Antworten zur Anhörung Drucksache 16/3434 „Schutz vor Wirtschaftsspionage durch PRISM und Tempora“

Jürgen Schmidt,
heise Security,
ju@heisec.de
GPG-Key: E1374764, 5161 90CC D42E 5A2A 8D99 0F84 5768 22F9 E137 4764

Vorab:

Ich habe zu einigen der gestellten Fragen keine ausreichenden Informationen, um mir dazu eine "Expertenmeinung" anzumaßen. Das habe ich dann entsprechend auch so beantwortet. Insbesondere quantifizierende Aussagen kann ich nur sehr eingeschränkt treffen, da mir kein entsprechendes Zahlematerial vorliegt.

Darüber hinaus habe ich leider keine Möglichkeit, meine Erkenntnisse auf das Bundesland NRW zu einzuschränken.

Teil I. Situationsanalyse

1. Man muss davon ausgehen, dass alle Länder sich an Wirtschafts- und Industriespionage versuchen. Besonders aktiv und vor allem erfolgreich sind dabei die technisch hoch entwickelten, also insbesondere -- aber nicht nur -- die USA, China und Russland.

Darüber hinaus darf man sich auch nicht der Illusion hingeben, dass Indsutrie- und Wirschaftsspionage alleiniges Terrain staatlicher Akteure sind. Es ist zu bedenken, dass für die Banden, die sich auf Cyber-Crime spezialisiert haben, der Handel mit Daten und Informationen die zentrale Einnahmequelle darstellt. Dies geschieht immer mehr auf einem so hohen professionellen Niveau, dass auch die Beschaffung und der anschließende Verkauf von Geschäftsgeheimnissen in Reichweite ist. Wer es schafft, etwa bei einem Zahlungsdienstleister wie Global Payments 1,5 Millionen Kreditkartendatensätze zu stehlen, der kann sich auch bei E.ON (nur als Beispiel) gewinnversprechende Geheimnisse besorgen. Naheliegende Interessenten für derartige Informationen sind natürlich direkte Konkurenten.

2. Ja, das ist sie definitiv. Nicht nur Edward Snowden hat das ausdrücklich als Ziel der NSA-Aktivitäten bestätigt. Auch US-amerikanische Politiker erklären immer wieder, dass die Förderung der eigenen Wirtschaftsinteressen weit oben auf der Liste der Aufgaben von Intelligence Agencies steht [1]. Der Fall Enercon/Kenetech hat das bereits 1998 eindrücklich demonstriert [2,3]. Nun liegt Enercon zwar in Ostfriesland; aber dass das genauso gut E.ON oder RWE treffen könnte, liegt auf der Hand.

[1] http://www.faz.net/aktuell/politik/ausland/amerika/nsa-affaere-ja-meine-freunde-wir-spionieren-euch-aus-12267465.html?printPagedArticle=true

[2] http://de.wikipedia.org/wiki/Enercon

[3] http://www.zeit.de/1998/39/199839.c_krypto_.xml

3. Dazu habe ich keine konkreten Zahlen.

4. Grundsätzlich werden zunächst Meta-Daten -- also Informationen, wer "spricht" wann mit wem -- systematisch abgeschöpft und einer Analyse nach allen denkbaren Kriterien zugänglich gemacht. Schon diese Informationen erlauben bei einer entsprechenden Auswertung vielfach tiefe Einblicke in sensible Bereiche. Darüber hinaus werden alle verschlüsselten Daten präventiv aufgezeichnet, um sie bei konkretem Bedarf oder nach einem neuen Durcbruch der Code-Breaker gezielt zu attackieren. Herkömmlicher Datenverkehr wird nach Schlüsselbegriffen gefiltert, um die Menge auf ein handhabbares Maß zu beschränken. Die Liste der Schlüsselbegriffe ist natürlich geheim; man sollte davon ausgehen, dass alles, was die spionierenden Länder als strategische Bereiche für Wirtschaft und Industrie identfizieren, dort ebenfalls präsent ist.

Das beschreibt nur das, was routinemäßig und ohne Anlass an Überwachungsdaten abegschöpft wird. Hinzu kommt natürlich, was bei gezeilten Aktionen anfällt und dann natürlich unter Umständen ebenfalls archiviert wird.

5. Zusammengefasst muss man feststellen, dass derzeit offenbar fast alles, was technisch machbar ist, auch tatsächlich umgesetzt wird. Selbst exotische Methoden der Informationsgewinnung, die man vor einem Jahr noch als rein theoretisch und paranoid verworfen hatte, haben sich als reale Bedrohung erwiesen. So wird bei Firmen eingebrochen, um Krypto-Schlüssel zu stehlen. Es werden unterirdisch verlegte Kabel "angebohrt", um die Glasfaser-Datenleitungen von großen Konzernen anzuzapfen und vieles mehr.

