Keine Sau

interessiert sich für mich?

Als ich kürzlich eine wichtige Email nicht mehr gefunden habe, hätte ich am liebsten bei der NSA nachgefragt: "Sehr geehrte Damen und Herren, ich habe vor vier Tagen eine sehr wichtige Mail von Hr. XY erhalten. Könnten Sie mir diese bitte noch einmal zustellen?" Ich hab's gelassen, bei den Herren weiß man ja nie.

Die NSA-Affäre rund um Edward Snowden wird zwar in den Medien vielfach behandelt, ein echter Aufreger ist das Thema dennoch nicht. Weil wir schon immer wussten, dass wir überwacht werden? Weil es uns egal ist? Oder weil eigentlich niemand mehr versteht, worum es geht?

Wer soll sich für meinen Mist interessieren, den ich so in die digitale Welt raushaue, meinen viele. Dabei wird in Wahrheit nicht nur unsere Kommunikation überwacht. Die deutschen Sicherheitsbehörden überwachen schon jetzt, was geht. Und es wird immer mehr. Bewegungsprofile gibt's sogar bald im Stadion:

„Bei Vorfällen könnten Fachleute künftig später jeden beliebigen Punkt des Innenraums aus der Gesamtaufnahme als perfekt scharfes Einzelbild herauszoomen", berichteten die Nürnberger Nachrichten im August 2013 über die seitens des 1. FC Nürnberg geplante neue Kameraüberwachung. Vermummung werde nichts mehr helfen, weil die ganze Spielzeit über gefilmt und aufgezeichnet werde. Totalüberwachung im Stadion - das schafft angeblich Sicherheit, meint die Zeitung.

Nun ja: In London soll ein Passant täglich von ca. 300 Videokameras aufgenommen werden, heißt es. Die Kriminalitätsrate aber ist ungebrochen hoch und London gilt als gefährlichste Großstadt Europas. Auch in Bayern wird bald alles und jeder gefilmt: 17.000 Kameras (private nicht mitgerechnet) sind ständig im Einsatz, wie die bayerische Staatsregierung im Februar mitteilte.

Bei mir jedenfalls ruft die Vorstellung, dass ich beim Stadionbesuch über 90 Minuten von einem Polizeibeamten herausgezoomt werden kann, wie ihm das gerade passt, alles andere als ein Sicherheitsgefühl hervor. Ohne Anlass darf er das zwar nicht. Können tut er es.

Und was bedeutet eigentlich „sicher"? Die Bayerische Staatsregierung hat dieser Tage angekündigt, für ein „sicheres Internet" einzutreten. Für mich ist das Internet sicher, wenn meine Kommunikation nicht abgefangen wird - sei es durch den Staat oder durch Virensoftware. Ob das der Staat auch mit „sicher" meint?

Die Dimensionen, die der NSA-Skandal aufzeigt, sind jedenfalls unerträglich. Yahoo bestätigte Zahlungen des US-Geheimdienstes an Internetfirmen. Diese werden also entlohnt, um ihre Technik den Geheimdienstanforderungen anzupassen. Unfassbar! In Anbetracht der Tatsache, dass ein riesiger Bereich der Email- und Internetverbindungen über die USA laufen, können wir getrost davon ausgehen, ebenfalls bestens überwacht zu werden.

Bei mir jedenfalls ruft die Vorstellung, dass ich beim Stadionbesuch über 90 Minuten von einem Polizeibeamten herausgezoomt werden kann, wie ihm das gerade passt, alles andere als ein Sicherheitsgefühl hervor. Ohne Anlass darf er das zwar nicht. Können tut er es.

Da hilft es auch wenig, wenn man davon ausgeht, die eigene Korrespondenz würde niemanden interessieren. Alleine die Vorstellung, welche Daten alle gespeichert werden können - und wohl auch werden, müsste eigentlich jeden zu Proteststürmen gegen dieses System anregen. Seit 2008 seien jedes Jahr tausendfach Datenschutzregeln seitens der NSA gebrochen worden, schreibt die Washington Post. Dabei seien auch „größere Mengen internationaler Daten, die Glasfaser-Kabel in den USA passiert hätten, vorläufig zur späteren Auswertung gespeichert worden", rügte das Geheimgericht der USA, das für die NSA zuständig ist.

Es geht also bei der NSA-Affaire nicht nur um das Filtern von Telekommunikationsfluss, sondern um Speichern. Der deutsche Geheimdienst tue das nicht, behauptet der Bundesinnenminister. Trotzdem sollen beim BND weitere 100 Millionen Euro in die technische Aufrüstung der Internetüberwachung gesteckt werden, meldete Spiegel-Online kürzlich. Ausgewertet werden Emails, Telefongespräche, Facebook-Konversationen oder auch Skype-Unterhaltungen.

Man braucht sich also nicht wundern, dass die Politik auf die NSA-Affäre nicht besonders leidenschaftlich reagiert. Fordern doch weite Kreise ebenfalls stärkere Überwachung. Weitgehend unbeachtet von der Öffentlichkeit beschloss der Bundestag im April 2013 eine Änderung des Telekommunikationsgesetzes und das mit gravierenden Folgen:

Die Bestandsdaten der Telekommunikationsanbieter können dadurch – weitgehend auch ohne richterliche Genehmigung - von Polizei und Geheimdiensten abgefragt werden. Bestandsdaten, das klingt harmlos. Ist es aber nicht! Dazu gehören auch die PUK des Handys, hinterlegte Passwörter, Dropbox-Daten, dynamische IP-Adressen. Und nicht einmal eine Straftat ist Voraussetzung für eine Anfrage der Polizei. Es genügt jetzt schon der Vorwurf einer Ordnungswidrigkeit oder Gründe der Gefahrenabwehr. Hier ist der Polizei Tür und Tor geöffnet. Man möchte sich gar nicht ausmalen, auf welche Ideen hier die Polizei künftig kommen kann. Die vom Bundesverfassungsgericht aufgehobene Vorratsdatenspeicherung* wird faktisch wieder eingeführt, nur eine Speicherfrist gibt es nicht mehr.

