Helmut Reimer, Christoph Wegener

Überwachung als Service?

Bereits in frühen Zeiten des Internets wurden die Möglichkeiten der asymmetrischen Kryptographie als Durchbruch für die Ende-zu-Ende-Verschlüsselung, den Integritätsschutz von Informationen und einer nachvollziehbaren Urheberschaft von Daten verstanden. Die notwendigen Services für die Namensvergabe und die Verwaltung und Verteilung der öffentlichen Teilnehmerschlüssel sollten – so die Vision – von hierarchisch geordneten „Trusted Third Parties (TTPs)" bereitgestellt werden. Die Begrifflichkeit der TTP erwies sich allerdings bald als idealistisch: Insbesondere konnte die Frage nach der Vertrauenswürdigkeit nicht abschließend beantwortet werden und außerdem fehlte ein Geschäftsmodell, denn alle TTP-Leistungen sollten altruistisch realisiert werden.

Aus dieser ursprünglichen Infrastrukturidee hat sich daraus in der Folge die Welt der Public Key Infrastructure (PKI) entwickelt. Ihre Services werden geschäftsmäßig angeboten, Vertrauen soll durch Aufwendungen für die notwendige physische sowie logistische Sicherheit gerechtfertigt sein und sie sind untereinander nicht Teil einer weltweiten Hierarchie.

Weil die PKI-Dienste heute ein wesentlicher Teil von elektronischen Geschäftsabläufen bei Finanztransaktionen, sowie in Verwaltungen und Unternehmen sind, gibt es inzwischen ein riesiges Paket von globalen Standards, nationalen gesetzlichen Regelungen und branchenorientierten Policies für ihre Leistungen. In Europa reicht diese Kette beispielsweise von der Signaturrichtlinie aus dem Jahre 1993[1] - mit den bekannten Folgen nationaler Regelungen in Europa – bis zur in Kürze erwarteten Europäischen eIDAS-Verordnung[2].

Das Dilemma der heute realen PKI-Landschaft besteht in ihrer Heterogenität. Verbunden damit sind mangelhafte Interoperabilität der Services und Intransparenz bei Sicherheitsqualitäten. Markante Beispiele für gravierende Sicherheitsmängel haben in den letzten Jahren zum Verlust des allgemeinen öffentlichen Vertrauens – auch in als gesetzeskonform und sicherheitsgeprüft eingestuften Infrastrukturdienstleister (z.B. DigiNotar und TürkTrust) – geführt.

Schon frühzeitig wurde erkannt, dass die im Zusammenhang mit einem PKI-Betrieb stehenden Daten attraktive Möglichkeiten für Internet-Angriffe und -Kriminalität und natürlich auch für eine gezielte Überwachung von Nutzeraktivitäten bieten. Bis heute sind die möglichen, dafür nutzbaren Schwachstellen der Sicherheitsarchitekturen der PKI und der Anwendungsumgebungen nicht bekannt.

Die Angriffspunkte sind allerdings vielfältig und reichen von organisatorischen, technischen bis hin zu per Gesetz verordneten Schwachstellen. Während die Fälle DigiNotar und TürkTrust eindrucksvoll die Schwachstellen auf organisatorischer Ebene belegen, machte der Heartbleed-Vorfall[3] vor wenigen Wochen allen Beteiligten klar, dass auch die zugrunde liegenden technischen Implementierungen nicht fehlerfrei sind.

Diese beiden Aspekte können vom Nutzer noch beeinflusst werden, etwa durch Wahl einer anderen CA oder Implementierung. Bei per Gesetz verordneten Eingriffsmöglichkeiten wird es allerdings sehr problematisch, denn hier hat der Einzelne in der Regel keinerlei Gelegenheit, sich möglichen Maßnahmen zu entziehen – falls er sie überhaupt mitbekommt, denn Transparenz und Rechtsschutz spielen häufig leider ebenfalls keine besondere Rolle.

Das ist aber kein Novum, wie kürzlich Josef Foschepoth im Buch „Überwachtes Deutschland"[4] zusammen getragen hat. Denn bereits seit Beginn der Bundesrepublik hat es, so Foschepoth, zahlreiche Überwachungsmaßnahmen gegeben, und das sowohl auf die (Brief-)Post- als auch die Telekommunikation.

Snowden's Enthüllungen sind also nicht wirklich „neu", denn auch in einem Land wie Deutschland wird seit langem überwacht. Die Dimension der Überwachung hat sich allerdings stillschweigend den technischen Möglichkeiten angepasst. Zudem wurden die Kooperationen der Überwacher ausgebaut und der rechtliche Rahmen so erweitert, dass mittlerweile zahlreiche Unternehmen im Bereich Post- und Telekommunikation den Geheimdiensten weltweit Schützenhilfe leisten müssen – meist ebenfalls völlig intransparent und ohne Möglichkeiten des Rechtsschutzes für die Betroffenen.

Wie weit dies gehen kann, zeigt auch das Urteil eines amerikanischen Bundesrichter James Francis[5], der die Herausgabe von Kundendaten an die Überwachungsbehörden auch dann für zulässig erachtet, wenn diese an nicht-amerikanischen Serverstandorten liegen oder nicht-amerikanische Bürger betroffen sind. Und das gibt wirklich Anlass zur Sorge.

1 COMRichtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen; Amtsblatt Nr. L 013 vom 19/01/2000 S. 0012 - 0020 (2012) 238 final

2 Entwurf der Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (COM 2012 238 final)

3 Details hierzu etwa unter: https://de.wikipedia.org/wiki/Heartbleed

4 Josef Foschepoth: Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik. Bundeszentrale für politische Bildung, Bd. 1415, Bonn, Dezember 2013.

5 Details hierzu etwa unter: http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398