Aktion: Gratis anonym surfen
mit JonDonym (1,5-GByte-Paket)

www.ctspecial.de

c't Security

c't Security

Startbereit auf DVD, Anleitung im Heft

Rundumschutz

Live DVD

Desinfec't
gegen Viren
plus c't Bankix, c't Surfix

Windows 8 härten
Android-Handys absichern
WLAN-Hotspots nutzen
Kinder schützen
Passwort-Cracking

Was wirklich geht

Rezepte gegen den Abhörwahn

Anonym im Netz, Verschlüsselung, Messaging

Editorial

Wir haben was gegen NSA und Prism, auch wenn gegen das Arsenal der Geheimdienste kaum ein Kraut gewachsen ist. Doch mit Hilfe dieses Sonderhefts machen Sie es den Schurken und allzu neugierigen Staaten so schwer wie möglich.

c't Security klärt verlässlich auf, gibt Anleitungen und enthält exklusive Werkzeuge, damit Sie sich das auf Ihre Bedürfnisse zugeschnittene Sicherheitspaket schnüren können. Wir zeigen Ihnen, wie Sie Apps kontrollieren, anonym surfen (ein Gutschein für JonDonym gehört dazu) und Schädlinge auf Ihren Rechnern mit dem exklusiven Desinfec't 2013 aufspüren, das direkt von der DVD startet.

Die Beiträge, wie Sie Mail und Daten verschlüsseln, über öffentliche Hotspots sicher surfen, Ihr Smartphone absichern und die Schutzmechanismen von Windows 8 einsetzen, erhalten durch die aufgedeckte Totalüberwachung besondere Brisanz. Das Anliegen des c't Security-Teams ist es aber auch, Sie über die aktuelle Nachrichtenlage hinaus über digitale Sicherheit zu informieren, denn das Thema wird uns langfristig begleiten.

Jürgen Rink

Inhalt

Globaler Abhörwahn

8 Globaler Abhörwahn
13 Prism yourself: Was finden Sie über sich heraus?
14 Gegen die Totalüberwachung
15 Wegweiser zu den Rezepten im Heft

Windows-Sicherheit

16 Die neuen Tricks der Internet-Gauner
20 Mehr Schutz beim Surfen
24 Das Schutzkonzept von Windows 8
28 Windows XP vor dem Support-Aus
32 Der c't-Trojaner-Test
38 Virenscanner im Test
44 FAQ Virenscanner

Mobil und Apps

46 Die Smartphone-Trojaner-Flut
50 Smartphones absichern
52 Android-Geräte verschlüsseln
56 Angriffe auf Smartphones mit Honeypots analysieren
61 Ortung auf dem Smartphone verhindern
62 Bezahlen mit dem Handy
68 Netzwerkverkehr von Smartphones kontrollieren

Risiko WLAN

72 Gefahren bei der Hotspot-Nutzung
76 Das Bestiarium der Hotspot-Angriffe
82 Öffentliches WLAN sicher nutzen

c't-Rundumschutz auf DVD

6 Übersicht DVD-Inhalt und Aktion
86 Virenjagd mit Power und Komfort
88 Scannen und Reinigen mit Desinfec't
94 FAQ Desinfec't 2013
96 Online-Banking und Finanzverwaltung mit c't Bankix
100 Sicher surfen mit c't Surfix

DVD-Download

Infos zum Download der Heft-DVD und zur Seriennummer finden Sie unter:

www.ct.de/cs1303004

Rundumschutz

6 Übersicht DVD-Inhalt und Aktion
86 Virenjagd mit Power und Komfort
88 Scannen und Reinigen mit Desinfec't
96 Online-Banking und Finanzverwaltung mit c't Bankix
100 Sicher surfen mit c't Surfix

Android-Handys absichern

46 Die Smartphone-Trojaner-Flut
50 Smartphones absichern
52 Android-Geräte verschlüsseln
61 Ortung auf dem Smartphone verhindern
68 Netzwerkverkehr von Smartphones kontrollieren

Rezepte gegen den Abhörwahn

8 Globaler Abhörwahn
13 Prism yourself: Was finden Sie über sich heraus?
14 Gegen die Totalüberwachung
15 Wegweiser zu den Rezepten im Heft

Passwort-Cracking

126 Die Passwortknacker
132 Die Tools und Techniken der Passwortknacker
138 Passwort-Schutz für jeden

Kinder schützen

106 Kinderschutz zwischen Laisser-faire und Total-Kontrolle
110 Webinhalte kindersicher filtern
116 Kindersicherungen für Smartphones und Tablets

Anonym im Netz

120 Dienste und Software zum Verbergen der IP-Adresse
123 Anonym surfen mit JonDonym
124 Tracking-Schutz im Browser

Identität und Passwörter

126 Die Passwortknacker
132 Die Tools und Techniken der Passwortknacker
138 Passwort-Schutz für jeden
142 Gefahr durch Identitätsdiebstahl
146 Digitale Identität schützen

Verschlüsselung

150 Vertrauenswürdige Kommunikation
154 Mail-Verschlüsselung auf dem Rechner und mobil
158 Daten auf Online-Speichern schützen
162 FAQ Verschlüsselung

Analyse und Forensik

164 Schädlinge in der Sandbox untersuchen
168 Spurensuche auf Festplatten

Zum Heft

3 Editorial
7 Aktion: Gratis anonym surfen
170 Impressum
170 Inserentenverzeichnis

c't-Rundumschutz und anonym surfen mit JonDonym

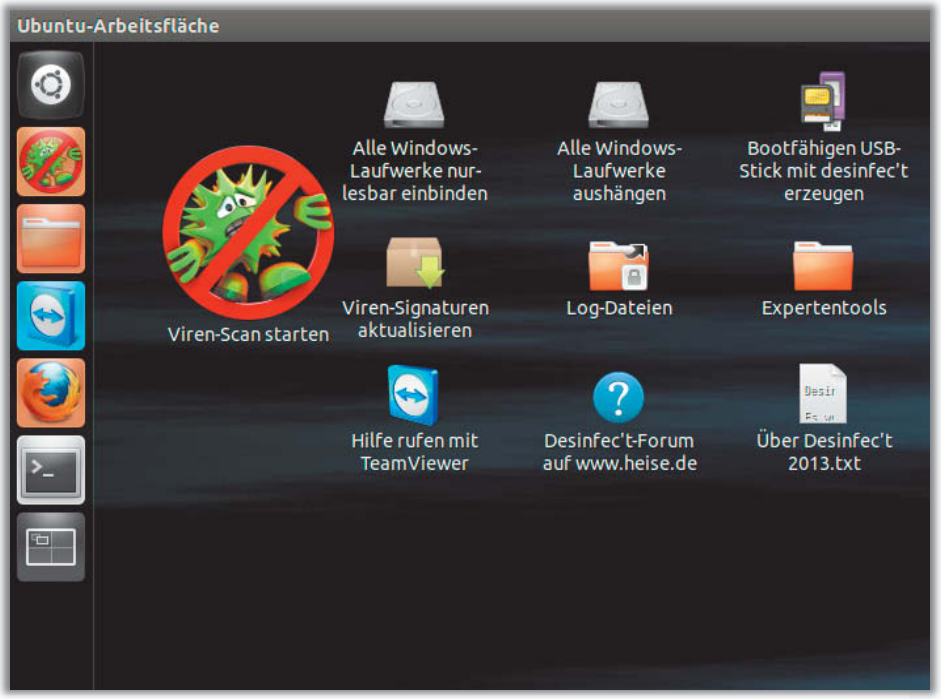
Komfortabel Viren jagen, risikolos surfen und die Bankgeschäfte online geschützt vor Angriffen erledigen: Mit den wahlweise direkt von der Heft-DVD bootenden Live-Systemen Desinfec't, c't Surfix und c't Bankix halten Sie Ihr System sauber. Wer beim Surfen nicht nur sein System, sondern auch seine Privatsphäre schützen will, dem hilft die kostenlose Aktion des Anonymisierungsdienstes JonDonym.

Desinfec't

Desinfec't 2013 ist ein bootfähiges Live-System zum Aufspüren und Löschen von Viren und anderer Malware. Gleich vier Virenscanner stehen Ihnen dabei zur Seite: Für dieses c't-Projekt dürfen wir freundlicherweise die Antiviren-Software von Avira, Bitdefender, ClamAV und Kaspersky verwenden, die bis Ende Juli 2014 auch die benötigten Viren-Signaturen bereitstellen. Besonderes Highlight dieser Desinfec't-Version ist die eingebaute Fernhilfefunktion. Die integrierte Software Teamviewer hilft Ihnen dabei, verseuchte Rechner von Bekannten und Verwandten per Fernwartung von ihren Plagegeistern zu befreien.

Desinfec't startet direkt von der Heft-DVD. Mit drei Mausklicks können Sie es aber auch auf dem USB-Stick installieren, auf dem Desinfec't deutlich schneller arbeitet als auf DVD.

Ausführlich erläutern wir den Umgang mit Desinfec't die Artikel ab Seite 86.

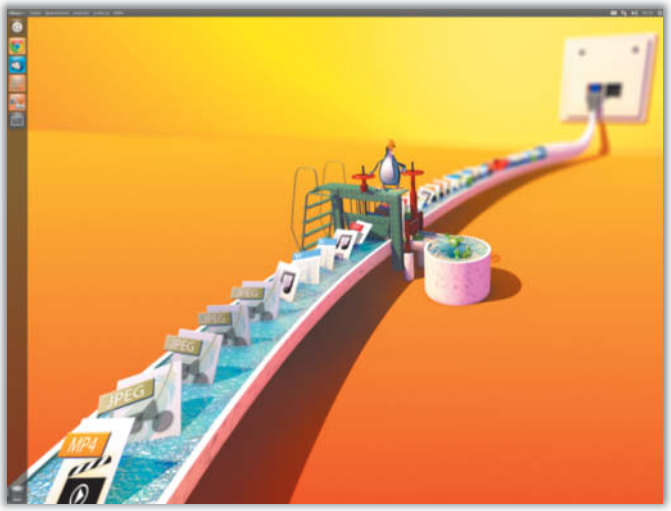


c’t Bankix

Besonders wichtig ist die Sicherheit des Systems, wenn man mit ihm Bankgeschäfte abwickeln will. Hier wünscht man sich eine bestmöglich vor Angriffen und Schadsoftware geschützte Umgebung. c’t Bankix ist ein speziell für das Online-Banking angepasstes und abgesichertes Linux-System.

