Presseschau zum Thema Internet Pishing und rechtloser Bereich

„Wer überwacht die Wächter“ fragte sich schon Juvenal im alten Rom und „Pekunia non olet“, Geld stinkt nicht sagen sich wohl alle, die mit viel Zeitaufwand und hoffentlich blanken Nerven Konten plündern und Daten manipulieren. In der gleichen Zeit eine saubere und sinnvolle Arbeit geleistet und allen ginge es etwas besser. Dass die Datenmanipulation aber immer wieder gelingt, zeigen die beiden Artikel in der Zeitschrift Chip 05 / 2010.

Ein Hohn für alle die mit harter und ehrlicher und ehrenhafter und respektierlicher und redlicher Arbeit Ihr Geld verdienen.

Ich habe selbst habe schon erlebt wie bei einem IT-Unternehmen Kreditkartendaten eines Shopkunden wieder aus dem virtuellen Mülleimer geholt wurden und habe schon mit „Drauflosprogrammieren“ über Datenschutz, Philosophie und andere unbekannte Größen und Anforderungen in der Welt des Drauflosprogrammierens gesprochen.

Wohl kaum einer erinnert sich noch an die alte Hackerethik, in der Schwachstellen aufgezeigt wurden, aber nicht der Manipulation dienten.

Es kann nicht sein, dass die Daten sozialer Netzwerke ausgebeutet und missbraucht werden, Daten illegal erhoben werden und wenn das Ganze auffällt, wird alles schnell gelöscht, so dass niemand nachvollziehen kann wer wann wo manipuliert hat.
Die eine ungesetzlich Handlung wird schnell beseitigt (aufgrund eines Bundesverfassungsurteils dass im Grundsatz richtig ist, für die bemängelten Rechtversöße aber zu spät kommt) und damit wird der nächste rechtsfreie Raum geschaffen, siehe Chip Artikel und dass ganze Spielchen beginnt von vorne. Spielen sich hier Politik und Ermittlungsbehörden und unseriöse Datenmanipulatoren gegenseitig in die Hände ? Qui Bono, wem nutzt es (?), zur Zeit doch wohl nur denen die unbemerkt davon kommen.

Dass ein Großteil des Geldbestandes virtuell ist, ist bekannt, dass er derartig schlecht geschützt und verwaltet wird, eine Schande. Wer nur unter Mühen sein Geld zurück bekommt, ist erschüttert wenn er an die in den Sand gesetzten Millionen des Bauunternehmers Schreiner erinnert wird, die ja nur Peanuts waren. Der Verdacht liegt nahe, dass hier und da ein paar Milliönchen mal schnell virtuell auftauchen, gebucht werden und wieder verschwinden, natürlich auf irgend einem Konto und einem nicht nachzuweisenden Buchungsweg.

Wenn sie die Summe der beantragten Telefonüberwachungen nehmen, erscheint diese zunächst nicht sehr hoch, Tatsache ist, ein Krimineller der mehrere Mobiltelefone benutzt, telefoniert unter Umständen mit hunderten Personen, bei einem großen Teil werden Fahnder annehmen, dass diese angerufenen Personen ebenfalls kriminell sind.

Im Klartext bedeutet dies dass unter Umständen hinter einer beantragten Abhöraktion, tausende abgehörte Anschlüsse verborgen sein können.

Darüber hinaus zeigen Artikel in seriösen Wochenzeitschriften wie Spiegel und Stern immer wieder, dass Geheimdienste und Netze wie Echelon fast alle Gespräche und Daten auswerten.

Gefiltert wird mit sogenannten Hit-Wörtern, aber sicherlich auch schon nach Tarn – Synonymen.

Nur, wer Überwacht die Wächter (?), wenn der Kumpel eines Geheimdienstlers oder Ermittlers eine Firma hat, wird er der Versuchung widerstehen können, dem von der neusten Erfindung in einer abgehörten Firma zu erzählen ? Wenn eine Regierung festgelegt hat, dass es wichtig für die eigene Industrie ist wenn solche Erkenntnisse an bestimmte, den Regierungen nahe stehende Unternehmen weitergegeben werden müssen, ist dass dann legal, weil der Zweck angeblich die Mittel heiligt und die Arbeitsplätze im eigenen Land nun mal wichtiger für die nächste Wahl sind, wie eine Pleiteunternehmen im Nachbarland ?
Wenn der Preis für ein Produkt oder eine Aktie steigt, wer widersteht sich selber über Strohmänner oder Freunde einzudecken, wenn er früh genug durch illegale Machenschaften davon erfährt ?

Jemand der so a*Gier*t, wird immer versuchen sich selber die Möglichkeiten zu erhalten die notwendig sind, um andere Konkurrenten so weit auf Abstand zu halten, dass sie ihn möglichst nicht einholen können, nur er lebt auch immer auf Kosten seiner Konkurrenten, Mitarbeiter und anderen.

Ist das fairer Wettbewerb (?), internationaler Sportsgeist (?), Fairness ?

So wird Ihr KONTO leergefischt

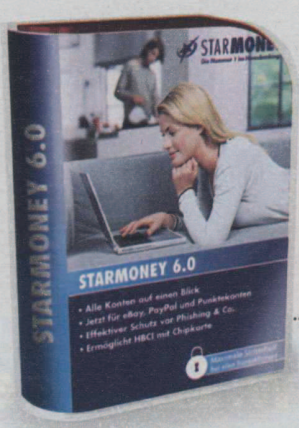
Ihr PC ist virenfrei? Sie fallen nicht auf Phishing rein? Von wegen! Längst nutzen die Hacker neue Methoden. CHIP zeigt, wie Sie sich beim Online-Banking schützen

VON DOMINIK HOFERER

Jahrelang Geld auf die hohe Kante zu legen, bringt nur dann etwas, wenn niemand Ihr Erspartes ergaunert. CHIP zeigt anhand aktueller Vorfälle, dass Sie weder Ihrer Bank, noch Ihren Freunden und schon gar nicht Ihrem Computer vertrauen dürfen, wenn es ums Geld geht. Doch Sie müssen nicht gleich zurück in die technologische Steinzeit und auf den PC verzichten: Wir liefern Ihnen auf Heft-DVD die Software, mit der Sie weiterhin Ihre Bankgeschäfte online erledigen können – und noch viel mehr. Die Vollversion der Banking-Software StarMoney schützt Sie und ermöglicht einen komfortablen Überblick über Ihre Geldgeschäfte.

