Die Welt der Datenspione

Alle paar Tage liefert der ehemalige Geheimdienstmitarbeiter Edward Snowden neue Erkenntnisse über die Abhörmethoden der Geheimdienste von USA oder Großbritannien. Wir zeigen, wo die Daten fließen, wer wie mitliest und wo die Bits vom eigenen Computer aus eigentlich genau hinsteuern.

VON LALON SANDER (RECHERCHE) UND ULRIKE DORES UND PASCAL SOBOTTA (GRAFIK)

Die USA: NSA

Im Mittelpunkt des von dem IT-Spezialisten Edward Snowden aufgedeckten US-Überwachungsskandals steht die National Security Agency (NSA) mit Sitz in Fort Meade, Maryland. Der Geheimdienst wurde Anfang der 50er Jahre gegründet und horchte im Kalten Krieg die Sowjetunion aus.

Heute konzentriert sich die Behörde, geschützt von Elektrozäunen und bewaffneten Wachen, auf die Abwehr terroristischer Gefahren. Mit ihren Rechenzentren filtert und sammelt sie riesige Mengen an Daten. Insgesamt arbeiten derzeit zwischen 30.000 und 40.000 Menschen für die NSA.

Innerhalb der Agentur soll es Recherchen der Zeitschriften *Wired* und *Foreign Policy* zufolge eine noch geheimere Abteilung mit dem Namen „Tailored Access Operations" geben, die in ausländische Computernetzwerke eindringt. Laut *Wired* war es diese Abteilung die den Computervirus Stuxnet entwickelte, der iranische Atomanlagen zum Ziel hatte. *Foreign Policy* berichtet, dass sie sich seit 15 Jahren in chinesische Computernetzwerke einhackt. Während die NSA laut Gesetz ohne Gerichtsbeschluss nur die Kommunikation von Ausländern abhören darf, ist es immer wieder vorgekommen, dass auch US-Bürger überwacht wurden.

Seit 2005 wird die NSA von General Keith Alexander geführt. In den geleakten Dokumenten wird er mit folgenden Worten zitiert: „Warum können wir nicht alle Signale zu jeder Zeit sammeln?" Im Jahr 2014 will Alexander in den Ruhestand gehen.

Die Briten: GCHQ

In Großbritannien ist das Government Communications Headquarters (GCHQ) mit Hauptsitz in Cheltenham und 5.500 Mitarbeitern der für Ver- und Entschlüsselung und Telekommunikation zuständige Geheimdienst. Die Ursprünge des GCHQ liegen im Ersten Weltkrieg. Vor allem im Zweiten Weltkrieg spielten die Entschlüsselungstechniken, die dort entwickelt und angewandt wurden, eine große Rolle: Die damalige Vorgängerorganisation knackte damals die Verschlüsselungstechniken von Nazideutschland.

Heute ist das GCHQ vor allem mit der Erfassung und Auswertung von Daten und mit anderen technischen Spionagemethoden befasst. Schon wenige Tage vor der Enthüllung des breit angelegten Überwachungsprogramms „Tempora", brachte die britische Tageszeitung *Guardian* den Geheimdienst in Erklärungsnot. Demnach hatte das GCHQ bei zwei G-20-Treffen ranghohe Delegierte ausspioniert, indem es Smartphones gezielt hackte und die Diplomaten in eigens für die Spionage eingerichtete Internetcafés lotste.

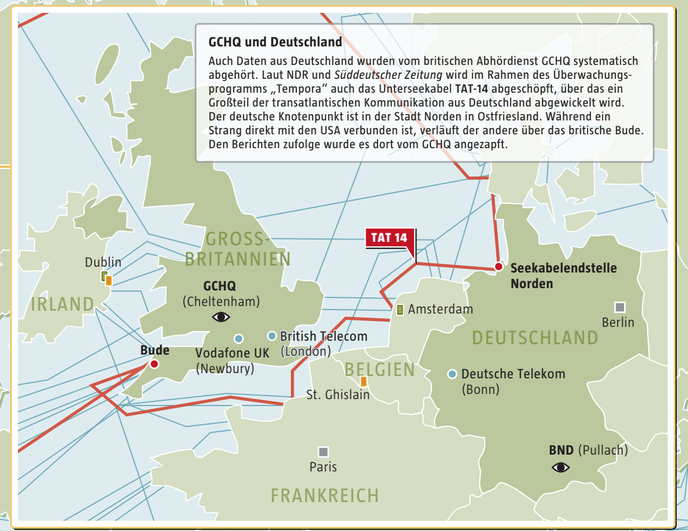
Die Deutschen: BND

In Deutschland überwacht der BND alle „internationalen Telekommunikationsbeziehungen", darunter auch E-Mails und Webforen. Sie werden nach mehr als 15.000 Stichwörtern gefiltert.

