

*Eine Bundesregierung ohne einen IT-Sicherheits-Plan versagt bei der Herausforderung, IT-Sicherheit herzustellen, da es an verbindlichen Zielvorgaben mangelt. In diesem Fazit waren sich die Experten auf einer Veranstaltung der Grünen NRW-Landtagsfraktion zum Thema 'IT-Sicherheit in der Wirtschaft' einig.*

Am 24. Oktober 2014 hatte die Grüne Landtagsfraktion in Nordrhein-Westfalen zu der Veranstaltung „Abgehört und Ausgespäht – Konsequenzen des NSA-Skandals für die Wirtschaft in NRW“ in den Landtag eingeladen. Neben den Grünen Landtagsabgeordneten Daniela Schneckenburger, Verena Schäffer und Matthi Bolte waren auf das Podium geladen: der Leiter des Verfassungsschutzes NRW, Burkhard Freier, Prof. Dr. Norbert Pohlmann als Geschäftsführender Direktor des Instituts für Internetsicherheit an der Westfälische Hochschule Gelsenkirchen sowie als Vertreter der IHK NRW Dr. Matthias Mainz.

Angesichts der stetig neuen Erkenntnisse aus dem Dokumenten-Fundus von Edward Snowden - insbesondere zur Wirtschaftsspionage von NSA und GCHQ – war eigentlich mit einer großen Resonanz zu rechnen. Doch leider verliefen sich nur wenige Personen im großen Veranstaltungsraum. Dennoch nutzten insbesondere Burkhard Freier und Professor Norbert Pohlmann die Gelegenheit, um die aktuelle Situation intensiv aus ihrem Blickwinkel zu beleuchten. Dabei unterstrich Freier natürlich zunächst die immense Bedrohung durch Wirtschaftsspionage und belegte dies auch mit Zahlen:

- Schaden durch Wirtschaftsspionage: ca. 50 Mrd. € in Deutschland / ca. 10 Mrd. € in NRW pro Jahr
- jedes 2. Unternehmen wurde bereits Opfer eines Spionageversuchs
- gefährdet sind auch kleinere und mittlere Unternehmen

Erschreckend sei die Reaktion der Wirtschaft auf diese Bedrohung: Knapp 60 % der Unternehmen habe keine Konsequenzen aus dem NSA-Skandal gezogen. Noch verheerender: Nach Erkenntnissen des BSI verhielten sich ArbeitnehmerInnen an ihrem Arbeitsplatz wesentlich unvorsichtiger als zu Hause. Die Gründe:

- 39 % vertrauen auf den Schutz der Unternehmens-IT
- 76% öffnen verdächtige Mails eher am Arbeitsplatz im Vertrauen auf die dort installierten Schutzprogramme
- 29% öffnen verdächtige Inhalte am Arbeitsplatz, das es sich dort nicht um die privaten Rechnersysteme handelt.

Dieses Verhalten am Arbeitsplatz birgt für Freier angesichts der aktuellen Angriffszahlen ein hohes Risikopotential für jedes Unternehmen:

- 200.000 neue Varianten von Viren, Trojanern und Würmern täglich (lt. Deutsche Telekom AG auf BKA-Herbsttagung 2013)
- 800.000 Angriffe täglich „mit der Schrotflinte“ auf 90 Sensoren - (Lockvogelsysteme/„Honeypots“ -) der Deutschen Telekom AG (lt. Deutsche Telekom AG auf BKA-Herbsttagung 2013)
- täglich 2 neue kritische Schwachstellen in Softwareprodukten (lt. „Schwachstellen-Lagebild“ des BSI vom 07. Mai 2014)
- in Deutschland im 2. Quartal 2013 bis zu 2,6% gefährliche Webseiten=Drive-by-Exploits (lt. „Schwachstellen-Lagebild“ des BSI vom 07. Mai 2014)
- Schätzung: 1.000.000 Bots in Deutschland, Rent a Bot: 10.000 Bots kosten 160\$ (lt. „Schwachstellen-Lagebild“ des BSI vom 07. Mai 2014)

Die Empfehlung des Leiter des Verfassungsschutzes angesichts dieser Bedrohungsanalyse: Ein Unternehmen solle sich auf 5-7 % seiner Betriebsdaten konzentrieren und diese als „Kronjuwelen“ maximal absichern. Für den Rest wären die Aufwendungen der Schutzmaßnahmen viel zu hoch, um einen wirksamen Schutz aufzubauen.