Phishing im sozialen Netz

Wie wichtig eine sichere Banking-Software ist, zeigen aktuelle Beispiele drastisch: Denn angesichts immer besser informierter User greifen die Hacker zu neuen Methoden. Und die führen selbst erfahrene Nutzer hinters Licht. Etwa mit einem neuen Facebook-Trick: Wie Felix Leder, Sicherheitsfachmann und Doktorand an der Universität Bonn berichtet, tracken moderne Trojaner nicht nur Banking-Log-ins, PINs und TANs, sondern auch die Zugangsdaten von Facebook. Diese sind meist weitaus weniger gut geschützt als Bankdaten und ermöglichen den Betrügern viel mehr als nur Einsicht in private Daten des Users. Sie können die Freunde des von ihnen gekaperten Useraccounts direkt ansprechen – und senden Links zu gefälschten oder infizierten Seiten. Die meisten Empfänger würden niemals auf Phishing-Links in Spammails klicken, aber auf Links ihrer Freunde immer.



AUF DVD

Die Vollversion der Banking-Software StarMoney schützt vor Phishing und verwaltet komfortabel, sicher und übersichtlich Ihre Finanzgeschäfte

Verschafft sich ein Krimineller Zugriff zum Facebook-Account, kann er etwa gefälschte eBay-Seiten veröffentlichen und trojanerinfizierte Software-Downloads oder verseuchte YouTube-Videos empfehlen. Durch Kurz-URL-Dienste wie TinyURL, die bei Twitter und Facebook üblich sind, verschleiert der Gauner die gefälschte Domain.

Auch Tricks, die per Mail nicht mehr ziehen, versprechen bei sozialen Netzwerken mehr Erfolg. So häufen sich Vorfälle, in denen Gauner Accounts gehackt und Freunde des Opfers direkt mit der Bitte um Hilfe angeschrieben haben. Sie gaukelten den Bekannten vor, dass sich der Freund im Urlaub in Not befinde und schleunigst Geld benötige. Die Überweisung soll dann binnen Minuten per Geldtransferanbietern wie etwa Western Union durchgeführt werden. Die Folge: Das Geld ist weg. Sollte Ihnen Ähnliches passiert sein, berichten Sie uns davon, senden Sie eine Mail an **bankingpanne@chip.de**.

Überlistet beim Online-Banking

Dass Banken bei Schäden durch Online-Betrug nicht immer zahlungswillig sind, zeigt der Fall des CHIP-Lesers Tom Reibel (Name

von der Redaktion geändert). Der Kunde einer Genossenschaftsbank nutzt das eTAN-Verfahren. Hierfür benötigt man eine Hardware, die per Knopfdruck eine TAN-Nummer generiert. Dieses Verfahren galt lange als sicher, da die TAN fest an die Empfängerdaten geknüpft ist. Will ein Betrüger die Überweisung umleiten, ist die TAN nicht gültig. Dass dieser Schutz Lücken hat, bewies die Sicherheitsfirma RedTeam Pentesting. Mit einem Trojaner hebelten sie im November 2009 den Mechanismus aus. Bereits zwei Monate zuvor spürte Reibel am eigenen Leib, dass dieses eTAN-Verfahren angreifbar ist.

Er tätigte zwei Überweisungen, die beide korrekt angezeigt wurden. Reibel ist seit 20 Jahren in der Computerbranche unter anderem als Netzwerkadministrator tätig. Er ist also kein Anfänger. Er fällt weder auf Phishing rein, noch hat er seinen PC ungenügend abgesichert. Beim erneuten Einloggen ein paar Tage später bemerkte er, dass die zweite Transaktion nicht am richtigen Ziel angekommen war. Der Empfänger war stattdessen ein Computerhändler, von dem Reibel noch nie gehört hatte. Dieser hatte zuvor eine übliche Bestellung des vermeintlichen Betrügers erhalten und nach Zahlungseingang die Ware im Wert von über 1.000 Euro ausgeliefert. Angaben über den illegal handelnden Kunden wollte das Unternehmen aus Datenschutzgründen nicht machen. Reibel wandte sich an die Service-Hotline der Bank, die ihm unterstellte, fahrlässig mit der TAN-Nummer umgegangen zu sein. Das Geld zurückzuholen sei nicht mehr möglich, da der Vorfall zu lange her sei, eine Nachforschung koste 16 Euro. Die Bank verwies Reibel an die Polizei.

Dort stellte er eine Strafanzeige. Von seinem Geldinstitut hörte er nichts mehr – bis er an den Vorstand schrieb. Daraufhin erhielt er eine Antwort des Unternehmensservice. Der Inhalt: Das eTAN-Verfahren sei sicher, der Fehler läge bei ihm. Doch aufgrund der guten Geschäftsbeziehungen erstattete die Bank die Summe. Durch seine Hartnäckigkeit gelangte Reibel an sein Geld – und zeigt damit, dass man sich bei einem Schadensfall nicht einfach abwimmeln lassen sollte. Die Bank gestand mit ihrer Vorgehensweise das Sicherheitsproblem nur halb ein. Mit gutem Grund. Ein Präzedenzfall könnte sehr teuer werden.

Wie die Gauner letztlich ihr Opfer ausrauben konnten, ist nicht mehr nachvollziehbar. Denn trotz intensiver Spurensuche auf seinem PC fand Reibel keine Malware. Daher muss man von einem Trojaner ausgehen, der sich per Rootkit-Funktion und DLL-Hijacking unauffindbar im System versteckt hat. Surft das Opfer mit dem kompromittierten PC auf die Bankwebsite, tauscht der Trojaner die komplette Seite durch eine gefälschte Kopie des Bankportals aus. Weder optisch noch anhand des Sicherheitszertifikats bemerkt der ahnungslose Nutzer, dass er in eine Falle tritt. Sämtlicher Datenverkehr läuft von nun an über den Gauner, der die Überweisung unbemerkt noch im Browser zu seinen Gunsten ändert.

Generiert das Opfer eine eTAN und gibt sie ein, sendet der Kriminelle die Überweisung an sein selbst definiertes Ziel – in unserem Fall die Computerfirma. Das Opfer ist machtlos und kann nur vorbeugend Betriebssystem, Virenschutz, Browser sowie alle darin enthaltenen Multimedia-Plug-ins auf dem Laufenden halten. Zusätzlicher Schutz: Eine extra Banking-Software wie zum Beispiel StarMoney, über die Sie Ihre →

Angesteckt! Ihre Facebook-Kontakte verbreiten Malware!

Getäuscht! Trojaner schleusen Sie auf falsche Seiten

Geldgeschäfte mit dem felsenfest sicheren HBCI erledigen. Dazu benötigen Sie die Anleitung im Kasten auf ►S. 54 und idealerweise noch ein Kartenlesegerät der Klasse 3 – es geht aber auch ohne Hardware.

Abgezockt am Automaten

Doch nicht nur online lauern Gefahren, Geld zu verlieren. Selbst das Abheben am Geldautomaten scheint unsicher zu werden. Die Liste der Vorfälle in der letzten Zeit: Manipulierte Automaten, die Karten auslesen oder gar mit einem Trojaner verseucht sind. Fehlerhaft programmierte Chipsätze, durch die ab dem 1. Januar 2010 über 30 Millionen Giro- und Kreditkarten nicht mehr richtig funktionierten. Anders als weitläufig dargestellt, handelte es sich hier nicht um ein verschobenes Millenium-Problem, bei dem der EMV-Chip den Wechsel von 2009 auf 2010 nicht beherrschte.