6. Das entzieht sich meiner Kenntnis.

7. Das entzieht sich meiner Kenntnis.

8. Besonders wichtige Angriffsziele sind insbeondere die Bereiche Telekommunikation und innovative Branchen wie die Energiewirtschaft. Als besonders unterstützungsbedürftig würde ich jedoch allgemein den Bereich kleiner und mittelständischer Unternehmen betrachten, bei denen (IT-)Sicherheit oft nicht ausreichend als Problem bewusst und im Unternehmen verankert sind.

9. Ausgehend davon, dass es in dieser Bezeihung NRW nicht sonderlich vom Rest der Republik abweicht, gehe ich davon aus, dass dies auch hier im KMU-Bereich nicht der Fall ist.

Teil II: Verbesserungsmöglichkeiten

10. Technisch würde ich sagen: Der richtige Einsatz von Kryptografie ist ein Schlüssel zum erfolgreichen Schutz vor Spionage. Dieser sollte aktiv unterstützt und gefördert werden. Praktisch brauchen wir einen Konsens, dass eben nicht alles, was technisch machbar ist, auch akzeptabel ist und natürlich Verträge und Abkommen, die dies absichern. Insbesondere gelten derzeit grundlegende Datenschutzbestimmungen immer nur für die jeweiligen Staatsbürger beziehungsweise Unternehmen eines Landes -- also im Fall der NSA für US-Amerikaner und amerikanische Firmen. Hier ist die Politik gefordert, diesen Schutz zumindest auch für andere Länder zu etablieren.

Darüber hinaus brauchen wir mehr Überwachung der Geheimdienste und Datenvermeidungstrategien.

11. Essentiell für eine Zusammenarbeit ist, dass eine eindeutige und ausschließliche Fokussierung auf den Schutz vor Spionage vorhanden und auch deutlich sichtbar ist. Sobald eine staatliche Behörde auch "offensive Aufgaben" -- also solche zum Sammeln von Informationen -- hat, fehlt das Vertrauen für eine konstruktive Zusammenarbeit.

12. Der Antrag ist aus meiner Sicht ein wichtiger Schritt in die richtige Richtung. Da das Thema nie abschließend behandelt werden kann, ist er natürlich nicht ausreichend.

13. Ich habe nicht den Eindruck, dass man hier von koordinierten Aktivitäten sprechen kann. Aber ich habe auch keinen speziellen Einblick.

14. Dazu habe ich keine konkreten Informationen.

15. Dazu habe ich keine konkreten Informationen.

16. Ja, verpflichtende Meldungen von Angriffen sind essentiell, um sich eine realistische Einschätzung der Situation zu verschaffen und dann angemessene Gegenmaßnahmen einzuleiten. Die Herausforderung ist eine sinnvolle Festlegung der Schwelle für eine Meldepflicht.

17. Das Thema ist äußerst problematisch, weil es in vielen Bereichen schlicht keine Alternativen gibt. Insbesondere wäre es fatal, etwa statt Router von der US-Firma Cisco einfach auf die des chinesischen Herstellers Huawei auszuweichen. Auch eine blinde Empfehlung für deutsche Alternativen fällt mir schwer, wenn ich sehe, dass etwa die Endkundenprodukte großer deutscher Diensteanbieter wie der Telekom zumindest bei der technischen Sicherheit in meinen Tests um Klassen schlechter abschneidet als etwa der amerikanische Konkurrent Google. Da mag ich nicht blind glauben, dass es um die Qualität der Angebote für Firmen so ganz anders bestellt ist.

Auf der anderen Seite ist zu beobachten, dass gerade kleinere deutsche Firmen aus Sicherheitssicht zum Teil exzellente Angebote haben. Aus meiner Sicht ist es deshalb besser, gerade kleinen und mittleren Firmen, die sich im Bereich Sicherheit profilieren, bessere Chancen und gezielte Förderung zukommen zu lassen, als dieses Geld in große Konzerne zu investieren, die sich Sicherheit vor allem auf die Fahne schreiben.

Zu den Unterpunkten:
a) Router, Netzwerkinfrastruktur und allgemein Hardware von ausländischen und insbesondere amerikanischen Firmen würde ich mittlerweile - also nach Snowden - auch als ernstes Problem betrachten. Aber ich sehe in diesen Bereichen wenig Alternativen.

b) Im Desktop-Bereich hat Microsoft Windows nach wie vor eine so dominante Rolle, dass ein genereller Verzicht darauf schlicht nicht möglich ist. Vor allem weil man mit dem zweitgrößten Player Apple ja auch nicht aus dem amerikanischen Einflussbereich heraus kommt. Trotzdem sollte man sich bewusst sein, dass diese beiden Hersteller sich zu einer weitgehenden Zusammenarbeit mit der NSA bereit erklärt haben. Die geht zumindest dem Anschein nach bei Microsoft über das, wozu sie rechtlich zwingend verpflichtet sind, noch hinaus.