Vorinstalliert haben wir unter anderem Firefox, Thunderbird und die Finanzverwaltung Hibiscus. Einmal eingerichtet, starten Sie das Live-Linux von DVD oder einem schreibgeschützten USB-Stick. Manipulationen am System sind so nicht möglich, Schadsoftware bleibt draußen. Trotzdem sind auch im laufenden Betrieb sichere Updates möglich.

Einen ersten Eindruck können Sie sich verschaffen, wenn Sie c’t-Bankix direkt von der Heft-DVD booten. Wie Sie sich ihr persönliches c’t Bankix einrichten und nutzen, erklärt der Artikel ab Seite 96.



c’t Surfix

Nur mal eben die Webseite aufgerufen und schon macht sich der Trojaner auf den Weg ins System (siehe Seite 16). Aber auch beim Mailen und Chatten lauern Gefahren.

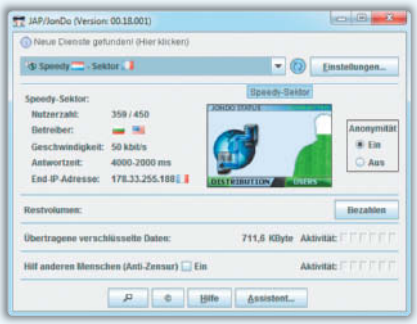
c’t Surfix ist speziell dafür entwickelt worden, Ihr System im Internet bestmöglich zu schützen. Das Live-Linux-System nutzt den Browser Google Chrome, Thunderbird kümmert sich um E-Mails und als Instant Messenger ist das Programm Pidgin vorgesehen. Für BitTorrent-Downloads haben wir Transmission installiert. Sie können c’t Surfix direkt von der DVD oder von einem USB-Stick booten oder in einer virtuellen Maschine starten.

Firmen und Schulen, die im Netz einen TFTP-Server installieren, steht mit c’t Surfix ohne weitere Installation ein sicheres Surfsystem zur Verfügung.

Was c’t Surfix alles kann und wie Sie es am besten nutzen, erklärt der Artikel ab Seite 100 im Detail. (anm)

Aktion:

Gratis anonym surfen



Online-Spione greifen von mehreren Seiten an. JonDonym verspricht hier Abhilfe: Während die Komponente JonDo die IP verschleiert, sorgt das Zusatzprogramm JonDoFox dafür, dass man beim Surfen mit dem Firefox-Browser möglichst wenig Spuren hinterlässt. JonDonym bietet hierzu auch einen Premiumdienst an mit Downloadgeschwindigkeiten von bis zu 1,5 MBit/s.

c’t-Security-Leser erhalten kostenlos ein Kontingent von 1,5 GByte für den Premiumdienst mit JonDo, das sie zwischen dem 23. Juli 2013 und dem 31. Januar 2014 nutzen können. Das Aktions-Kontingent gilt auch, wenn Sie das von JonDonym angebotene ISO-Image einer Live-CD herunterladen. Damit erhalten Sie ein fertig konfiguriertes Linux zum anonymen Surfen, Mailen oder Verwalten eines Servers, das sich von DVD oder USB-Stick starten lässt.

Um das Premium-Kontingent freizuschalten, müssen Sie während der Installation einmal einen 16-stelligen Code eingeben. Details hierzu finden Sie über den Link unten. Achtung: Der Code funktioniert nicht, wenn Sie im Client bereits ein Konto angelegt haben; Sie müssen diesen dann mit allen Kontoeinstellungen (vorher sichern) deinstallieren und neu aufsetzen.

Mehr dazu, wie JonDonym funktioniert und worauf man bei der Anwendung achten sollte, erfahren Sie in den Artikeln auf den Seiten 120 und 123.

www.ct.de/cs1303006

Holger Bleich

Globaler Abhörwahn

Was der Whistleblower Edward Snowden ans Tageslicht befördert hat, zwingt auch jene zum Umdenken, die bislang nach dem Motto leben: „Wer nichts zu verbergen hat, muss nichts befürchten." Der US-Auslandsgeheimdienst durchleuchtet Kommunikation großflächig und anlasslos. Ins Visier der NSA geraten mitunter Unschuldige. Auch deutsche Behörden sind nicht zimperlich. Es ist Zeit, über Maßnahmen gegen die Erosion der eigenen Privatsphäre nachzudenken.

Den 24. Januar 2012 wird Saad Allami aus dem kanadischen Quebec nicht so schnell vergessen. Als er gerade seinen siebenjährigen Sohn aus der Schule abholen wollte, fingen ihn Polizeibeamte ab und setzten ihn fest. Anschließend stürmten Ermittler seine Wohnung, durchkämmten die Räume und erklärten seiner Frau, sie sei mit einem Terroristen verheiratet. Arbeitskollegen von ihm wurden parallel dazu während einer Geschäftsreise in die USA an der Grenze abgefangen und mehrere Stunden zu ihren Verbindungen zu Allami befragt.

Was war geschehen? Saad Allami ist Vertriebsmanager bei einem Telekommunikationsunternehmen – und er ist unbescholtener kanadischer Bürger marokkanischer Abstammung. Drei Tage vor der Festnahme wollte er seine Kollegen motivieren, die sich gerade auf dem Weg zu einer Verkaufsmesse in New York City machten. Allami sendete ihnen eine SMS hinterher, sie mögen mit ihrer Präsentation die Konkurrenz „wegblasen".

Die kanadische Polizei durchleuchtete den Manager erst nach der Festnahme gewissenhaft und stellte fest, dass der Terrorverdacht haltlos ist. Allami nutzte in seiner SMS das französische Wort „exploser". Die Echtzeit-Analyse des US-amerikanischen Auslandsgeheimdiensts konstruierte offensichtlich aus der marokkanischen Herkunft, der abgefangenen SMS mit dem Begriff „explodieren" und einer Truppe Einreisender als Empfänger der Nachricht eine Terrorwarnung.

Im Raster

Allami wurde zum zufälligen Opfer der US-amerikanischen Rasterfahndung modernster Ausprägung. Ein Rückblick: Um RAF-Terroristen schneller aufzuspüren, hatte in den 70ern der damalige Präsident des Bundeskriminalamts Horst Herold in seiner Verzweiflung erstmals zu dieser Ermittlungsmethode gegriffen. Das Prinzip: Behörden füttern Computer mit allen verfügbaren Daten über Bürger und suchen darin EDV-gestützt Merkmale, die auf das zuvor festgelegte kriminelle Verhaltensmuster hindeuten. Erreichen die Treffer einen Schwellenwert, schlägt das System Alarm – ein Verdacht ist hergeleitet, die Ermittlung läuft an.

Die Rasterfahndung steht seit jeher in der Kritik, weil sie ein rechtsstaatliches Grundprinzip untergräbt: die Unschuldsvermutung. Demzufolge soll der Staat Bürger erst dann ausforschen und gegen sie ermitteln dürfen, wenn er einen begründeten Verdacht auf kriminelle Taten hegt. Bei der Rasterfahndung geraten aber alle ins Visier. Schlimmstenfalls müssen sie ihr Verhalten möglichen Rasterkriterien anpassen, um nicht aufzufallen. Saad Allami hätte in seiner SMS an die Kollegen sicherlich den Begriff „exploser" gemieden, wenn er die Konsequenzen gekannt hätte.

Seit Anfang Juni dieses Jahres liefert Edward Snowden scheibchenweise Beweise dafür, dass der US-amerikanische Auslandsgeheimdienst bestrebt ist, möglichst jede digitale Kommunikation von Bürgern anderer Länder zu belauschen und auszuwerten. Insbesondere in Deutschland reagierten Politiker und Medien entsetzt. Dabei ist es – offensichtlich unter dem Radar der breiten Öffentlichkeit – seit Jahren kein Geheimnis mehr, mit welchen Methoden die NSA und Geheimdienste anderer westlicher Industrienationen vorgehen, um Massen von Informationen an sich zu reißen, zu sieben und auszuwerten.

Ohne Schranken

Ende der 90er Jahre forschten Journalisten unter anderem des Heise-Verlags das Echelon-Projekt aus, das die USA im Verbund mit Großbritannien, Kanada, Australien und Neuseeland bereits Anfang der 60er Jahre in die Wege geleitet hatten. 2001 belegte ein Untersuchungsbericht des Europäischen Parlaments, dass die NSA mit Echelon Telefonate, Mails und sonstige Kommunikation großflächig belauscht hatte.

Der Verdacht lautete damals übrigens, dass es nicht nur um präventive Terrorbekämpfung gegangen sei, sondern wesentlich auch um das Ausspähen von Know-how ausländischer Unternehmen, also um Wirtschaftsspionage. Der Echelon-Skandal geriet weitgehend in Vergessenheit, weil kurz nach den Enthüllungen die Anschläge vom 11. September 2001 die Arbeit der Auslandsgeheimdienste in ganz anderem Licht erscheinen ließen.