Laut Insider-Informationen ist der Fehler darauf zurückzuführen, dass implementierte Programme auf dem Chip ab dem 1. Januar 2010 in einer Reihenfolge ausgeführt wurden, die zufälligerweise in der Kombination mit dem Jahreswechsel zu einem Absturz geführt haben. Ein Szenario, das von dem niederländischen Hersteller Gemalto trotz umfangreicher Tests nicht bedacht wurde. Für den weltweit größten Anbieter von Chipkarten war dieser Fehler ein Fiasko. Millionen Deutsche sind beunruhigt – und der englische Sicherheitsexperte Ross Anderson wurde bestätigt. Er hatte behauptet, dass der EMV-Standard, der von einem Konsortium aus Europay International, MasterCard und VISA entwickelt wurde und auf Zahlungskarten mit Prozessorchip angewandt wird, zu komplex und unsicher sei. Zudem bemängelte er die Ingenieursarbeit und das miserable Qualitätsmanagement.

Anderson ist es mit einem Forscherteam an der Universität Cambridge gelungen, die PIN-Prüfung bei EC- und Kreditkarten auszuhebeln. Die Expertengruppe zeigt in ihrem Bericht, wie sie es mit wenigen Mitteln geschafft haben, durch eine Man-in-the-Middle-Attacke ein Zahlungsterminal zu überlisten. Zum einen gaukelten sie der Karte vor, das Terminal hätte auf die Legitimation per Unterschrift umgestellt. Zum anderen ließen sie das Terminal glauben, dass die korrekte PIN eingegeben wurde. In einem Testlauf in der Universitätsmensa von Cambridge überlisteten die Experten so das Zahlungssystem, was dazu führte, dass jede PIN-Kombination akzeptiert wurde.

Für Anderson ist klar, dass der EMV-Standard unsicher ist. Die großen Probleme seien auf die Komplexität des Verfahrens zurückzuführen, das niemand in der Branche so richtig kennt. Banken, Terminal- oder Kartenhersteller und Software-Programmierer verfügen laut Anderson nur über Teilwissen. Den vollständigen Überblick besitze kaum jemand. Das bestätigt Salim Güler von der Kobil Systems GmbH, die Kartenlesegeräte für Online-Banking herstellt. „Wir erhalten lediglich ein Software-Development-Kit, das uns die Schnittstellen zur Verfügung stellt, die wir benötigen. Viel mehr wissen wir über den EMV-Standard nicht."

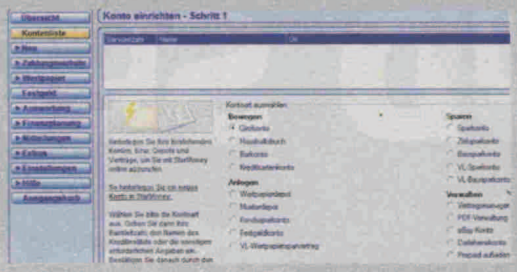
Für viele Programmierer ist die fehlende Transparenz nicht gerade ein Zeichen für Sicherheit. Denn so können Schwachstellen nur schwer entdeckt werden. Ross Anderson fügt hinzu: „Die Implementierungen des EMV-Verfahrens liefern nicht immer die Ergebnisse, wie es die Spezifikation behauptet. Man muss davon ausgehen, dass es weitere Lücken auf den Girokarten gibt, die auch eines Tages ausgenutzt werden."

Der Zentrale Kreditauschuss (ZKA) hingegen meldet, dass deutsche Karten sicherer sind, als die getesteten britischen. Der angebliche Grund: Während auf deren fehlerhaften Karten das EMV-Verfahren direkt implementiert ist, läuft auf dem Plastikgeld, das in Deutschland ausgegeben wird, das →

Vollversion von StarMoney für sicheres Online-Banking auf Ihrem PC

Wir zeigen Ihnen, wie Sie mit der Banking-Software Überweisungen gefahrlos abschicken und ganz übersichtlich mehrere Konten bei unterschiedlichen Geldinstituten verwalten können

Für viele Sicherheitslücken beim Online-Banking ist der Webbrowser verantwortlich. Durch Schwachstellen in Multimedia-Plug-ins wie Adobe PDF oder Flash können Schädlinge auf den Rechner gelangen und die Banking-Zugangsdaten des Nutzers ausspionieren. Deutlich sicherer ist da das Banking-Programm StarMoney. Es ist viel weniger anfällig für Malware-Angriffe, als der Browser. Zudem ist das Banking deutlich übersichtlicher: Sie loggen sich nur einmal in das Programm ein und erhalten einen Überblick über alle Ihre Konten. Also zum Beispiel Giro- und Tagesgeldkonten oder Festgeldanlagen – auch wenn Sie Ihr Geld unterschiedlichen Banken anvertraut haben. Vorausgesetzt, die jeweiligen Institute unterstützen HBCI+. Sie verwalten mit StarMoney sogar Ihr PayPal- und eBay-Konto und bezahlen gewonnene Auktionen direkt aus dem Programm heraus. Außerdem laden Sie per StarMoney Prepaid-Handy-Karten auf und erhalten eine Übersicht von Punktesystemen wie Payback oder Miles & More der Lufthansa. Noch sicherer wird StarMoney, wenn Sie eine zusätzliche Hardware einsetzen. Mit Kartenlesegeräten der Klasse 3, die es ab etwa 60 Euro im Handel gibt, haben Schädlinge auf dem PC keine Chance. Der Reader baut eine verschlüsselte Verbindung direkt zur Bank auf und nicht über den PC. Sicherer geht es momentan nicht.



1. Konto anlegen

Nach dem Installieren richten Sie die einzelnen Konten ein. Dazu genügen Bankleitzahl, Kontonummer und Ihre PIN. Voraussetzung: Ein Konto, das HBCI+-fähig ist. Fragen Sie im Zweifelsfall bei Ihrer Bank nach.

2. Überweisung ausführen

Das Formular für Transaktionen sieht genauso aus, wie der Überweisungsträger Ihrer Bank. Wie gewohnt ausfüllen und abschicken. Je nachdem, welches TAN-Verfahren Sie nutzen, die TAN-Nummer eingeben – fertig.

3. Finanzplanung

StarMoney kann auch Kalkulationen, wertet Ihre Einnahmen und Ausgaben nach Kategorien aus, hilft bei der Baufinanzierung sowie beim Zuwachssparen und rechnet aus, wann ein Kredit getilgt ist.