Die Folge aus alledem? Sorgsamer Umgang mit eigenen Daten, mit Internet und Mails und natürlich auch dem Handy ist wichtiger denn je. Aber das reicht nicht aus, wenn man bewusst abgehört, abgefragt und überwacht wird. Auf wundersame Weise ist die Verschlüsselung vollkommen aus der Mode gekommen. Wen wundert es? Weder Staat noch Wirtschaft haben daran ein Interesse. Der gläserne Bürger, der auch zu Werbezwecken nach allen Regeln der Überwachungskunst ausgeforscht werden kann, ist doch wunderbar. Wehren dagegen muss man sich leider selbst.

**Hintergrund: Das deutsche Bundesverfassungsgericht erklärte die deutschen Vorschriften zur Vorratsdatenspeicherung mit Urteil vom 2. März 2010 für verfassungswidrig und nichtig. Zur Begründung gab das Gericht an, dass das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und zudem die Hürden für staatliche Zugriffe auf die Daten zu niedrig seien. Die Regelung zur Vorratsdatenspeicherung verstoße laut Bundesverfassungsgericht gegen Art. 10 Abs. 1 Grundgesetz (GG).*
Interessant und schockierend ist es nun jedoch zu sehen, wie leicht mit der Änderung des Telekommunikationsgesetzes faktisch ein Entscheid vom BVerfG umgegangen werden wurde. Folgreichtig gibt es Bestrebungen gegen diese Änderung Verfassungsbeschwerde einzureichen. Ausführliche Informationen findet ihr auf

http://stopp-bda.de

NSA, Vorratsdatenspeicherung, Totalüberwachung im Stadion: Willkommen im Überwachungsstaat!

Email-Verschlüsselung

Das Prinzip

Ihr wollt nicht, dass jeder Staatsbüttel eure Mails mitliest? Dann wäre jetzt ein guter Zeitpunkt, endlich mal PGP zu benutzen. Damit könnt ihr schon seit achwasweißichwievielen Jahren eure Mails so verschlüsseln, dass kein Schlapphut mitlesen kann.
Das Prinzip der Mailverschlüsselung ist schnell erklärt. Jeder Teilnehmer hat 2 Schlüssel: einen privaten und einen öffentlichen. Der öffentliche wird an alle Leute gegeben, mit denen ihr kommuzieren wollt. Den privaten behaltet ihr immer nur für euch. Nie rausgeben. Klar?
Nehmen wir an, ihr wollt mit Berta verschlüsselt kommunizieren. Ihr gebt Berta euren öffentlichen Schlüssel, Berta gibt euch ihren öffentlichen Schlüssel. Nun könnt ihr Berta eine Mail schicken, die ihr mit Bertas öffentlichem Schlüssel abschließt.
Der Clou: Mails, die mit Bertas öffentlichem Schlüssel verschlüsselt wurden, können nur mit Bertas privatem Schlüssel wieder lesbar gemacht werden. Will Berta antworten, so verschlüsselt sie mit eurem öffentlichen Schlüssel, diese Mail ist nur mit eurem privaten Schlüssel zu öffnen. Das Ganze nennt sich Asymmetrische Kryptographie und wird bei Wikipedia nochmal mit anderen Worten erklärt.
Das Prinzip der öffentlichen und privaten Schlüssel setzt voraus, dass jeder Teilnehmer seinen privaten sowie die öffentlichen Schlüssel aller anderen Teilnehmer hat. Solche Schlüssel sind reine Textdateien und können prinzipiell per Mail verschickt werden. Sicherer ist aber natürlich eine persönliche Übergabe.

So gehts!

Die Einrichtung eines verschlüsselten Accounts würde hier den Rahmen sprengen, daher wollen wir lediglich auf zwei Links verweisen:

blog.ch-becker.de/2011/04/27/pgpgpg-unter-windows-mit-thunderbird-emails-verschlusseln

youtube.com/watch?v=ieuHHu4MoMo

Achtung!

Laut neuesten Medienberichten soll die NSA auch verschlüsselte Daten auslesen können. Das kann man natürlich nicht ausschließen, allerdings kann uns die NSA mal kreuzweise, hier soll es ja eher darum gehen, das heimische Schnittlauch etwas zu beschäftigen.

Sicher chatten, surfen, simsen...

Natürlich ist verschlüsseltes Mailen nur ein Teil sicherer Kommunikation. Aber auch chatten, surfen, simsen etc kann - weitesgehend - privat vollzogen werden. Dazu finden sich im Internet ebenfalls zahlreiche Tutorials, man muss jedoch etwas Zeit und Wille mitbringen, sich damit zu beschäftigen. Auch wenn man nichts zu verbergen hat, ist es mit Sicherheit ein besseres Gefühl, nicht ständig von Firmen oder Behörden beobachtet zu werden. Vielleicht können wir in einer der nächsten Ausgabe noch etwas ausführlicher zu diesen Themen berichten - notwendig wäre es!