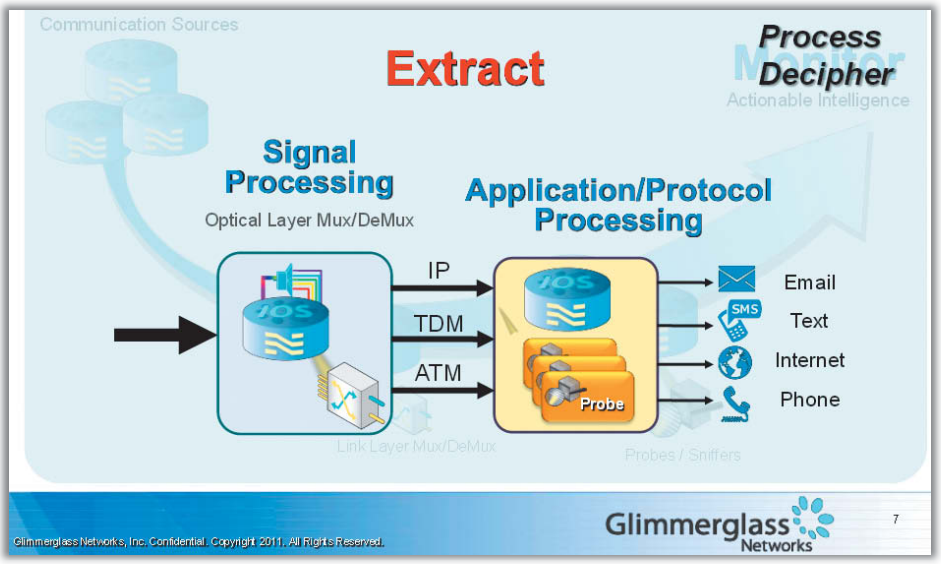
Die Vereinigten Staaten reagierten auf die Anschläge mit dem „Patriot Act". Das Gesetz erweiterte die Befugnisse von FBI, CIA und NSA zur „lawful interception", also zur präventiven Telefon- oder Internetüberwachung erheblich und setzte den Richtervorbehalt in Teilen außer Kraft. In Zusammenhang mit der Ermächtigung zur Auslandsüberwachung („Foreign Intelligence Surveillance Act", FISA) aus dem Jahre 1978 hatten die Geheimdienste nun völlig freie Hand beim Belauschen des weltweiten Telefon- und Datenverkehrs. Sowohl der Patriot Act als auch FISA gelten nach Verlängerungen auch heute noch.

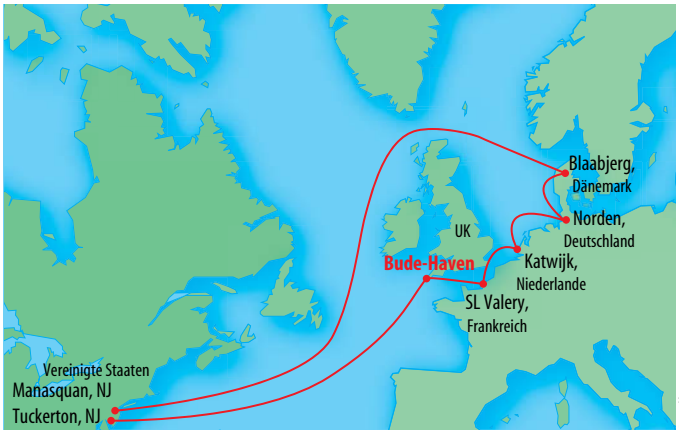
Glasfaser-Angriffe

Edward Snowdens Aussagen, die NSA könne über Abhör-Schnittstellen in Glasfaser-Backbones fast den gesamten weltweiten Internet-Datenverkehr belauschen, stießen in der Öffentlichkeit auf Skepsis. Es sei kaum denkbar, solche Datenmengen auszuleiten und zu speichern, hieß es allerorten. Dabei hatte bereits im Jahr 2006 ein Vorfall genau das enthüllt, was Snowden nun mit den veröffentlichten Geheimdokumenten erneut belegt: Die NSA nutzt den gegebenen Spielraum, um die US-Provider zur Kooperation zu zwingen und den Telefon- und Datenverkehr möglichst aller Menschen abzufangen und zu filtern.

Ein ehemaliger Techniker des US-Telekommunikationsriesen AT&T hatte damals nachgewiesen, dass das Unternehmen der NSA gestattete, sämtliche Telefongespräche

Der Hersteller Glimmerglass brüstet sich in einer Präsentation damit, Kommunikationsinhalte direkt an Glasfaser-Backbones abgreifen zu können.





An der Seekabel-Landestation Bude hat sich der britische Nachrichtendienst GCHQ in die US-europäische Kommunikationsschlagader, das Unterseekabel TAT-14, eingeklinkt.

und IP-Daten direkt an den Backbones auszuleiten. Dazu hatte die NSA nach Angaben des Technikers in einem geheimen Raum im AT&T-Datacenter San Francisco eine Abhörschnittstelle des Typs Narus STA 6400 installiert.

Das ehemals israelische Unternehmen Narus ist auf den Bau von Supercomputern spezialisiert, die für Geheimdienste sogar an 100-GBit-Glasfaser-Leitungen den Datenverkehr mitschneiden und nahezu in Echtzeit filtern können. Das neueste Produkt „Narus nSystem" bietet nach Angaben des Unternehmens eine Komplettlösung inklusive Data-Warehouse, Big-Data-Reduzierung und Forensik-Portal. Schon im Jahre 2004 war klar, dass Narus zum Zulieferer des US-amerikanischen Geheimdiensts avancierte – der ehemalige NSA-Direktor William Crowell wurde als Vorstand installiert. Seit 2010 gehört Narus zur Rüstungssparte des Boeing-Konzerns.

Als zweiter Zulieferer für Lauschaktionen an Glasfasern dürfte das wenig bekannte Unternehmen Glimmerglass fungieren. In einer nicht öffentlichen Präsentation warb das Unternehmen 2011 damit, dass seine Schnittstellen erfolgreich von US-Geheimdiensten eingesetzt werden. Glimmerglass „Cyber-Sweep" könne aus IP- und ATM-Datenströmen beispielsweise Gmail-Mails, Facebook-Daten oder Twitter-Tweets in Echtzeit extrahieren und speichern.

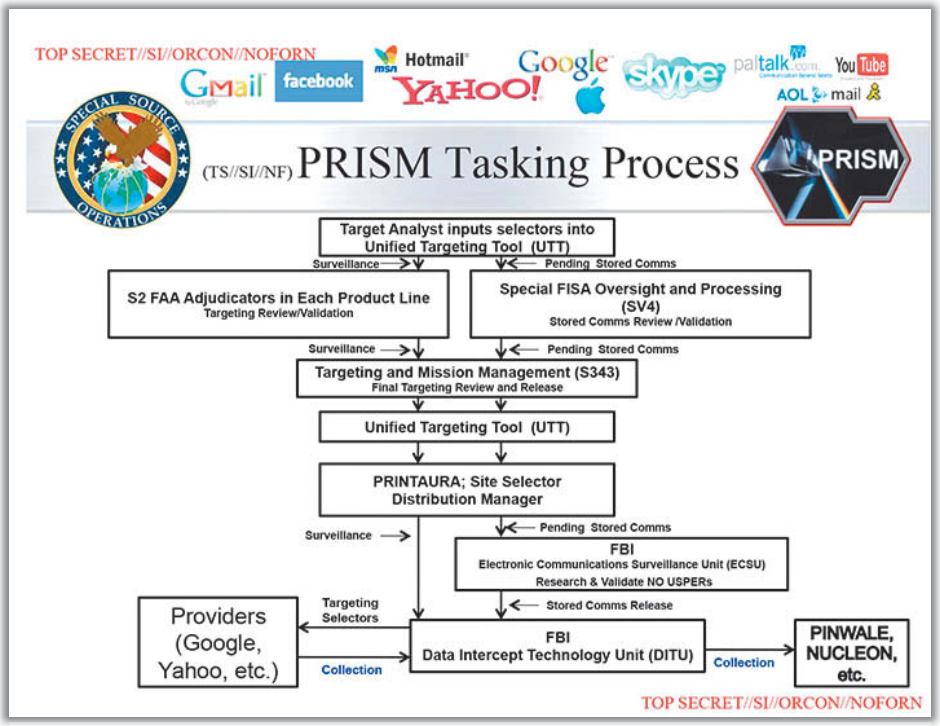
Im Interview mit der US-amerikanischen Aviation Week wurde Glimmerglass-Chef Robert Lundy 2010 zu einer möglichen Ausspäh-Aktion an den afghanischen Internet-Backbones befragt. Er antwortete: „Wenn man einmal die Wellenlängen auf der Glasfaser extrahiert hat, kann man dynamisch jene auswählen, die man abhören will – ohne anwesend zu sein. Wenn wir dort ein Operation Center errichten würden, könnten unsere Systeme dazu genutzt werden, im Land alle Glasfaser-Ein- und Ausgänge auszuspähen." Glimmerglass-Equipment werde bereits von Geheimdiensten dazu eingesetzt, Untersee-Glasfaserkabel anzuzapfen.

Die riesige Masse an Rohdaten speichert die NSA in verteilten, hochparallelisierten Datenbanken. Dazu hat sie ausgerechnet das Big-Table-Storage-Modell von Google um eine Rechteverwaltung weiterentwickelt. Die daraus entstandene Java-Software „Accumulo" hat sie im September 2012 sogar via Apache Foundation als Open-Source-Projekt bereitgestellt. Zur Analyse der Daten wendet die NSA das Java-Software-Framework Hadoop an, mit dem sich Analyseaufgaben auf Tausende Cluster-Knoten verteilen lassen. Doch der Datenberg, der zu einfach handhabbaren Graphen reduziert werden soll, wächst. Das stellt die NSA-Techniker vor große Herausforderungen, wie interne Präsentationen belegen.

Bislang analysiert die NSA alle gesammelten Daten in ihrem Hauptquartier, doch in Bluffdale/Utah entsteht derzeit ein riesiges Rechenzentrum, das den Nachrichtendienst in die Lage versetzen soll, Daten im Yottabyte-Bereich zu speichern und auszuwerten – ein Yottabyte entspricht einer Billion Terabytes (10^{24} Byte). Ein weiterer Schwerpunkt des zwei Milliarden US-Dollar teuren Komplexes soll in der Entschlüsselung kryptografischer Informationen liegen.