Betriebssystem SECCOS. EMV ist hier sozusagen nur eine Software, so ein Kartenexperte gegenüber CHIP. Dieses System zu knacken, sei eine deutlich kompliziertere Aufgabe, als bei den getesteten Karten. Erschwerend komme hinzu, dass die deutschen Girokarten eine dynamische Autorisierung (DDA-Chip) einsetzen, während in Großbritannien eine statische Autorisierungsform (SDA-Chip) zum Einsatz kommt.

Ross Anderson prophezeite jedoch bereits bei Veröffentlichung des Hacks, dass die deutschen Banken das Problem von der Hand weisen werden. Er kündigte gegenüber CHIP an, dass sich das Team die Karten hierzulande genauer anschauen werde – und rechnet mit Schwachstellen. Ob und inwieweit die Forscher recht behalten werden, wird sich also zeigen. So lange müssen wir der Girocard (ehemals EC-Karte) vertrauen.

Schock in der Schalterhalle

Aber es muss nicht immer eine Panne bei den digitalen Geldgeschäften sein, die Sie um Ihr Geld bringt. Denn es kann durchaus passieren, dass die Bank bei klassischen Sparbüchern die Auszahlung verweigert. Die Begründung: das Guthaben sei verjährt. CHIP ist ein Fall bekannt, in dem ein große deutsche Bank einem Leser kein Geld auszahlen wollte, da das Sparbuch seit 2001 brach lag. Der Angestellte versicherte, das Konto sei nicht mehr auffindbar, die Kontonummer bereits an eine andere Person vergeben. Daraufhin behielt der Mitarbeiter das Sparbuch ein. Erst nach energischer Aufforderung erhielt der Kunde eine beglaubigte Kopie des Buches. So bekam er acht Wochen später sein Erspartes zurück. Ohne Beleg wäre das Geld vermutlich verloren gewesen.

Ein selten auftretender Vorfall, aber kein Einzelfall, wie uns ein weiterer Leser meldete. Ihm wurde auf demselben Weg ein kaum benutztes Sparbuch weggenommen, er bekam jedoch keine Quittung. Wochen später wollte der Bankmitarbeiter nie ein Sparbuch entgegengenommen haben – das Geld war weg. Ein Angestellter einer Postbank-Filiale berichtete uns ebenfalls von Fällen, dass Konten aus dem System verschwinden. Ein bis zwei Mal pro Jahr muss er Kunden an das Reklamationsmanagement weiterleiten, da eingeschlafene Konten nicht mehr auffindbar sind. Laut Aussage der Postbank kommen alle Kunden wieder an ihr Geld, denn im Rahmen der Schuldrechtsreform darf ein Guthaben nicht verjähren. Banken, die das anders handhaben, handeln rechtswidrig.

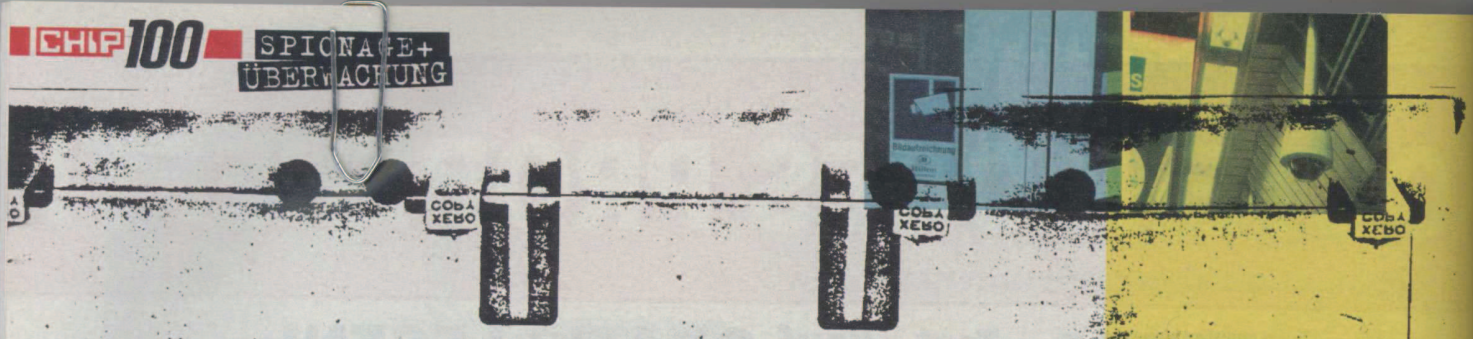
Doch viele Banken haben einen anderen Weg gefunden, sich von brachliegenden Konten zu befreien – mit ihren AGB. Legt der Kunde ein Sparkonto an, unterschreibt er mitunter, dass Konten nach einem gewissen Zeitraum ohne Bewegung relativ hohe Gebühren kosten. So schmelzen die unangetasteten Guthaben allmählich dahin.

DOMINIK.HOFERER@CHIP.DE

AUF DVD

CHIP-Sicherheitsbrowser ist ein sicherheitsoptimierter Firefox, der extra für das Online-Banking konfiguriert wurde
ClamWin durchsucht als zusätzlicher Virenscanner den PC
CWShredder verhindert das Umleiten auf ungewollte Seiten
Gmer schützt vor Eindringlingen mit Rootkit-Funktion
HiJackThis entdeckt Änderungen am Rechner durch Viren
Panda Cloud Antivirus bietet schlanken und effektiven Virenschutz, der den Rechner kaum ausbremst
RootAlyzer bekämpft Rootkit-Trojaner
StarMoney – umfangreiche Vollversion, die komfortabel Konten verwaltet und sicheres Online-Banking per HBCI ermöglicht

Die Tools finden Sie unter CHIP-Code **GELDPANNE**



Das Zeitalter der ÜBERWACHUNG

Die Vorratsdatenspeicherung ist vorerst ausgesetzt. Doch machen wir uns keine Illusionen: In einer Welt, die zunehmend aus Daten besteht, wird jeder überwacht. Zwangsläufig

VON ANDREAS HENTSCHEL

Man kann im Internet einen Nistkasten für Vögel kaufen. Das edle Modell aus Aluminium und Birkenholz kostet 70 Euro und heißt „Wolfgang S." „Sicherheit und Privatsphäre für unsere Singvögel", steht in der Produktbeschreibung. Und natürlich: Die Brutstätte sieht aus wie eine Überwachungskamera. Obwohl Schäuble nun nur noch über die Staatsfinanzen wacht, bleibt das Image des ungenierten Überwachers, der viele Informationen über seine Bürger sammelt, an ihm haften. Wahrscheinlich zu Recht. In den vier Jahren seiner Amtszeit hat eine allgemein akzeptierte Überwachungskultur in unserer Gesellschaft Einzug gehalten, die jedem auffallen dürfte, der mit offenen Augen durch die Stadt geht – sehen Sie sich einmal unser Video auf CHIP 100, Punkt 11, an.