Im Jahr 2010 wurden so 37 Millionen Nachrichten gefiltert, von denen 209 „relevant" waren. Laut einem Bundestagsbericht wurde im Jahr darauf die Spamerkennung so weit verbessert, dass nur etwa 3 Millionen Nachrichten gefiltert wurden. Davon wurden 190 als „relevant" eingestuft.

GCHQ und Deutschland

Auch Daten aus Deutschland wurden vom britischen Abhördienst GCHQ systematisch abgehört. Laut NDR und *Süddeutscher Zeitung* wird im Rahmen des Überwachungsprogramms „Tempora" auch das Unterseekabel **TAT-14** abgeschöpft, über das ein Großteil der transatlantischen Kommunikation aus Deutschland abgewickelt wird. Der deutsche Knotenpunkt ist in der Stadt Norden in Ostfriesland. Während ein Strang direkt mit den USA verbunden ist, verläuft der andere über das britische Bude. Den Berichten zufolge wurde es dort vom GCHQ angezapft.



Prism

Das Programm:
Prism heißt ein Programm des US-Geheimdienstes NSA, mit dem offenbar die Internetnutzung von Menschen auf der ganzen Welt überwacht wird. Die Informationen werden dabei bei sieben der großen Internetfirmen eingesammelt: Microsoft, Yahoo, Google, Facebook, Skype, AOL, Apple und der weniger bekannte Chatservice Paltalk. Alle haben ihren Sitz in den USA, weshalb sich US-Behörden auch Zugriff verschaffen können.

Die Methode:
Unklar ist bisher, ob die Daten einfach direkt an den Servern der Unternehmen abgeschöpft oder erst nach Anfragen von ihnen freigegeben werden.
Die geleakten Dokumente legen die erste Variante nahe, sowohl die Firmen als auch die US-Regierung behaupten, die Daten würden erst nach Anfrage freigegeben.

Die Einschätzung:
Das muss allerdings nicht im Widerspruch stehen. So schreibt der amerikanische Journalist und Geheimdienst-Experte Marc Armbinder: Facebook könnte die Anordnung bekommen haben, Informationen über bestimmte Profile herauszurücken. Da diese Konten ständig aktualisiert würden, könnte die Firma eine Kopie ihres Servers erstellen, zu der nur die NSA Zugang hat. Die ausgewählten Profile würden dann in Echtzeit auch auf dem gespiegelten Server aktualisiert.

Der Umfang:
Ein Dokument zeigte, dass 97 Millionen Datenpunkte aus der ganzen Welt allein im März 2013 gesammelt wurden, die meisten aus dem Iran, aus Pakistan und Jordanien. Deutschland wurde ähnlich stark überwacht wie China, andere europäische Staaten weniger.

Die Aufklärung:
In den Tagen nach der Enthüllung berichteten die betroffenen Firmen von Zehntausenden Anfragen durch Behörden zu noch mehr Konten. Allerdings bezogen sich diese Zahlen auf alle Behörden und nicht allein auf die NSA. Facebook beispielsweise wies darauf hin, dass es sich bei den Anfragen auch um Fälle vermisster Kinder oder um Kriminalfälle handle.

Informationen aus Datenzentren von Internetfirmen werden abgefragt

Y! Google

Tempora

Das Programm:
Das Überwachungsprogramm Tempora wird vom britischen Abhördienst GCHQ betrieben. Statt Firmen zur Herausgabe von Daten zu bringen, hat er sich direkt an die Quelle gesetzt: 200 Glasfaserkabel, die – in Unterseekabel zusammengefasst – Daten über den Atlantik transportieren. Es ist eine der wichtigsten Internetverbindungen der Welt.
Jedes einzelne Kabel transportiert mehr als 1 Gigabyte pro Sekunde, also den gesamten Inhalt einer DVD in drei Sekunden – insgesamt schöpft GCHQ also den Inhalt von etwa 70 DVDs pro Sekunde ab.