Riesiger Lauschangriff

Den von Edward Snowden veröffentlichten Dokumenten zufolge besteht die NSA-Auslandsüberwachung des Telefon- und Datenverkehrs aus mehreren Komponenten. An mehr als 100 Schnittstellen hat sich demnach der Geheimdienst in Glasfaserleitungen eingeklinkt, und das keineswegs nur in den USA. In Europa beispielsweise erhält die NSA Unterstützung vom britischen Nachrichtendienst Government Communications Headquarters (GCHQ). Aus den Dokumenten geht hervor, dass das GCHQ unter anderem die meistgenutzte transatlantische Datenautobahn, das Unterseekabel TAT-14, angezapft hat (Projekt „Tempora"). Alle abgefangenen Inhaltsdaten sollen für drei Tage, die Verbindungsdaten sogar für 30 Tage gespeichert werden.



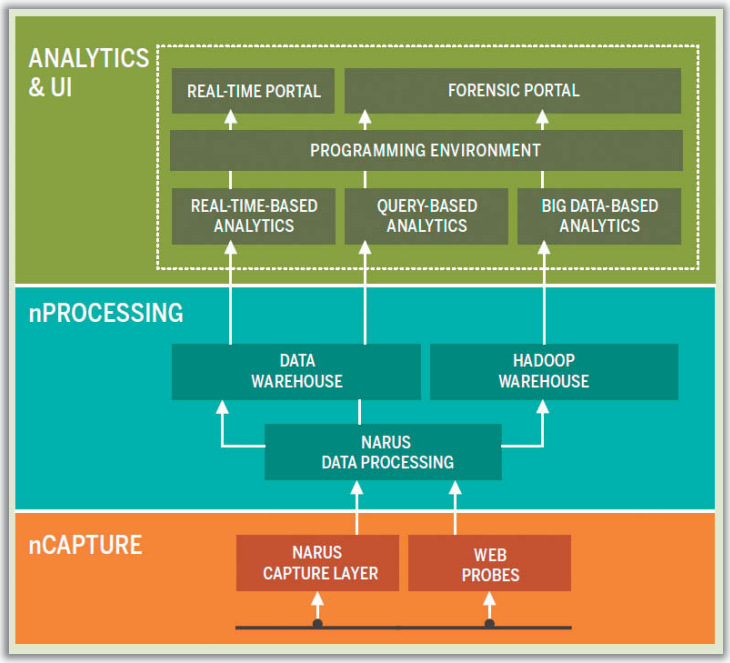
In einer streng geheimen Präsentation zeigte die NSA das Schema, nach dem die Abhörmaßnahmen des Auslandsgeheimdienstes bei Google, Facebook und Co. ablaufen.

Der Spiegel hatte Einblick in einen Teil der Snowden-Dokumente und daraus ersehen, dass die NSA auch an deutschen IP-Datendrehkreuzen „in West- und Süddeutschland“ lauscht. In Frankfurt habe die NSA „mit Wissen der Deutschen“ Zugang zu jenen Internet-Knotenpunkten, „die vor allem den Datenverkehr mit Ländern wie Mali oder Syrien regeln, aber auch mit Osteuropa“. Ob der deutsche Bundesnachrichtendienst (BND) direkt am Frankfurter De-Cix – also dort, wo die meisten Provider ihre Netze zusammenschalten – abhört, wie ebenfalls vom Spiegel kolportiert, wollte der De-Cix-Betreiber eco auf Anfrage von c’t nicht bestätigen oder dementieren – für derlei Fragen sei der BND zuständig, teilte man uns mit.

Deutschland steht offenbar mehr als andere westliche Staaten im Fokus der NSA. Snowdens Dokumente belegen laut Spiegel, dass der US-Auslandsnachrichtendienst an „normalen Tagen“ bis zu 20 Millionen Telefonverbindungen und um die 10 Millionen Internetdatensätze hierzulande sammelt. An Spitzentagen wie dem 7. Januar 2013 habe der Geheimdienst rund 60 Millionen Telefonverbindungen aufgezeichnet. Allerdings, und das geht in der Berichterstattung oft unter, beschränkt sich die NSA dabei den Dokumenten zufolge auf Verbindungsdaten, also die sogenannten „Metadaten“. Dabei geht es darum, wer mit wem wie lange gesprochen hat, nicht um den Inhalt des Gesprächs. Analog bedeutet das beim Datenverkehr: Wer hat wann und wie lange diese oder jene Webseite angesehen, wer hat mit wem gemailt, gechattet oder per Skype konferiert?

Details zum Prism-Projekt zeigen aber, dass die NSA eine jährlich erneuerte Pauschalvollmacht hält, um bei Unternehmen wie Facebook, Google, Yahoo, Microsoft oder Apple nahezu in Echtzeit Inhalte anzufordern. Generiert die Keyword-Suche einen Raster-Treffer, dürfen NSA-Mitarbeiter über das Prism-Portal eine Live-Überwachung von Personen starten: Die Unternehmen leiten dann über eine von der Bundespolizei FBI installierte Schnittstelle sämtliche Aktivitäten der Zielperson an Prism weiter. Außerdem können „Case Notifications“ an die NSA-Analysten verschickt werden, wenn sich eine überwachte Person in einen der Dienste einloggt, eine E-Mail verschickt oder einen Voice- und Videochat startet oder beendet. Den Prism-Enthüllungen nach standen Anfang April 117 675 Menschen weltweit unter Echtzeit-Überwachung der NSA.

Narus bietet für Geheimdienste eine Komplettlösung zum Belauschen von Glasfaser-Backbones, wie diese Abbildung aus einer Werbebroschüre des Unternehmens verdeutlicht.



Kontrollierte Überwachung

Von derlei allumfassenden Überwachungstechniken ist der bundesdeutsche Auslandsgeheimdienst weit entfernt. Der in Pullach bei München ansässige BND beschränkt sich derzeit nach eigenen Angaben im Rahmen der sogenannten „strategischen Fernmeldeaufklärung“ auf das Abfangen von Telefonaten und Mails, die die Landesgrenze überqueren. Dazu betreibt er bei Providern „Auslandskopfüberwachung“, lauscht also mit einem Schlüsselwort-Filter an den Servern und Leitungen.

Die Aktivität des BND wird – anders, als es in den USA üblich ist – laufend kontrolliert, und zwar von einem parlamentarischen Kontrollgremium (PKG). Der letzte Bericht des PKG legte Zahlen aus dem Jahr 2010 offen. Demzufolge umfasste die Schlüsselwort-Liste damals 16 400 Begriffe, wobei allein 13 000 davon explizit auf den Waffenhandel zielten. 2010 wurden 37 Millionen Mails und Telefonate maschinell ausgewertet, wobei 90 Prozent davon Spam-Mails waren. Nach PKG-Bericht enthielten lediglich 213 davon verwertbare Hinweise, die zu einem Anfangsverdacht führten. Insgesamt darf der BND gemäß G10-Gesetz höchstens 20 Prozent der Übertragungskapazität ins Ausland dauerhaft belauschen, nach Aussagen aus dem PKG sind es momentan etwa 5 Prozent.

Im deutschen Inland geht die größere Gefahr für die Privatsphäre der Bürger von Ermittlungsbeamten aus, die bei strafrechtlichen Verdachtsfällen die zur Verfügung stehenden Mittel über Gebühr anwenden. Dies reicht von der Auswertung der omnipräsenten Überwachungskameras bis hin zur Funkzellenabfrage. Nur in besonders krassen Fällen geraten derlei Maßnahmen an die Öffentlichkeit. Ende 2009 etwa haben Polizei und Staatsanwaltschaft die „Erfassung und Übermittlung sämtlicher Verkehrsdaten und Verbindungsdaten“ eines Stadtgebiets bei allen vier Netzbetreibern angefordert und bekommen – wegen versuchter Pkw-Brandstiftung. Halb Friedrichshain wurde ohne Erfolg unter Generalverdacht gestellt und gerastert.

Diese Abfrage ist rückwirkend möglich, weil die Provider alle Verbindungs- und Funkzellendaten ihrer Kunden zu Abrechnungszwecken lange vorhalten. Vodafone etwa speichert die Standorte eingeloggter Mobiltelefone satte 210 Tage lang, die Telekom immerhin für 30 Tage. So existiert de facto eine Vorratsdatenspeicherung im Mobilfunkbereich, obwohl das Bundesverfassungsgericht derlei langen Speicherfristen mehr als skeptisch gegenübersteht.

Die Telekommunikations-Überwachungsverordnung (TKÜV) gestattet es Ermittlern bei Verdacht auf schwere Straftaten gemäß Paragraf 100a Strafgesetzbuch außerdem, eine Live-Mail-Überwachung zu starten. Bei jedem Provider, der mehr als 9999 Konten verwaltet, steht dafür eine Schnittstelle bereit. Meist handelt es sich um die sogenannte SINA-Box, die verschlüsselt eine „IP-gestützte Übermittlung der Kopien zur berechtigten Stelle“ ermöglicht. Der Kunde muss von einer solchen Überwachungsmaßnahme nicht informiert werden.

Wer nun meint, einer solchen Überwachung mit Verschlüsselung entgehen zu können, unterschätzt die Möglichkeiten der Ermittler. Seit 2010 ist bekannt, dass hierzulande auch die sogenannte „Quellen-TKÜV“ zum Einsatz kommt, also das Belauschen von Verdächtigen direkt an ihrem Endgerät. Auf diese Weise haben Behörden bereits verschlüsselte Skype-Telefonate mitgehört und Mails nach der Entschlüsselung am PC abgefangen.