Ein bisschen ungerecht ist das aber dennoch. Es könnte nämlich genauso gut Nistkästen namens Sergey B., Larry P. oder Mark Z. geben. Das sind die Gründer von Google und Facebook, den beiden größten und erfolgreichsten Firmen des digitalen Industrie-Zeitalters. Diese Unternehmen stellen keine physischen Waren her, sie machen Daten zu Geld. Die Daten ihrer Nutzer. Vier Millionen Deutsche haben einen Facebook-Account, der Suchmaschinen-Marktanteil von Google liegt in Deutschland jenseits der 90 Prozent. Auch Google, Facebook und viele andere Internetkonzerne überwachen ihre Nutzer ungeniert – und in weit höherem Maße als der Staat seine Bürger. Doch warum wird das Speichern von Informationen so unterschiedlich bewertet? Warum begegnet man dem Staat höchst argwöhnisch, während Twitter, Social Networks und Google-Handys völlig bedenkenlos genutzt werden? „Die breite Masse der Bevölkerung ist da in der Tat noch undifferenziert und blauäugig", sagt Dr. Thilo Weichert vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. „Im Internet fehlt die Sensibilität für diese Themen noch – das ist allenfalls in der Nerd-Szene angekommen."

Andererseits scheint das Misstrauen gegenüber dem Staat aber auch übertrieben. Gut: Ja, unser Staat ist neugierig. Immer mehr Telefone werden abgehört (▶ S. 116, Grafik). Auch Verkehrsdaten werden →

tausendfach überprüft – also wer mit wem und wann Mails schreibt oder wie lange telefoniert. Aber machen wir uns nichts vor: Im Schnitt kommen auf 100.000 Einwohner gerade einmal 18 solcher Abhör- und Abfrage-Aktionen. Von einem Überwachungsstaat kann nicht die Rede sein. Die Quantität ist nicht erschreckend, vielleicht schon eher die Qualität: Der Chaos Computer Club hat in einem Gutachten für das Bundesverfassungsgericht einmal aufgezeigt, welche aussagekräftigen Profile sich allein aus den bei der Vorratsdatenspeicherung gesammelten Informationen erstellen lassen – siehe dazu die Grafik auf ► S. 118 und das komplette Gutachten auf CHIP 100, Punkt 29.

Solche Profile wird es vorerst nicht geben. Denn gerade hat das Bundesverfassungsgericht in Karlsruhe eines von Schäubles Lieblings-Projekten gekippt: Das „Gesetz zur Neuregelung der Telekommunikationsüberwachung" vom 21. Dezember 2007 – oder umgangssprachlich: die Vorratsdatenspeicherung. Doch das Urteil aus Karlsruhe bedeutet nicht das Ende jeglicher staatlicher Neugier, ganz im Gegenteil. Die Richter halten nur die Ausgestaltung dieses Gesetzes für verfassungswidrig, das eigentliche Ansinnen aber ausdrücklich nicht. Einer der zentralen Sätze in der Urteilsbegründung liest sich so: „Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist [...] für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung." Das Bundesverfassungsgericht hält es also für legitim, dass der Staat Telekommunikationsdaten speichern lässt – und zwar ohne konkreten Anlass. Was die Richter ansonsten einfordern, würde auch Google, Facebook & Co. gut zu Gesicht stehen: hinreichende Datensicherheit und eine Begrenzung der Verwendungszwecke der Daten.

Rechtsfreier Raum: Wer zurzeit im Web ein krummes Ding dreht, bleibt wahrscheinlich unentdeckt

Den Holzhammer holten die Richter allerdings raus, indem sie die bestehenden Regeln für nichtig erklärten. Das heißt, sie wurden sofort außer Kraft gesetzt. Und das heißt: Alle Vorratsdaten konnten direkt nach dem Urteil gelöscht werden, was die Provider auch schnell taten. Darüber herrschte übrigens beim Verfassungsgericht keine Einigkeit, die Nichtigkeit wurde mit 4:4 Richterstimmen entschieden – ein Patt gilt als Ja. Die Alternative wäre die Festlegung einer Übergangsfrist gewesen, innerhalb der das überarbeitete Gesetz in Kraft treten muss. Die gibt es aber nicht, und so haben wir momentan in der Praxis tatsächlich das, was man einen rechtsfreien Raum nennt.

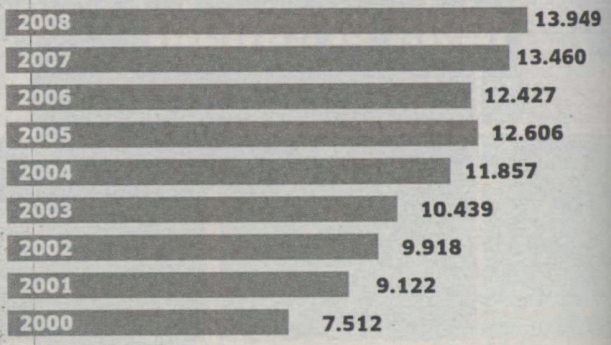
„Wir können praktisch nicht mehr ermitteln, weil uns die Spuren fehlen", sagt Klaus Jansen, Bundesvorsitzender des Bundes Deutscher Kriminalbeamter. Natürlich vertritt der Gewerkschaftsboss eine Lobby, als Polizist muss er so etwas sagen. „Ich will ja keine Bedrohungsszenarien aufbauen, aber in einem bestimmten Feld können wir nun nichts mehr machen." Bei einem Einbruch, bei →

NEUGIERIGE BEHÖRDEN

Die Polizei hört immer mehr Telefonate mit. Ein Grund dafür ist der Handy-Boom, ein anderer ist die Digitalisierung der Kriminalität

Die vom Bundesamt für Justiz jährlich veröffentlichten Statistiken (siehe Grafik) sprechen Bände: Von 2000 bis 2008 hat sich die Zahl der Telefonüberwachungen nahezu verdoppelt. Ein Grund dafür ist, dass Kriminelle zunehmend viele Mobiltelefone parallel benutzen – die sich alle in der Statistik niederschlagen. Allerdings: In dem vorliegenden Neun-Jahres-Zeitraum ist auch die Zahl der Verfahren, in denen Telekommunikations-Überwachung angeordnet wurde, massiv gestiegen: von 3.353 im Jahr 2000 auf 5.348 im Jahr 2008.

