden muss.», sagt Martin Gafner von der auf Sicherheit spezialisierten Zbinden Infosec AG aus Bern (http://www.infosec.ch/). In der Regel werden Hacks verschwiegen – aus Angst vor einem Imageverlust und Nachahmungstätern. «Einmal bekannt geworden, zieht ein Hack weitere Angriffe nach sich», so Gafner. Angriffe auf Privatpersonen sind ihm nicht bekannt. Meistens würden solche Vorfälle als Programmfehler oder Virus abgetan.

Für Kopfschmerzen hatte im letzten Jahr ein Bericht des Datenschutzbeauftragten der Zürcher Regierung gesorgt. Simulierte Angriffe auf das Netzwerk der Kantonalen Verwaltung hatten ergeben, dass zwar die Firewalls – die elektronischen Sicherheitsbarrieren zwischen Internet und Netzwerk – standhielten, das Suchprogramm aber anstandslos Kennwörter für ein Login fand. Zudem waren die Hacker auf Modems gestossen, die in keinem Inventar der Verwaltung aufgeführt waren, aber Login-Möglichkeiten geboten hätten. In einem zweiten Versuch wurde noch die netzinterne Sicherheit geprüft. Mit einem Laptop, der ans Netz der Kantonalen Verwaltung angeschlossen wurde, konnten die Hacker in Kürze sämtliche Bewegungen sichtbar machen, E-Mails lesen und beliebig Daten abrufen.