In einem geheimen Prospekt beschreibt das Unternehmen Gammagroup Fähigkeiten des Staatstrojaners FinFisher. Das BKA hat jüngst zehn Lizenzen der Software eingekauft.

Feature Overview

Target Computer – Example Features:

- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communication** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communication using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

For a full feature list please refer to the Product Specifications.

WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION

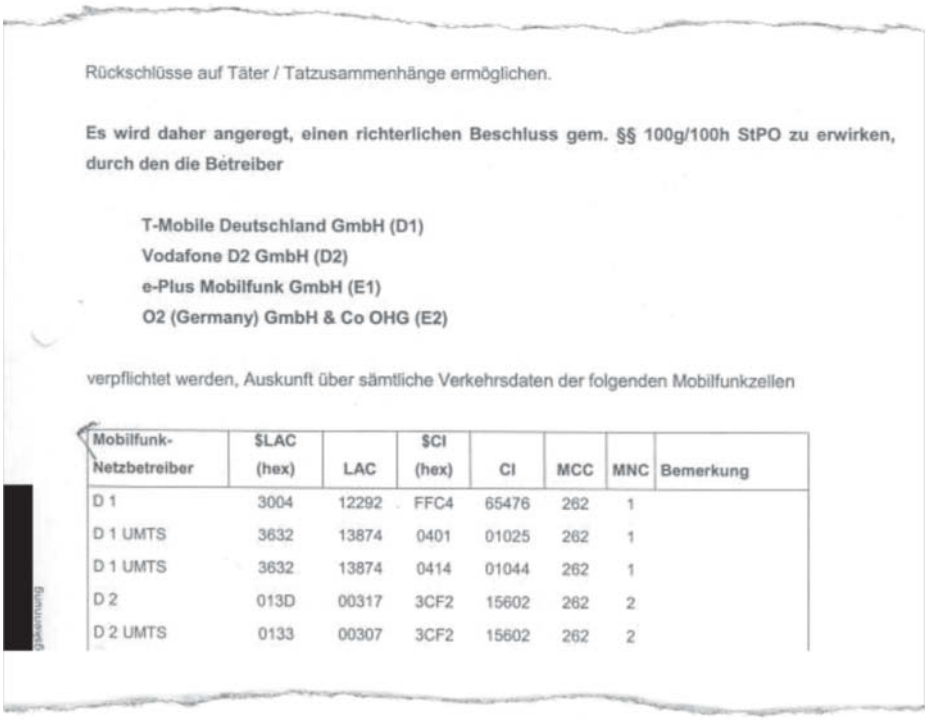
Aus geheimen Papieren des Innenministeriums geht hervor, dass das „Kompetenzzentrum Informationstechnische Überwachung" im Bundeskriminalamt (BKA) derzeit für eine umfassendere Quellen-TKÜV kräftig aufrüstet: 147 000 Euro kosteten Anfang 2013 zehn Lizenzen des Staatstrojaners FinFisher von Gamma/Elaman, der Ermittlungsbehörden vollen Zugriff auf Kamera, Mikrofon und den gesamten Datenverkehr des Nutzers ermöglicht und von dem außerdem eine Variante fürs Smartphone-Betriebssystem Android existiert. Setzt das BKA FinFisher wirklich ein, hilft in Verdacht Geratenen auch keine Verschlüsselung mehr.

Clouds im Fokus

Sowohl Privatleute als auch Unternehmen stehen seit den Snowden-Enthüllungen US-amerikanischen Cloud-Services argwöhnisch gegenüber. Die einen befürchten die Erosion ihrer Privatsphäre, die anderen sorgen sich um die Vertraulichkeit ihrer Betriebsgeheimnisse. Ein weit verbreiteter Tipp lautet daher derzeit, auf Clouds auszuweichen, die in Europa beheimatet sind und auf hiesiger Rechtsgrundlage betrieben werden. Abgesehen davon, dass auch der Zugriff auf deutsche Server nicht zwingend ausschließlich über deutsche Leitungen geroutet wird und am Netz belauscht werden kann, sind die Clouds aber längst ins Visier europäischer Überwachungsbestrebungen geraten.

Das European Telecommunications Standards Institute (ETSI), ein Zusammenschluss von europäischen Unternehmen und Forschungseinrichtungen, arbeitet zurzeit an einem Projekt namens „Lawful Interception – Cloud/Virtual Services". Man plant eine Schnittstelle, um Sicherheitsbehörden im Rahmen der jeweiligen Gesetze die Überwachung von Cloud-Kommunikationsdaten in Echtzeit zu ermöglichen. Die Anbieter sollen ein eigenes API für Ermittler bereitstellen. Außerdem setzt man auf Deep Packet Inspection direkt an den Servern. In Deutschland eruieren parallel dazu Bundespolizei, BKA und Verfassungsschutz im Strategie- und Forschungszentrum Telekommunikation (SFZ TK) bei Berlin Zugriffsmöglichkeiten auf deutsche Cloud-Dienste.

Unabhängig von den angestrebten neuen Inlands-Überwachungstechniken zur Strafverfolgung: Es steht fest, dass der BND als Auslandsgeheimdienst über die Zusammenarbeit mit Diensten anderer Länder eine Menge Abhörprotokolle zu deutschen Bürgern erhält. Insbesondere rühmt man sich des Austauschs mit der NSA und leistet willfährig Unterstützung. Und so entsteht eine absurde Aushöhlung der Rechtsstaatsprinzipien. Alle Nachrichtendienste der westlichen Industriestaaten dürfen nur im Ausland lauschen, ihre Ergebnisse aber bilateral austauschen – so wird jeder Bürger weltweit zum überwachbaren Ausländer. (hob)



Rückschlüsse auf Täter / Tatzusammenhänge ermöglichen.

Es wird daher angeregt, einen richterlichen Beschluss gem. §§ 100g/100h StPO zu erwirken, durch den die Betreiber

T-Mobile Deutschland GmbH (D1)
Vodafone D2 GmbH (D2)
e-Plus Mobilfunk GmbH (E1)
O2 (Germany) GmbH & Co OHG (E2)

verpflichtet werden, Auskunft über sämtliche Verkehrsdaten der folgenden Mobilfunkzellen

Mobilfunk-Netzbetreiber	$LAC (hex)	LAC	$CI (hex)	CI	MCC	MNC	Bemerkung
D 1	3004	12292	FFC4	65476	262	1	
D 1 UMTS	3632	13874	0401	01025	262	1	
D 1 UMTS	3632	13874	0414	01044	262	1	
D 2	013D	00317	3CF2	15602	262	2	
D 2 UMTS	0133	00307	3CF2	15602	262	2	

Wegen versuchter Brandstiftung erwirkten Berliner Ermittlungsbehörden die Herausgabe von Funkzellendaten bei den deutschen Providern.

Literatur

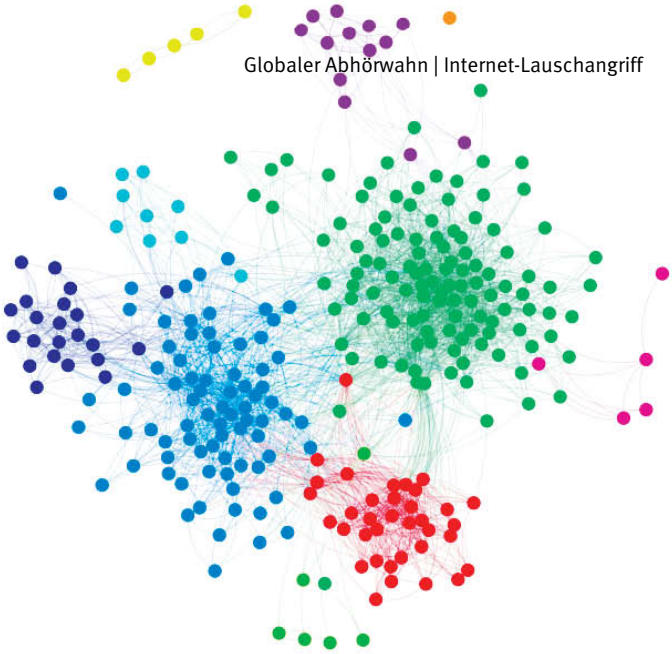
[1] c't Dossier: Raus aus der Cloud-Falle, http://heise.de/-1897895

www.ct.de/cs1303008

Holger Bleich, Sebastian Mondial

Prism yourself

Verbindungsdaten sind für Lauscher eine wahre Goldgrube. Aus ihnen lassen sich Schlüsse über soziale Gruppen, Lebensgewohnheiten oder Interessen ziehen. Das glauben Sie nicht? Dann testen Sie es mit Ihren eigenen Daten – eine Reihe von Tools macht es möglich.



Das Tool NameGenWeb sortiert das eigene Facebook-Netzwerk, gliedert es in Gruppen und stellt soziale Mittelpunkte heraus.

Die NSA-Datensauger suchen nicht die Nadel – sie holen sich gleich den ganzen Heuhaufen. Sie horten Metadaten, also zum Beispiel, wer wann eine Mail wohin geschickt hat. Damit wird es möglich, die Verbindungen zwischen den Halmen zu finden – dann, so das Kalkül der NSA-Techniker, ist die Nadel auch auffindbar.

Welche Erkenntnisse die Analyse von Metadaten liefert, kann jeder mit frei verfügbarer Software selbst ausprobieren. Für fundierte Aussagen über Netzwerke muss man nur ausreichend viele Daten haben und den thematischen Kontext kennen, was direkt zur weltweit größten sozialen Plattform Facebook führt.

Facebook

Facebook sammelt von über einer Milliarde Nutzern mit deren Einverständnis unermesslich viele Daten. Freiwillig geben die Mitglieder über Mail-Adressbücher ihre Kontakte bekannt, laden Bilder mit Ortsinformationen hoch und erzeugen detaillierte Profile mit teils sehr intimen Angaben. Schon die neue Facebook-Graph-Suche deutet an, wie umfangreich die Datensammlung ist: Wer von meinen Freunden ist eigentlich offen schwul? Facebook nennt das in der englischen Graph-Suche in „My male friends interested in men“ um und spuckt alle Freunde aus, die diese Informationen innerhalb von Facebook preisgeben.