Die Kabel:
Im Internet suchen sich Daten den schnellsten und billigsten Weg zu ihrem Ziel, nicht unbedingt den kürzesten. Da die Verbindungen zwischen Nordamerika und Europa die am besten ausgebauten sind, werden viele Daten über diesen Weg übermittelt. Zudem sind Südamerika und Afrika gar nicht verbunden, die Kommunikation läuft in der Regel auch über Nordamerika.

Die Server:
Zugleich stehen die Server der weltweit wichtigsten Unternehmen in den USA. Selbst wenn europäische Nutzer von Googlemail ihre Daten von einem europäischen Datenzentrum – in Finnland, Belgien oder Irland – abrufen, müssen diese mit den Datenzentren in den USA synchronisiert werden. Sie werden also trotzdem über den Atlantik geschickt, durch die Abhörstelle des GCHQ.

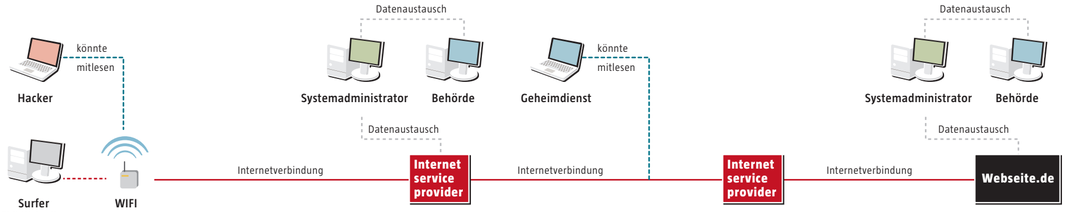
Der Umfang:
So werden Unmengen abgegriffen. „Das ist eine riesige Menge an Daten", heißt es dazu wörtlich in einem der geleakten Dokumente. Um zielgerichteter zu suchen, werden erst einmal Daten aus Peer-to-peer-Netzwerken herausgefiltert, meist Film- und Musikdateien getauscht werden. Damit reduziert sich der Datensatz um etwa 30 Prozent. Der Rest wird nach 70.000 Suchbegriffen durchsucht, darunter Namen, Telefonnummern und Mailadressen.

Legende

- weltweite Tiefseekabelverbindungen
- Datenzentren Facebook
- Datenzentren Google
- Datenzentren Yahoo
- Datenzentren Apple
- Datenzentren Microsoft

Fotos: dpa (BND), reuters (NSA, GCHQ)

Wie Behörden, Geheimdienste oder Hacker spionieren können



1. Wenn Nutzer im Netz E-Mails lesen – wie beispielsweise auf der Googlemail-Seite –, können fünf Informationen abgeschöpft werden: die angesurfte Website, die Logindaten, der Aufenthaltsort des Absenders, der Empfänger und der Inhalt einer Mail. Alle vier sind dem Nutzer bekannt, deshalb liegt hier die erste Schwachstelle: Mit Schadsoftware, die neben Netzkriminellen auch Geheimdienste nutzen, oder durch das Einfangen des WLAN-Verkehrs lassen sich diese Daten auslesen.
Schutz: Rechner gegen Schadsoftware schützen. WLAN mit einem WPA-Passwort verschlüsseln.

2. Beim eigenen Internetanbieter fließen die Daten, wenn sie nicht geschützt sind, unverschlüsselt durch die Knotenpunkte. Darunter alle fünf genannten Datenpunkte. Sie können vom Systemadministrator eingesehen werden. Auch Behörden wie die Polizei können sie mit Gerichtsbeschlüssen ganz legal anfordern.
Schutz: gesicherte Version von Websites nutzen. Statt HTTP://www.gmail.com HTTPS://www.gmail.com eingeben, die meisten wie etwa Gmail stellen automatisch darauf um.

3. Auch die Website, die angesurft wurde, hat einen Internetanbieter, bei dem dasselbe gilt wie nebenstehend. Ist dieser in den USA, haben US-Behörden ebenfalls Zugriff auf die Daten. Die letzte Schwachstelle ist allerdings der Betreiber der Website selbst: Googlemail hat natürlich auch alle Logindaten, Mail-Empfänger und -inhalte vorliegen und kann von Behörden zur Herausgabe gezwungen werden.
Schutz: E-Mails mit PGP auf dem eigenen Rechner verschlüsseln – selbst wenn Google die Mails rausgeben muss, liegen sie dann nur verschlüsselt vor.
Und: TOR benutzen, um den eigenen Aufenthaltsort zu verschleiern.
Link: torproject.org

Quelle: EFF/taz