Es gibt hier allerdings die Chance durch eine gezielte Förderung des Einsatzes offener Systeme wie Linux im öffentlichen Bereich, die im Licht der Enthüllungen neu bewertet werden sollte. China hat etwa ca 2000 ein eigenes Linux entwickelt, um strategisch gegen seine Abhängigkeit von Microsoft zu reduzieren und wurde dafür belächelt. Heute haben sie mit Red Flag Linux eine durchaus realistische Perspektive. Laut Wikepedia etwa arbeiten mittlerweile Firmen wie "Hewlett-Packard, Oracle, IBM, Dell und Intel" mit Red Flag zusammen.

Bei den Antiviren-Produkten gibt es bereits gute deutsche Anbieter, deren Einsatz gegenüber Firmen wie Symantec eigentlich vorzuziehen ist.

c) Der Einsatz von Cloud- und Internet-Diensten aus dem amerikanischen Hoheitsgebiet ist ebenfalls äußerst problematisch. Unter anderem deshalb, weil hier ohne großen Aufwand unter Umständen direkt zu verwertende Daten anfallen. Bislang zu wenig berücksichtigt wurde die Tatsache, dass im Rahmen von "legitimen Ermittlungen" oft auch viele anderen Daten zugänglich werden, die dann zweifelsohne in den großen NSA-Daten-Pool einfließen, um dann unter Umständen später zweitverwertet zu werden. So kann beispielsweise eine erzwungene Herausgabe des geheimen Schlüssels eines Servers alle Daten dechiffrieren, die jemals über diesen Server gingen. Man darf sich nicht der Illusion hingeben, dass die Daten von Ausländern die da "quasi nebenbei" anfallen in irgendeiner Weise tabu sind.

18) Wichtig ist vor allem, dass klar gestellt wird, dass technische Standards sakrosankt sind. Wer wie die NSA internationale, technische Standards mit einer Hintertür versieht, um sich einen Vorteil zu verschaffen, agiert als Brunnenvergifter und sollte von der internationalen Gemeinschaft als solcher behandelt werden.

19) "Made in Germany" hat das Potential ein Gütesiegel für Sicherheit und Datenschutz zu werden. Dazu müsste es allerdings auch ganz gezielt mit entsprechender Qualität gestärkt werden. "E-Mail Made in Germany" etwa ist ein krasses Beispiel dafür, wie es nicht funktionieren kann. Die Firmen boten Sicherheitsstandards, die u.a. weit hinter dem amerikanischer Anbieter wie Google zurückfielen und verkaufen Maßnahmen, die dort schon seit Jahren als selbstverständlich sind, als großen Fortschritt in Sachen Datenschutz und Sicherheit.

20) Grundsätzlich ist ein möglichst direktes Routing natürlich zu bevorzugen. Deshalb tauschen auch fast alle deutschen Internet-Provider ihre Daten gegenseitig und kostenneutral am DE-CIX aus. Der einzige große Provider, der sich diesem so genannten Peering verweigert, ist die Telekom. Hintergrund: Sie hat mit ihrem Quasi-Monopol bei DSL-Endkunden einen ausreichend großen Hebel, um die anderen Provider zu zwingen, für dieses Peering zu bezahlen. Da manche das nicht tun, gehen die Daten dann über ausländische Netze. Dass ausgerechnet der Telekom-Chef jetzt ein "Schengen-Routing" fordert, ist eigentlich absurd. Denn er könnte durch ein kostenneutrales Peering die Umleitung über ausländische Netze sofort beenden. Ihm schwebt offenbar eher eine Zwangsverpflichtung zu einem kostenpflichtigen Peering mit der Telekom vor -- also eine

Zwangsabgabe für die Konkurrenz, was offensichtlich kontraproduktiv und schädlich wäre.

Beim aktuellen Stand der Dinge ist darüber hinaus ebenfalls fraglich, ob das direkte Routing eine Spionage durch die NSA wirklich ausschliessen würde. Das wäre nur dann gewährleistet, wenn die Daten nicht etwa indirekt über deutsche Dienste oder Low-Level-Provider wie Level 3 zugänglich gemacht würden.

21. Edward Snowden war ein extremer Glücksfall für unsere Gesellschaft. Weil er nämlich ein funktionierendes Gewissen hatte und sich - soweit können wir das jetzt schon beurteilen - bei dem was er tat, nicht von Profitgier sondern von diesem Gewissen leiten ließ. Snowden hat auch demonstriert, dass ganz offensichtlich nicht einmal die NSA eine nicht autorisierte Nutzung der gesammelten Daten ausschließen kann. Im Gegeneil -- wie er mehrfach betonte, sind die internen Kontrollmechanisnmen -- also wer, wann aus welchen Gründen Zugriff auf diesen Daten-Pool nimmt -- sehr unterentwickelt bis gar nicht vorhanden. Man muss davon ausgehen, dass hunderte, vielelicht sogar tausende Menschen ähnlichen Zugang zu solchen Daten haben wie er. Zu hoffen, dass niemals ein anderer auf die Idee kommt, diese Daten anders als vorgesehen zu nutzen, ist blauäugig. Dann aber auch noch davon auszugehen, dass das ebenfalls ein solcher Glücksfall ist, bei dem Profitgier offenbar keine Rolle spielt, wäre schon
mehr als fahrlässig.