Mehrere Werkzeuge ermöglichen es, die Daten des eigenen Netzwerks zu analysieren. **NameGenWeb** etwa ist eine Facebook-App, die nach Datenfreigabe das eigene Beziehungsnetzwerk anzeigt. Im abgebildeten Beispiel sehen Sie, wie NameGenWeb die einzelnen sozialen Gruppen der Testperson erkennt – und das sehr genau. Schulfreunde haben eine andere Farbe als Mitstudierende aus der Uni-Zeit, die Kollegen aus der alten Firma unterscheiden sich von denen am neuen Arbeitsplatz.

Geht man nun davon aus, dass die NSA alle Daten bei Facebook einsehen kann, liegen alle Verbindungen zwischen Mitgliedern offen vor ihr. Die Verknüpfung erfolgt über die Adressbücher, die vor allem Neulinge gerne einfach mal hochladen, um einfacher Bekannte zu finden. Stand man selbst in solch einem Adressbuch, kann die Facebook-Datenbank Verbindungen aufzeigen, obwohl man dort gar kein Konto hat.

Twitter

Die Vernetzung bei Twitter ist loser als bei Facebook. Mit dem gegen- oder einseitigen Folgen und mit dem Versand privater Nachrichten spannen die Nutzer aber auch hier Netzwerke auf. Hinzu kommen Metadaten, etwa der Aufenthaltsort sowie das Gerät beim Versenden von Tweets, sofern diese Einstellungen aktiviert sind.

Die Website **Mentionmap** zeigt Twitter-Nutzern nach Autorisierung an, welche öffentlichen Twitter-Konten sich gegenseitig erwähnen. Die Netzwerkdarstellung bietet nur einen Schlüssellochblick – große, komplexe Netzwerke kann sie nicht darstellen. Bei der Testperson wurde immerhin sichtbar, welche Nutzer häufiger ihre Nachrichten retweeten.

Mit der kostenlosen Erweiterung **NodeXL** kann man Office ab Version 2007 zur Analyse von Verbindungen von Twitter-Nutzern erweitern. Sofern die Follower öffentlich sind, stellt die Software Netzwerke übersichtlich dar. Allerdings funkt das sogenannte „Rate-Limit“ von Twitter dazwischen: Über das API darf NodeXL nur eine geringe Anzahl von Anfragen pro Stunde senden, und so können Darstellungen mit etwa 250 Followern schon einige Stunden dauern. Ein Nachteil, den die NSA nicht hat – für sie gelten keine API-Schranken.

E-Mail

Selbst wenn der Inhalt von Mails verschlüsselt ist, lassen sich die Metadaten – also Empfänger, Absender, Zeit und Betreff – einfach lesen respektive abhören. Sie befinden sich im Header der E-Mail immer im Klartext. Damit entsteht für Lauscher ein gutes Bild der Vernetzung und Lebensgewohnheiten, etwa zu den Arbeits-, Frei- und Ruhezeiten.

Um mal eben das eigene Archiv nach Inhalten und Meta-Informationen zu durchstöbern, eignet sich das Werkzeug **MUSE**. Es ist Ausfluss eines aktiven Forschungsprojekts des Mobisocial Laboratory an der Stanford University. Seit 2012 bietet die Java-Software die Möglichkeit, große mbox-Mail-Archive zu analysieren, wie sie etwa Thunderbird anlegt. Dies geschieht auf dem eigenen PC, es werden keine Daten nach außen übertragen.

Speziell für den Mail-Account von Google haben Forscher des Massachusetts Institute of Technology die Analyse-Software **Immersion** entwickelt. Geben Sie ihr Zugriff auf Ihr GMail-Konto, untersucht sie die „From“, „To“, „Cc“ und „Timestamp“-Header aller Mails. Die Macher bezeichnen ihre Analyse-Grafiken als „kubistische Gemälde“, die verschiedene Perspektiven auf die Metadaten ermöglichen. Beispielsweise verdeutlichen sie, wer einen über wen bekanntgemacht hat oder mit wem Sie in bestimmten Zeiten bevorzugt Mails austauschen. (hob) *ct*

www.ct.de/cs1303013

Axel Kossel, Andreas Stiller, Jürgen Schmidt

Gegen die Totalüberwachung

Wer sich vor der gigantischen Datensammelei von NSA & Co. schützen will, kann auf eine ganze Reihe von Techniken und Tools zurückgreifen. Doch nur wer weiß, was wovor schützt, kann seine Privatsphäre effizient verteidigen.

Die jetzt bekannt gewordenen Details zu PRISM zeigen, dass die NSA zwei Arten von Daten sammelt: zum einen fischen sie im großen Stil Meta-Daten ab: „Wer spricht mit wem und wie oft?“ Dabei handelt es sich um viele Milliarden Datensätze; das Ziel ist quasi die komplette Weltbevölkerung. Zum Zweiten sammeln sie von einer limitierten Zahl von Nicht-Amerikanern – die Rede ist von etwas über 100 000 – Klartext-Informationen ein.

Im wesentlichen gibt es zwei Ansätze, der Schnüffelei zu entgehen: Anonymisierung und Verschlüsselung. Das ist aber kein Entweder-oder; wirklich effizient funktioniert das nur, wenn man es richtig kombiniert.

Anonym im Netz

Bei der Anonymisierung gilt es, die eigene IP-Adresse zu verbergen. Anonymisierende Proxies oder VPN-Dienste, mit denen man beispielsweise Regionalsperren ausländischer Video-Portale umgehen kann [1], eignen sich wenig: Zu groß ist die Gefahr, dass diese zentralen Knoten besonders intensiv überwacht werden.

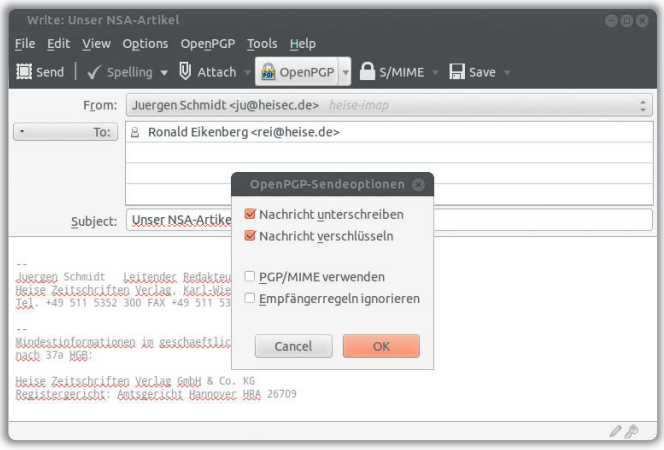
Besser sind dezentrale Dienste wie Tor und JonDonym (siehe Seite 120). Beide leiten die Daten, die bereits auf dem Client verschlüsselt werden, über mehrere Knoten, wovon der letzte (Exit) dann die entschlüsselten Daten zur Zieladresse schickt. Die Konzepte sind dabei etwas unterschiedlich, gemein ist beiden, dass jemand schon große Bereiche des Internet in verschiedenen Ländern lückenlos unter Kontrolle haben müsste, um zu wissen, wessen Daten wo rauskommen.

Allerdings kann man sich durch die falsche Nutzung von Tor sehr schnell ein regelrechtes Eigentor schießen. Das liegt am Konzept, das zwar versucht Anonymität zu gewährleisten, die Sicherheit der übertragenen Daten jedoch weitgehend dem Anwender überlässt. So kommt bei einem Tor-Exit-Knoten der gesamte Internet-Verkehr des Anwenders als Klartext vorbei, den dieser nicht speziell verschlüsselt hat. Das prädestiniert diese Position natürlich geradezu für Schnüffeleien aller Art.

Weil Tor von Freiwilligen in aller Welt betrieben wird, lässt sich das sehr leicht bewerkstelligen. So spähte Dan Egerstad 2007 auf seinem testweise aufgesetzten Tor-Exit-Knoten reihenweise E-Mail-Zugangsdaten von Botschaften und Behörden aus. Man darf getrost davon ausgehen, dass heute ein beträchtlicher Teil aller Tor-Exit-Knoten von Geheimdiensten mit genau diesem Ziel betrieben wird.

Neben dem passiven Lauschen kann man dort als Man-in-the-Middle dann nämlich auch gezielte Angriffe auf verschlüsselte Verbindungen fahren. Das Arsenal reicht vom Einsatz von Tools wie sslstrip, das Verweise auf verschlüsselte https-Seiten in solche auf reguläre http-Seiten ersetzt, bis hin zum Einsatz gefälschter Zertifikate.

Wer also Tor nutzt, muss äußerst penibel darauf achten, dass er ausschließlich verschlüsselte Verbindungen benutzt und bei jeder Zertifikatswarnung die Verbindung ab-



Mit der Enigmail-Erweiterung von Thunderbird kann man E-Mail via OpenPGP so verschlüsseln, dass sich auch Geheimdienste die Zähne daran ausbeißen.

bricht. Sicher ist das dann jedoch immer noch nicht, denn bei Verfolgern vom Kaliber der NSA muss man damit rechnen, dass sie auch scheinbar echte Zertifikate einsetzen. Die sind dann von CAs ausgestellt, denen der Browser vertraut und erzeugen somit keine Warnung im Browser. Wer Google, Microsoft und Apple in der Tasche hat, wird kaum vor Zertifikatsausstellern wie Versign zurückschrecken.