ANZAHL DER BUNDESWEITEN TELEFONÜBERWACHUNGEN



E-BOOK
Risiko Tauschbörse
Millionen Menschen surfen im Netz – und wissen gar nicht, was ihre IP-Adresse verrät und wer sie kennt. Dieses E-Book klärt Sie auf
27

HÖRBUCH
Angriff auf die Freiheit (Auszug)
Der Staat sammelt biometrische Daten, Überwachung gehört zum Alltag. Sind unsere Rechte überhaupt noch etwas wert?
30

SPIEL: SPECIAL AGENT
Werden Sie Spezialagent
Suchen Sie sich in diesem Jump-'n'-Run-Game Ihren Weg als schick gekleideter Spezialagent durch 15 knifflige Missionen
34

24 25 26 27 28 29 30 31 32 33 34 35 36

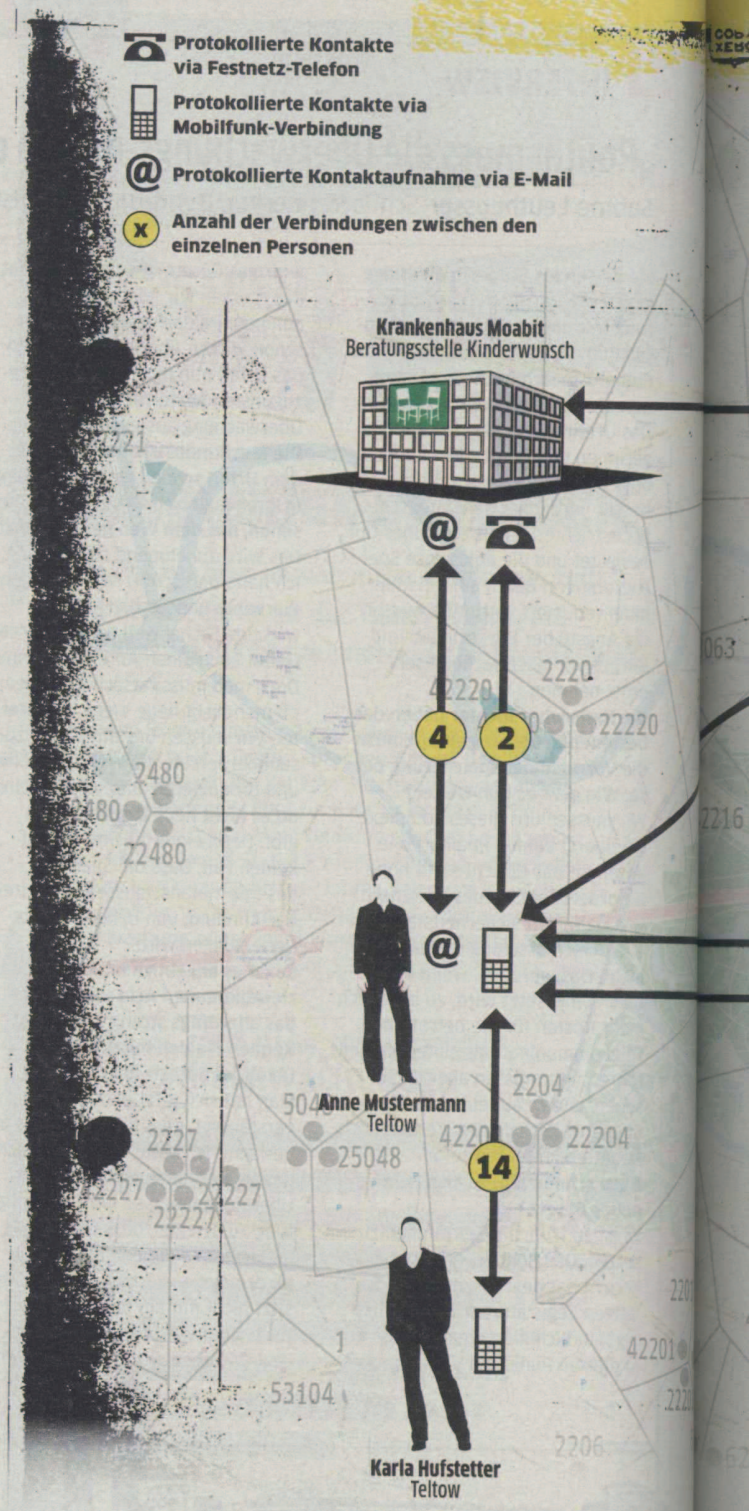
einem Mord, bei einem Autounfall – überall gibt es Spuren. Bei Computerkriminalität gibt es in der Regel nur eine Spur: die IP-Adresse. Die ist aber im Moment nichts wert.

Telefonat mit einem Ermittler im Bereich Computerkriminalität. Keine Namen hier, Kripo-Beamte dürfen nicht mit Journalisten über ihre Arbeit reden. Etwa ein Drittel seiner Ermittlungen kann der Kriminalhauptkommissar nach dem Karlsruher Urteil zu den Akten legen. Zu den Akten der nicht aufgeklärten Fälle. „Sicher, das sind nicht alles Kapitalverbrechen", sagt er und erzählt von einem kuriosen Fall. Ein Kunde einer großen Bank hat Anzeige erstattet. Irgendjemand, der seine Kontonummer kennt, macht sich seit Monaten einen Spaß: Er gibt diese auf der Online-Banking-Seite ein und dann dreimal ein falsches Passwort. Das führt zur Sperrung. Der Online-Zugriff auf das Konto wird erst nach ein paar Tagen wieder freigeschaltet. Nach kurzer Zeit beginnt das Spiel von vorn. „Der Kunde ist genervt, die Bank ist genervt, alle sind genervt."

Rotz und Wasser: 7.000 Euro weg vom Konto – aber keine polizeilichen Ermittlungen

Die Bank hat nach einigem Hin und Her die IP-Adressen rausgerückt, mit denen zu den fraglichen Zeiten auf das Konto zugegriffen wurde. Die Daten liegen jetzt auf dem Schreibtisch des Ermittlers, doch sie kamen zwei Tage nach dem Urteil. Bei den Providern war da schon alles gelöscht. Vielleicht drei Tage bleiben die IP-Adressen derzeit noch in deren Datenbanken gespeichert. Dann sind sie weg. Für die Polizei ein GAU. Drei Tage kann es allein schon dauern, bis eine Anzeige von der Dienststelle ins zuständige Kommissariat weitergeleitet wird. Und nicht alle Fälle sind so lapidar wie das Lausbuben-Stück mit dem Online-Konto. „Ich habe hier ja auch Fälle von Industriespionage liegen, von Kreditkarten- oder Identitätsklau." Letztens saß eine Hausfrau bei ihm im Büro, der 7.000 Euro vom Konto gephisht wurden. „Die hat Rotz und Wasser geheult. Wenn ich dem Opfer dann sagen muss, Entschuldigung, ich würde ja gerne ermitteln, scheitere aber am Datenschutz – das kann es doch nicht sein."