Professor Norbert Pohlmann hielt sich in seinem Vortrag nicht lange mit der aktuellen Analyse auf – diese wurde ja von seinem Vorredner ausführlich durchgeführt. Vielmehr machte Pohlmann schon in seinen Anfangsworten deutlich, wo das eigentliche Problem aus seiner Sicht liegt: Es gäbe in Deutschland keinen Plan, wie nun tatsächlich mehr Sicherheit für Daten erreicht werden könnte.

Dabei verglich Pohlmann die aktuelle Situation bei Datenschutz und Datensicherheit mit der Situation auf den Straßen in der BRD Anfang der 70er Jahre. Angesichts von fast 20.000 Toten pro Jahr hatten die Verkehrsminister damals Konsequenzen gezogen und eine über Jahre andauernde Sicherheitskampagne gestartet. In der Folge wurden nicht nur Airbags und Sicherheitsgurte in den Fahrzeugen verbaut. Auch das Sicherheitsbewusstsein der Bürgerinnen und Bürger wurde über Jahre geschult. Der Erfolg: Heute sterben im vereinigten Deutschland nur noch 3.600 Menschen pro Jahr im Straßenverkehr.

In der heutigen Situation im Internet hätten nach Pohlmann Unternehmen sowie die

Bevölkerung zwar die Möglichkeit, Airbags und Sicherheitsgurte zu benutzen. Doch das 'Internet-Fahrzeug' müsse sich jeder selber zusammen bauen, da nur Einzelteile, aber keine funktionierende Gesamtlösung bereit stünde. Und so käme es immer wieder zu Kollateralschäden auf den Datenautobahnen, bei denen so manches Unternehmen in die Insolvenz getrieben wird.

Pohlmann forderte von der Politik, endlich einen Sicherheitsplan aufzusetzen ähnlich wie die deutschen Verkehrsminister vor über 40 Jahren. Kern dieses Plans sollten verbindliche Meilensteine sein, wann welche Sicherheitsmaßnahmen umzusetzen wären. Dabei käme insbesondere dem Bewusstseinswandel in und der Teilhabe von der Bevölkerung eine große Bedeutung zu. Das Sicherheitsproblem ließe sich nicht mit einzelnen Maßnahmen lösen, da es sich um eine globale und gesamtgesellschaftliche Herausforderung handeln würde.

In der anschließenden Diskussion nahmen zwei Themen einen größeren Raum ein. Zum einen stimmten Freier und Professor Pohlmann darin überein, dass wieder Vertrauen in die IT in der Bevölkerung wachsen müsse. Dabei betonte Freier, dass auch der Verfassungsschutz dieses Vertrauen braucht, um bei der Abwehr von Spionageangriffen erfolgreich zu sein. Hier sei aber nicht nur der Dienst selber in der Pflicht, sondern auch die Politik, die eben für mehr Transparenz sorgen müsse.

Ein weiterer Diskussionspunkt drehte sich um die Strategie, wie sichere IT-Systeme in die Infrastruktur einzuführen wären. Es wurden zwei Wege angedacht – einmal über den Markt, der die neuen Systeme liefert, sobald diese auch von den Anwendern gefordert würden. Alternativ wurde darüber nachgedacht, in wie weit der Staat Regeln vorschreiben müsse, welche Systeme wie einzusetzen wären.

Meine persönliche Bilanz der Veranstaltung: Die interessantesten Themen hätten mehr Publikum verdient gehabt. Insbesondere die richtigen Forderungen an die Politik müssen lauter und penetranter vorgetragen werden. Eine Anschlussveranstaltung, die sich mit konkreten Sicherheitsplänen und 'Meilensteinen' bei deren Umsetzung beschäftigt, ist dringend geboten. Und: Natürlich muss der Staat die Sicherheitsregeln bis in den privaten Haushalt hinein streng vorschreiben. Denn ohne den Gurtzwang würden heute noch unbelehrbare Schädel an der Windschutzscheibe zerplatzen.

Quellen:

[Runden Tisch „Wirtschaftsspionage“ -&gt; Ein paar Gedanken zum Thema](#) , Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen, <http://www.internet-sicherheit.de>

[Wirtschaftsspionage – Abgehört und Ausspioniert](#) , Burkhard Freier, Leiter des Verfassungsschutzes Nordrhein-Westfalen