Etwas weniger kritisch ist die Situation bei JonDonym, dessen Mixbetreiber vom Betreiber JonDos des Netzes, der JonDos GmbH, ausgewählt und überprüft werden. Letztlich muss man sich aber auch hier auf die Integrität von Firmen verlassen, die sich im Zweifelsfall offiziellen Anfragen von Strafverfolgern und Nachrichtendiensten beugen müssen.

Nicht nur die Sicherheit, auch die Anonymität durch Dienste wie Tor und JonDonym ist fragil. Sie hängt ganz entscheidend davon ab, dass der Anwender konsequent auf jegliche Erweiterungen wie Flash, Java und so weiter verzichtet (siehe Seite 124). Pakete wie das Tor Browser Bundle und JonDoFox erleichtern das zwar; Spaß macht das dann aber nicht mehr.

Verschlüsselung

Auch die zweite Säule steht auf tönernen Füßen. Die Verschlüsselung vieler Dienste beruht auf SSL/TLS; etwa die von von https-Web-Seiten, gesicherten Verbindungen zu Mail-Servern und E-Mail-Verschlüsselung via S/MIME und vieles mehr. Doch dieses Konzept weist eine lange Liste von Schwachstellen auf, die von der verbreiteten Nutzung schwacher Implementierungen bis zum Einbruch bei der niederländischen Zertifizierungsstelle DigiNotar reicht.

Der Forscher Axel Ambak fasst das so zusammen: „Das SSL-System ist grundlegend defekt – und jemand muss es reparieren." Doch Ansätze wie das Pinning von Zertifikaten, wie es etwa das Microsoft Sicherheits-Tool EMET ermöglicht, sind weit davon entfernt, endanwendertauglichen Schutz vor Angriffen zu bieten.

Sehr guten Schutz auf höchstem Niveau bietet hingegen die E-Mail-Verschlüsselung mit GnuPG nach dem OpenPGP-Standard. Es handelt sich dabei um Open-Source-Software, die allgemein als sicher anerkannte Verfahren einsetzt und darüber hinaus von ausreichend vielen, renommierten Experten inspiziert wurde, sodass man dort keine Hintertüren befürchten muss.

Das Hauptproblem dabei ist, dass man natürlich den Kommunikationspartner ebenfalls von dessen Benutzung überzeugen muss. Und weil der Einsatz keineswegs trivial ist und selbst für Eingeweihte beträchtlichen Zusatzaufwand bedeutet, ist GnuPG zwar für Spezialfälle eine gute Lösung, aber leider noch nicht wirklich alltagstauglich. Unter anderem gibt es etwa immer noch keine komfortable und sichere Möglichkeit, PGP-Verschlüsselung auf Smartphones zu nutzen.

Auch das von c't immer wieder empfohlene Verschlüsselungs-Tool Truecrypt ist keineswegs über alle Zweifel erhaben – im Gegenteil. Das fängt damit an, dass man nicht so genau weiß, wer eigentlich dahintersteckt. Die Domain truecrypt.org war früher wenig vertrauenerweckend über die Adresse „Nava-Station Antarctica" gemeldet. Später war als Besitzer David Tresarik in Tschechien eingetragen und schließlich die „TrueCrypt Developers Association LC" in Henderson, Nevada, eine klassische Briefkastenfirma. Die – inzwischen abgelaufene – Signatur der aktuellen Windows-Version 7.1a durch Globalsign Objectsign CA und Verisign lautet auf die TrueCrypt Foundation.

Zwar wurde der Truecrypt-Quellcode unter anderem 2011 vom Ubuntu Privacy Remix Team genau analysiert und im Großen und Ganzen für okay befunden. Allerdings weiß man nicht so genau, ob die zum Download bereitgestellten, fertigen Programme wirklich mit diesem identisch sind oder unter Umständen kleine Erweiterungen für „Spezialaufgaben" beherbergen.

Die Empfehlung des Remix-Teams, vorsichtshalber mit selbst kompiliertem Code zu arbeiten, stellt sich trotz der beigelegten Visual-Studio-2008-Projekt-Dateien als überraschend schwierig heraus. Das Kompilieren eigener Windows-Binaries gelang uns nur mit beträchtlichem Aufwand. Und die dabei erstellten Programmdateien wiesen in allen Fällen Unterschiede zu den Download-Versionen auf, die sich nicht restlos klären ließen. Das muss nicht unbedingt etwas bedeuten – Vertrauen schafft das alles jedoch nicht.

Fazit

Trotz aller Zweifel gibt einem das Verschlüsseln etwa von E-Mails und der Einsatz von Anonymisierern wie Tor oder JonDonym ein ganzes Stück Privatsphäre zurück. Man muss dabei eben abwägen, wie weit man damit gehen will. Für den Normalsterblichen wird die auf Seite 154 vorgestellte E-Mail-Verschlüsselung via S/MIME durchaus ausreichen, auch wenn die NSA unter Umständen Mittel und Weg findet, die im Einzelfall auszutricksen.

Geheimdienste, die Waterboarding als legitimes Mittel der Wahrheitsfindung betrachten, sind ohnehin Gegenspieler, bei denen man ganz andere Faktoren mit berücksichtigen muss. Denn selbst eine unknackbare E-Mail-Verschlüsselung mit GnuPG, 4096-Bit-RSA und 20-stelligem Passwort hilft wenig, wenn jemand mit einer Pistole in der Hand nach dem Kennwort fragt. Aber das sind dann Einzelfälle, die nicht skalieren und sich nicht auf die großflächige Überwachung der gesamten Kommunikation im Internet erweitern lassen.

Gegen die drohende Totalüberwachung hilft Verschlüsselung und auch die Nutzung von Anonymisierungsdiensten sehr wohl. Die im Kasten zusammengestellten Artikel geben Ihnen das Wissen und konkrete, praxistaugliche Anleitungen an die Hand, mit denen Sie sich der Neugier der Geheimdienste weitgehend entziehen und der NSA ein Schnippchen schlagen können. Darüber hinaus sind der grassierende Überwachungswahn und dessen Auswüchse wie PRISM vor allem ein politisches Problem, das man natürlich primär auch auf politischer Ebene bekämpfen muss. (ju)

Unsere Rezepte gegen den Abhörwahn

Ortung auf dem Smartphone verhindern	Seite 61
Öffentliches WLAN sicher nutzen	Seite 82
Dienste und Software zum **Verbergen der IP-Adresse**	Seite 120
Anonym surfen mit JonDonym	Seite 123
Tracking-Schutz im Browser	Seite 124
Vertrauenswürdige Kommunikation	Seite 150
Mail-Verschlüsselung auf dem Rechner und mobil	Seite 154
Daten auf **Online-Speichern** schützen	Seite 158

Literatur

[1] Holger Bleich, Axel Kossel, Ich sehe was, was du nicht siehst, Das Geoblocking von Video- und TV-Angeboten umgehen, c't 8/13, S. 126

www.ct.de/cs1303014

Jürgen Schmidt

Die neuen Tricks der Internet-Gauner

Erpressung mit gesperrten PCs, kommerzielle Exploit-Kits im Leasing-Modell und ein Phishing-Revival mit geklauten Adressdaten – über die folgenden Angriffe sollte man Bescheid wissen.

Der Schädling, den ich bei Hilferufen von Lesern oder Bekannten seit einiger Zeit am häufigsten vorfinde, ist der sogenannte BKA-Trojaner, der in vielen verschiedenen Varianten kursiert. Das heißt natürlich nicht, dass Online-Banking-Betrug mit Zeus oder SpyEye verschwunden wäre. Aber der BKA-Trojaner hat der einst weitverbreiteten Dummy-Antiviren-Software beim Geschäft mit der Angst den Rang abgelaufen.

Das Prinzip der neuen Scareware-Generation ist immer das gleiche: Es erscheint eine bildschirmfüllende Meldung, dass der Rechner gesperrt wurde. Als Absender der Nachricht firmieren BKA, Bundespolizei, BSI oder gerne auch die GVU oder Microsoft – Hauptsache, es strahlt irgendwie Autorität aus. Das unterstützen Insignien der Macht wie Bundesadler, Landesflagge oder Polizeiabzeichen. Eine Variante blendete sogar ein Echtzeitbild einer angeschlossenen Webcam ein. Sie sendete dabei jedoch gar keine Daten ins Netz – es geht allein um den Eindruck allgegenwärtiger Überwachung, der das Opfer einschüchtern soll. Offenbar mit Erfolg: „Ganz schön scary" meinte das hilfesuchende Opfer, als sie den Rechner präsentierte.

Die angezeigte Meldung beschuldigt den Anwender verschiedener Formen des Betrugs oder Missbrauchs. Offenbar experimentieren die Gauner dabei ein wenig. Manchmal kommt der Trojaner mit knallharten Anschuldigungen wie dem Besitz und der Verbreitung von Kinderpornografie. Andere Versionen spekulieren auf das schlechte Gewissen und fabulieren von Raubkopien, nichtlizenzierter Software und ähnlichen Dingen, bei denen der Betroffene nicht ganz ausschließen mag, dass so was auf seinem Rechner mal gefunden worden sein könnte.

Der Rechner wurde jedenfalls vorgeblich gesperrt, um „weiteren Missbrauch zu verhindern", „Beweise zu sichern" oder Ähnliches. Tatsächlich lässt sich Windows nicht mehr benutzen; je nach Trojaner-Variante funktionieren sogar Tricks wie der Aufruf des Task-Managers via Strg + Alt + Entf oder das Booten in den abgesicherten Modus nicht mehr.

Erpressung

Eines haben all diese Trojaner-Varianten gemein: Man kann sich angeblich loskaufen. Auch hier variiert der Wortlaut, das Prinzip bleibt jedoch immer gleich. Gegen eine Mahngebühr, ein Bußgeld oder eine Geldstrafe in Höhe von irgendetwas zwischen 50 und 250 Euro würden die Anschuldigungen fallen gelassen und der Rechner wieder freigeschaltet. Das Geld ist über eines der Internet-Bezahlverfahren Paysafecard, Ukash oder neuerdings auch MoneyPak zu transferieren.