Das kann es doch nicht sein, meint auch Datenschützer Dr. Thilo Weichert. „Es kann doch nicht sein, dass wir Datenschützer immer wieder als Verhinderer von Polizeiarbeit dargestellt werden", sagt er hörbar genervt. Auch Weichert betreibt Lobby-Arbeit, sogar eine, die der des Gewerkschafts-Bosses Jensen ähnelt. Er fordert mehr Geld vom Staat: Das Problem der Polizei sei die notorisch dünne Personaldecke und dass es an vernünftigen Verfahren mangele. „Es kann jedenfalls nicht sein, dass wegen all dieser Versäumnisse die ganze Bevölkerung unter Generalverdacht gestellt wird", sagt Weichert. Die Verfassungsrichter sehen diesen Punkt anders. Anlasslose Speicherung gestehen sie dem Staat zu, das muss auch der Datenschützer anerkennen: „Dann muss die Speicherung aber so sicher wie möglich und so dezentral wie möglich erfolgen. Und vielleicht können →

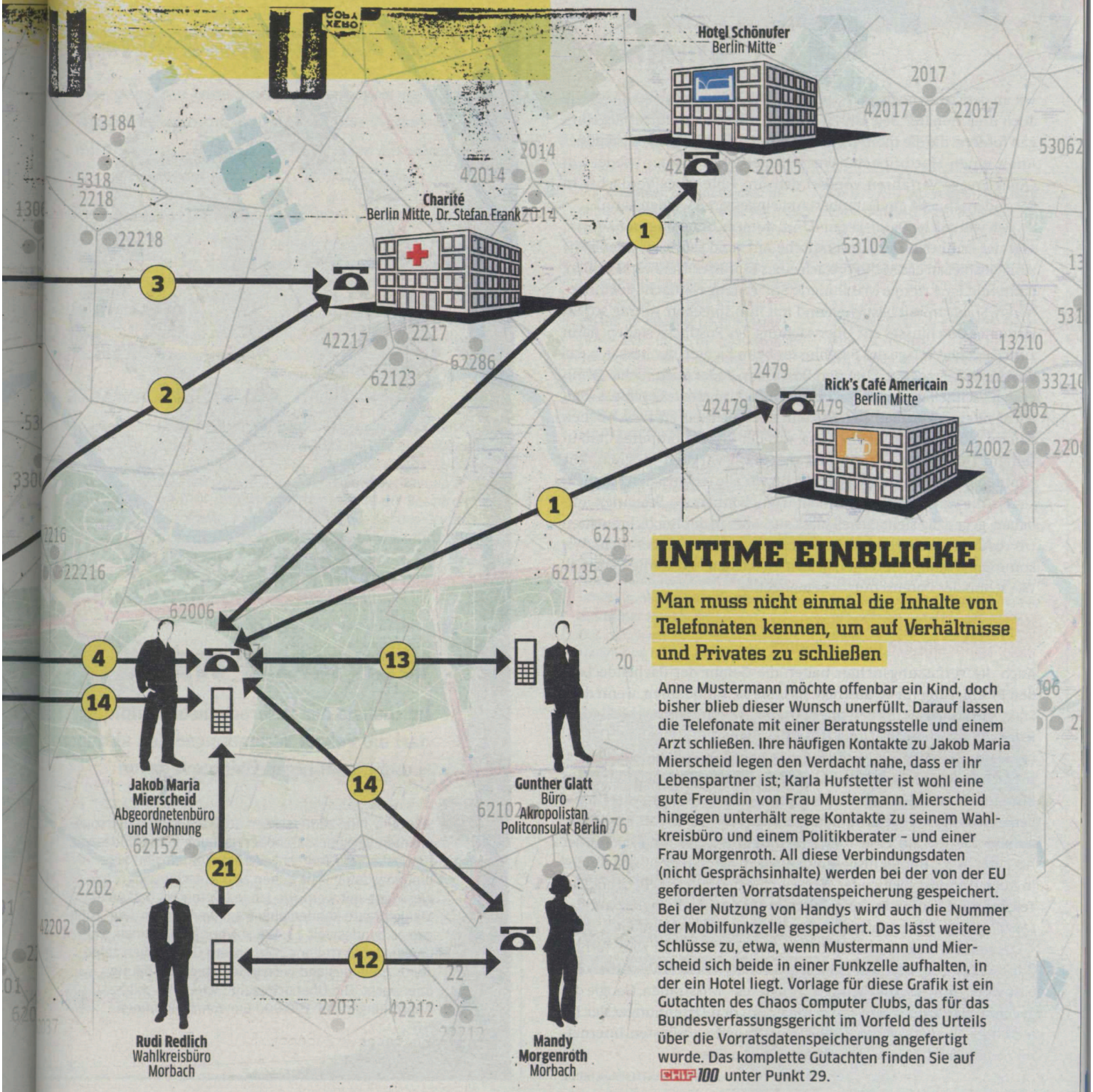


SOFTWARE
Schluss mit Internetspionage
SpyBot Search & Destroy durchsucht Ihre Windows-installation nach spionierenden Programmen und eliminiert diese
52

SOFTWARE
Überwachung mit Webcams
Stellen Sie Ihre Webcams im Büro auf. CamSpy erkennt Bewegungen und startet die Aufnahme
57

SOFTWARE
Wichtige Texte verschlüsseln
Mit dem Textprogramm Crypditor schützen Sie Ihre Daten vor neugierigen Blicken und fiesen Langfingern
59

50 51 52 53 54 55 56 57 58 59 60 61 62



INTIME EINBLICKE

Man muss nicht einmal die Inhalte von Telefonaten kennen, um auf Verhältnisse und Privates zu schließen

Anne Mustermann möchte offenbar ein Kind, doch bisher blieb dieser Wunsch unerfüllt. Darauf lassen die Telefonate mit einer Beratungsstelle und einem Arzt schließen. Ihre häufigen Kontakte zu Jakob Maria Mierscheid legen den Verdacht nahe, dass er ihr Lebenspartner ist; Karla Hufstetter ist wohl eine gute Freundin von Frau Mustermann. Mierscheid hingegen unterhält rege Kontakte zu seinem Wahlkreisbüro und einem Politikberater – und einer Frau Morgenroth. All diese Verbindungsdaten (nicht Gesprächsinhalte) werden bei der von der EU geforderten Vorratsdatenspeicherung gespeichert. Bei der Nutzung von Handys wird auch die Nummer der Mobilfunkzelle gespeichert. Das lässt weitere Schlüsse zu, etwa, wenn Mustermann und Mierscheid sich beide in einer Funkzelle aufhalten, in der ein Hotel liegt. Vorlage für diese Grafik ist ein Gutachten des Chaos Computer Clubs, das für das Bundesverfassungsgericht im Vorfeld des Urteils über die Vorratsdatenspeicherung angefertigt wurde. Das komplette Gutachten finden Sie auf CHIP 100 unter Punkt 29.

