Unter dem Radar der NSA

Zeit: Freitag, 27.9.2013, 11.00 Uhr
Ort: Hörsaal 0.19
Moderation: Rigo Wenning, Justitiar, W3C
Referenten: Erich Möchel, Journalist

Es war ein Paukenschlag als der Wistleblower Edward Snowden mit Hilfe des Guardian die generelle Überwachung des Internet durch die US- und die britische Regierung ans Licht der Öffentlichkeit brachte. Seitdem erfahren wir täglich neue Einzelheiten.

Es war schon vorher Einiges herausgekommen: 2005 hatte Joe Klein von AT in einer Zeugenaussage einen Abhörraum der NSA beschrieben. 2007 folgten Erkenntnisse über Abhörmaßnahmen bei Verizon. Nachdem Verizon die Schnittstellen lieferte, bekam die Firma eine große Anzahl Militäraufträge. Der Provider Qwest dagegen hatte sich gegen die Übergabe jedweder Kommunikation gesperrt und hat in der Folge alle Regierungsaufträge verloren. Der Vortrag ließ einführend eine kleine Historie der Vor-Skandale Revue passieren.

Bis heute weiß man nicht, wo überall die Schnittstellen liegen, an denen die Daten abgegriffen werden. Was Snowden schreibt entspricht also den Erwartungen. Die Methode bleibt immer ähnlich. An einem zentralen Knotenpunkt wird eine Schnittstelle installiert, wo der gesamte Traffic dupliziert wird. Die so kopierten Daten werden dann in ein Datencenter weitergeleitet und aufbereitet. Wie das genau passiert, hängt von den jeweiligen lokalen Gegebenheiten ab. Als Beispiel werden das Abhören von Unterseekabeln und die Schnittstelle am zentralen Knotenpunkt vorgestellt. Es wird an allen großen Internetknoten mitgehört. Ein direkter Zugang zu den großen amerikanischen IT-Unternehmen erlaubt unkontrolliertes oder vollständiges Abschöpfen jedweder Kommunikation in den Sozialen Netzwerken oder in den Webmail – Diensten.

Ist einmal klarer, was und wie abgehört wird, stellt sich die Frage nach Gegenmaßnahmen. Es werden Tipps und Tricks geboten, wie das Abgreifen von Information erschwert oder sogar unmöglich gemacht werden kann. Diese Tipps richten sich insbesondere an die Anwaltschaft, die ein vitales Interesse an privater Kommunikation hat.

Den Gerichten und dem Recht kommen nunmehr eine besondere Bedeutung zu. Denn die Abhörtätigkeit erschüttert die Demokratie und unsere Grundrechte im innersten Kern. Die ertappten Regierungen zeigen nicht etwa ein reumütiges Gesicht, sondern verdoppeln alle Anstrengungen Details zu verschleiern. Dazu wird zu oppressiven Maßnahmen gegriffen.

In seinem Vortrag erläuterte Referent Möchel wie NSA & GCHQ die Sicherheit im Netz systematisch unterminieren, warum Wirtschaftsspionage im Raum steht und wie man das Radar der Dienste mit einfachen Methoden unterfliegen kann. Er betonte, dass eine Entzauberung stattgefunden habe, deren Folgen erst nach und nach deutlich werden. Die NSA habe nicht nur ihre eigenen Methoden enttarnt, sondern die aller Geheimdienste. Das Wissen um die Methoden ist nicht mehr aus der Welt zu schaffen und die Suche nach den Schwachstellen habe gerade erst begonnen. Die Kryptografie wird weltweit hochgefahren und der Verdacht auf Wirtschaftsspionage erhärtet sich. Möchel stellte klar, dass nur gespeichert wurde, wer mit wem wann und wo kommuniziert habe. Eine Abhörung der Gespräche habe es nicht gegeben. Stimmprofile seien für die NSA interessanter als der Inhalt der Gespräche, Stimmprofile seien individueller als ein Fingerabdruck. Die NSA habe die Krypotgrafie nicht

geknackt und sei auch noch Lichtjahre davon entfernt. Es wurde immer nur auf die Verschlüsselung selbst geschaut, nicht jedoch auf die Umgebung der Verschlüsselung.

Möchel gab Tipps, um Gegenmaßnahme zu ergreifen. Mit dem Merksatz „Der Browser ist immer der Verräter“ empfahl er dringend mehrere Browser zu benutzen. Es würde auch schon helfen, Firefox mit gewissen Plugins aufzurüsten. Hinsichtlich der Browsernutzung solle man schizophren sein. Als Beispiel nannte er die Benutzung von Chrome nur für Google-Services, Kreditkarte nur bei Firefox, Facebook und Amazon nur mit Safari und Firmenaccounts und Online-Banking nur mit Internet-Explorer. Man müsse sich von der eigenen Bequemlichkeit verabschieden, um mehr Sicherheit zu erhalten. Die Gegenmaßnahmen müssten in einer gewissen Breite gesetzt werden. Es haben bisher nur Rasterfahndungen, aber keine Abhörung der Inhalte stattgefunden. Der Referent gab den Tipp, alte Handys mit neuer Pre-Paid-SIM-Karte zu benutzen oder alte Computer mit Linux zu reaktivieren.