Ein Trojaner bei der Arbeit: BKA, Bundespolizei, GVU oder Microsoft haben angeblich den Rechner gesperrt.

Die funktionieren so, dass man gegen Bezahlung Codes erwirbt, die einen bestimmten Geldwert repräsentieren – gängige Stückelungen sind 10, 20 und 50 Euro. Gibt man diese Codes weiter, kann der Empfänger damit anonym einkaufen gehen oder sich den Gegenwert vom Herausgeber wieder in echtem Geld auszahlen lassen. Was diese Internet-Währungen für Betrügereien besonders geeignet macht, ist die Tatsache, dass es einen sehr aktiven Untergrundmarkt gibt. So verscherbeln die Betrüger die ergaunerten Codes in größeren Stückzahlen zu einem Teil ihres Werts weiter. Strafverfolger, die das Geld zurückverfolgen, verzweifeln an unzähligen Zwischenstationen, die natürlich keine Ahnung haben, von wem sie ihre Codes erworben haben.

Die Hoffnung, dass nach einer Bezahlung der Rechner freigeschaltet wird, ist naiv. In der Realität ist das Geld futsch und der Rechner weiterhin verseucht. Trotzdem floriert das Geschäft. Andreas Buick von der Staatsanwaltschaft Göttingen, die für die Ermittlungen in dieser Erpressungsserie zuständig ist, erklärte gegenüber c't, dass bundesweit allein 2012 circa 20 000 Strafanzeigen eingegangen sind. „In etwa 2000 Fällen haben die Anzeigeerstatter den geforderten Geldbetrag gezahlt", resümiert der Staatsanwalt. Darüber hinaus sei von einer „hohen Dunkelziffer" auszugehen. Somit ist es wohl realistisch, von mehreren hunderttausend Opfern auszugehen – das Ganze ist also ein Millionengeschäft.

Ein interessanter Randaspekt ist die Tatsache, dass diese Fälle als Auslandsstraftaten gewertet werden, weil die Täter vermutlich im Ausland sitzen, und somit nicht in die polizeiliche Kriminalstatistik eingehen. Kein Wunder, dass Bundesinnenminister Friedrich Ende letzten Jahres erfreut eine rückläufige Zahl der Internet-Straftaten und eine „positive Gesamttendenz" bilanzierte.

Dabei ist längst nicht mehr von einem Einzeltäter oder auch nur einer einzelnen Tätergruppe auszugehen. Ermittler erklärten gegenüber c't, dass der Trojaner bereits als Bausatz im Untergrund gehandelt wird, der sich einfach anpassen lässt. So kommt das „Erfolgskonzept" auch international zum Einsatz, unter anderem in Spanien, Portugal und Frankreich. In den USA sah sich das FBI auch bereits genötigt, eine Warnung zu „Reveton" – so werden die BKA-Trojaner international bezeichnet – herauszugeben.

Innenleben

Anders als die verbreiteten Online-Banking-Trojaner wie SpyEye, Zeus und Sinowal, die mittlerweile auf einem sehr hohen technischen Niveau operieren, sind die meisten BKA-Trojaner recht simpel gestrickt. Die Installationsroutine trägt sie in einem der gängigen Autostart-Einträge von Windows ein; nicht selten kopiert sie dazu den Trojaner sogar nur in den Autostart-Ordner des gerade angemeldeten Anwenders. Eventuell deaktiviert sie dabei noch via Registry diverse Rettungsanker wie den Task Manager (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System DisableTaskMgr) oder den Registry Editor (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System DisableRegistryTools). Anschließend erscheint nach der Anmeldung oder manchmal auch erst beim Herstellen einer Internet-Verbindung der Sperrbildschirm.

Internet-Währungen wie Ukash und Paysafecard, mit denen man sich bei einigen Trojanern angeblich loskaufen kann, werden im Internet rege gehandelt und sind deshalb kaum zurückzuverfolgen.

Dieser einfache Aufbau macht es besonders schwer, neue Varianten zu erkennen. Da ist nicht viel, woran sich ein Virenwächter orientieren könnte: Ein Programm, das ein paar Registry-Einträge setzt und ein Meldungsfenster anzeigt – das trifft auf sehr viele Programme zu. Und so verwundert es kaum, dass sich die jeweils aktuellen Versionen immer wieder am Virenschutz vorbeimogeln können.

Dafür lässt sich der Trojaner vergleichsweise einfach aufspüren und deaktivieren. In der Regel genügt dazu etwa ein Desinfec't (siehe Seite 86), das von USB-Stick oder DVD ein Linux-System startet. Vor dort aus kann man das Schädlingsprogramm entfernen und anschließend Windows wieder starten. Beim Aufspüren der fraglichen Datei helfen hoffentlich die vier Virenscanner – wenn wenigstens einer der Hersteller bereits Signaturen für diese spezielle Variante bereitstellt. Wird bei einer neuen Variante keiner der vier fündig, muss man sich selbst auf die Suche machen und etwa die bekannten Autostart-Mechanismen checken.

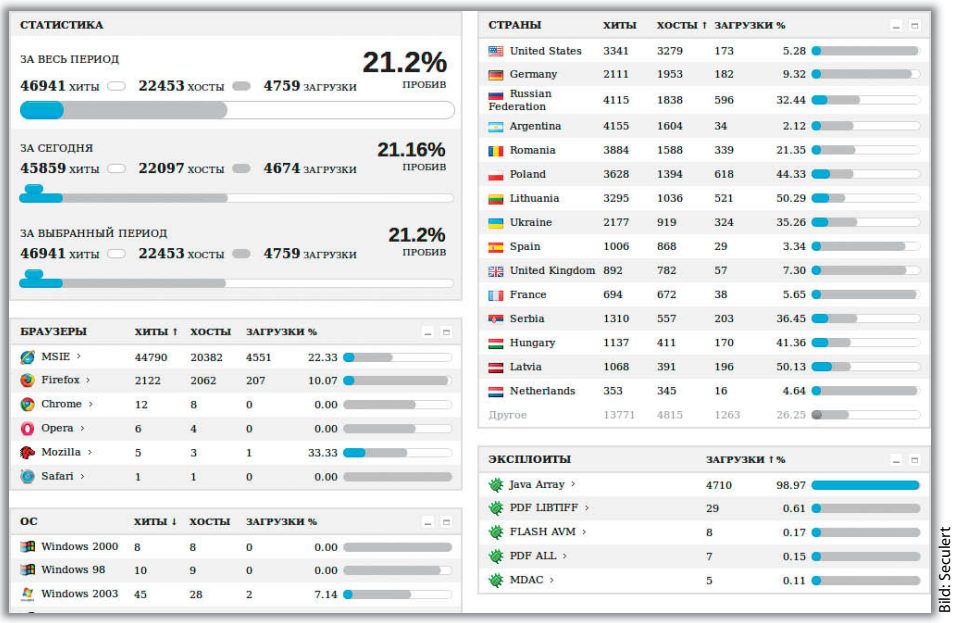
Den Trojaner zu deaktivieren ist jedoch nur der erste Schritt. Das System danach wieder richtig sauber zu bekommen ist die eigentliche Herausforderung – und die sollte man nicht auf die leichte Schulter nehmen. Denn es gibt tausend Dinge, die der Trojaner heimlich am System verbogen haben könnte. So gibt es Versionen, die ganz gezielt Sicherheitseinstellungen herabsetzen – vermutlich, um nach einer nachlässigen Reinigung eine spätere Neuinfektion zu erleichtern. Eine besonders heimtückische Variante ersetzt in der Registry den Eintrag für die Windows-Shell, die normalerweise auf den Windows Explorer zeigt. Entfernt man den Trojaner, findet Windows beim Start keine Shell und erzeugt einen Bluescreen. Der „Kaspersky Windows Unlocker" in den Experten-Tools von Desinfec't entdeckt diese Manipulation und macht sie wieder rückgängig.

Es gibt natürlich keine Garantie, dass über das gleiche Sicherheitsloch nicht auch schon andere Schädlinge ihren Weg auf den Rechner gefunden haben. Wer also auf Nummer sicher gehen will, bootet von einem sauberen System wie Desinfec't, bringt seine wichtigen Daten in Sicherheit und installiert danach Windows von Grund auf neu. Kommt das nicht in Frage, ist die beste Anlaufstelle für Hilfesuchende die Website www.bkatrojaner.de. Dort findet man über Screenshots konkrete Informationen zu vielen bekannten Versionen des Trojaners. In den angeschlossenen Foren des Anti-Botnet-Beratungszentrums geben kompetente Mitarbeiter auch konkrete Hilfestellung bei der Beseitigung.

Verbreitungswege

Der BKA-Trojaner verbreitet sich nach unseren Beobachtungen vor allem über Webseiten, die Sicherheitslücken in Systemen der Besucher ausnutzen. Das sind dann entweder kompromittierte Webserver, in deren Seiten etwa ein IFrame eingebettet wurde, das den Exploit lädt und damit das System infiziert. Oder die Schadsoftware wird über dubiose Werbenetze verteilt. Besonders gefährlich sind da Webseiten, die illegale oder zumindest anrüchige Inhalte kostenlos anbieten oder vermitteln. Die müssen ihre Einnahmen natürlich anderweitig erzielen und können es sich nicht leisten, dabei viele Fragen zu stellen.

In drei von vier Fällen fand ich in letzter Zeit auf infizierten Systemen Java-Versionen mit bekannten Sicherheitslücken vor – zum Teil fanden sich sogar noch Rückstände von Java-Exploits im Cache. Aber auch Flash und Adobe Reader sind beliebte Angriffsziele. Oft testen spezielle Frameworks verschiedene



Das Exploit-Toolkit Blackhole hat mehr als 20 Prozent der Besucher infiziert, einen Großteil davon via Java.

Bild: Seculert