SOFTWARE
Verschlüsseln Sie Ihren PC
TrueCrypt kann nicht nur einzelne Dateien, sondern sogar ganze Festplatten unknackbar verschlüsseln
63

SOFTWARE
Finden Sie Netzwerkspione
Mit Wireshark lässt sich der gesamte Netzwerkverkehr aufzeichnen und analysieren – so sind Schwachstellen schnell gefunden
68

CHIP-PDF
Spionage am Arbeitsplatz
Dank geheimer Spionagetools weiß Ihr Chef immer, was Sie gerade tun. CHIP sagt, wie Sie sich schützen
73

63 64 65 66 67 68 69 70 71 72 73 74 75

wir an der Dauer noch etwas ändern. Vielleicht reichen statt sechs ja auch drei Monate." Seit Jahren würden die Datenschützer Regelungen fordern, die die Interessen der Polizei und die des Datenschutzes unter einen Hut bringen: „Wir schlagen etwa immer wieder ein Quick-Freeze-Verfahren vor, bei dem im Falle eines Verdachts in Sekundenschnelle ein Datenbestand eingefroren werden kann."

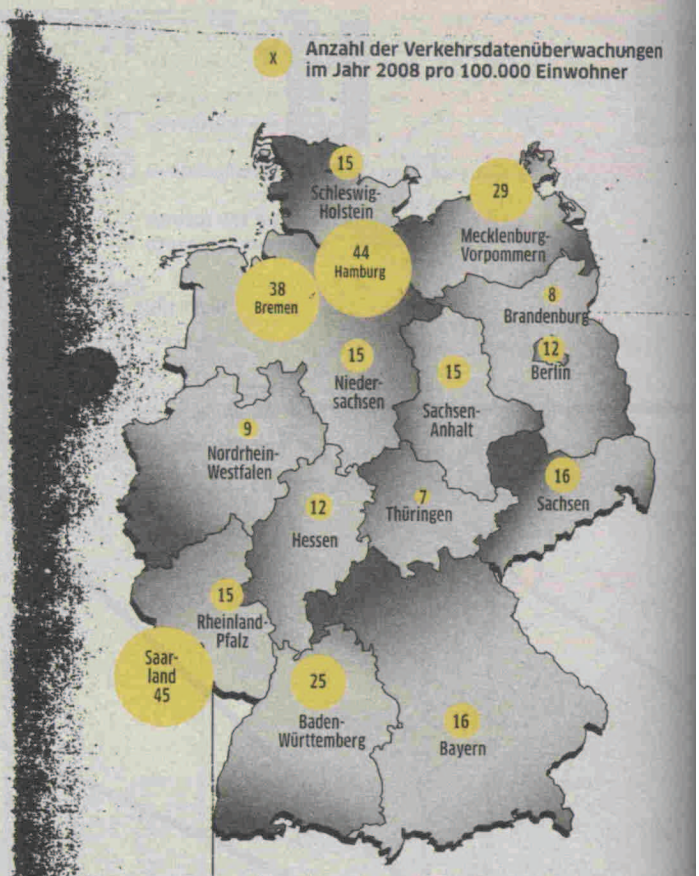
„Ich will solche Daten ja nur dann, wenn es unbedingt sein muss", sagt der Ermittler. Der bürokratische Aufwand sei riesig. „Wenn wir zum Beispiel an das Mail-Postfach eines Erpresser-Netzwerks wollen, dann rollt eine riesige Maschinerie an." Anfangsverdacht dokumentieren, Staatsanwalt besuchen und mit ihm sprechen, Antrag auf Erlass eines Beschlusses zur Überwachung des Postfachs stellen, dann zum Gericht, Vorlage des Beschlusses beim Richter, der liest sich das durch, stellt Fragen, erlässt den Beschluss – oder auch nicht. „Wenn es ganz schnell gehen muss, bekomme ich so einen Beschluss vielleicht in einem halben Tag. Es kann aber auch bis zu zwei Wochen dauern", so der Kripo-Mann. „Das, was der Chaos Computer Club in seinem Gutachten schreibt, ist technisch wirklich möglich. Wir könnten so etwas herausfinden. Wenn wir alle technischen Möglichkeiten, die wir haben, zusammenfassen, können wir Szenarien aufbauen, gegen die sieht Orwell blass aus. Aber in der Praxis bräuchten wir dafür Heerscharen von Beamten. Die haben wir aber nicht. Wir kommen ja kaum hinterher, gezielt zu suchen." Zu wenig Personal. Wie schon der Datenschützer bemängelte.

Keine Profile möglich: Datenspeicherung über sechs Monate ist in Ordnung

Auch die Verfassungsrichter halten die Gefahr der flächendeckenden Profilierung für so abstrakt, dass sie sie hinnehmen, wenn dem Staat nicht die Gesamtheit aller Daten zur Verfügung steht. Und da jedes Telekommunikations-Unternehmen seine eigenen Datenbanken unterhält, ist es den Behörden nach Einschätzung der Karlsruher Juristen nicht möglich, umfassende Profile jedes einzelnen Bürgers zu erstellen. „Eine Speicherung der Telekommunikationsverkehrsdaten für sechs Monate stellt sich auch nicht als eine Maßnahme dar, die auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt wäre. Sie knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotenzial, das sich mit dieser verbindet."

Gegenüber dem Staat, der in einigen Fällen auf ein paar Verbindungsdaten zugreifen will, herrscht bei den meisten Menschen ein – zum Teil diffuses, zum Teil sehr konkretes – Misstrauen. Google dagegen belegt, trotz aller Diskussionen um den Datenhunger der Informationskrake, auf der Liste der vertrauenswürdigsten Internetmarken in Deutschland derzeit den zweiten Platz.

ANDREAS.HENTSCHEL@CHIP.DE



WER MAILT WEM?

Im Dienste der Verbrechensbekämpfung darf die Polizei Verbindungsdaten abfragen – und macht regen Gebrauch davon

Seit dem Jahr 2008 werden auch die Zahlen der sogenannten Verkehrsdatenüberwachung vom Bundesamt für Justiz veröffentlicht. Verkehrsdaten sind Verbindungsdaten – sie geben also Aufschluss darüber, wer wann mit wem wie lange telefoniert hat. Auch Mailkontakte können abgefragt werden. Im Jahr 2008 gab es bundesweit 13.426 solcher Maßnahmen. Mit ungleicher Verteilung, wie unsere Grafik oben zeigt: Je nach Bundesland wird unterschiedlich häufig überwacht. Die Übersicht zeigt, wie viele solcher Anordnungen auf 100.000 Einwohner kommen.

SOFTWARE
Keine Mitleser bei E-Mails
Enigmail, eine Erweiterung zu Thunderbird, ver- und entschlüsselt E-Mails, die mit OpenPGP kodiert sind
77

SOFTWARE-LINK
Werden Sie zum IP-Amerikaner
Hotspot Shield vergibt sichere IP-Adressen aus den USA. So kann bei öffentlichen Hotspots keiner im PC schnüffeln
83

GOOGLE-SPIONAGE
Autofahrer bei kurzer Pause
Google Street View bietet zahlreiche Bildinhalte, die witzige Details enthalten – werden Sie zum Street-View-Spion
85