Ministerium für Inneres und Kommunales
des Landes Nordrhein-Westfalen

Ministerium für Inneres und Kommunales NRW, 40190 Düsseldorf

An die
Präsidentin des Landtags
Frau Carina Gödecke MdL
Platz des Landtags

40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE

STELLUNGNAHME
16/1351

Alle Abg

30. Januar 2014
Seite 1 von 1

Aktenzeichen
(bei Antwort bitte angeben)
614

Telefon 0211 871-2701
Telefax 0211 871-

Öffentliche Anhörung des Ausschusses für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk zum Thema:
„Nordrhein-westfälische Unternehmen vor staatlicher Wirtschaftsspionage durch Überwachungsprogramme wie PRISM und Tempora schützen!"
am 6. Februar 2014, 12.00 Uhr, Plenarsaal,
Antrag der Fraktion der Piraten, Drucksache 16/3434
Antworten zu den Fragen des Fragenkatalogs

Sehr geehrte Frau Landtagspräsidentin,

ich bedanke mich für die Einladung zu der o.g. Anhörung am 6.Februar 2014 und übersende Ihnen anliegend meine Antworten nebst einer Anlage zu den Fragen.

Mit freundlichen Grüßen

Im Auftrag

(Freier)

Dienstgebäude und
Lieferanschrift:
Haroldstr. 5, 40213 Düsseldorf
Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@mik.nrw.de
www.mik.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle: Poststraße

Burkhard Freier
Leiter der Abteilung Verfassungsschutz
Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen

Öffentliche Anhörung
des Ausschusses für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk
zum Thema: „Nordrhein-westfälische Unternehmen vor staatlicher Wirtschaftsspionage durch Überwachungsprogramme wie PRISM und Tempora schützen!“

Antrag der Fraktion der Piraten, Drucksache 16/3434

am 6. Februar 2014, 12.00 Uhr Plenarsaal

Antworten zu den Fragen des Fragenkatalogs

1. **Welche Dienste, Staaten und Unternehmen betreiben in welchem Umfang Wirtschafts- und Industriespionage in NRW?**

Unter dem Begriff Wirtschaftsspionage verstehen die deutschen Sicherheitsbehörden die staatlich gelenkte oder gestützte Ausforschung von Wirtschaftsunternehmen oder Forschungseinrichtungen durch fremde Nachrichtendienste. Im Gegensatz dazu handelt es sich bei der sogenannten Industrie- und Konkurrenzspionage um die illegale Beschaffung von Know-how und Waren durch konkurrierende Unternehmen.

Da es sich bei der staatlich gelenkten Wirtschaftsspionage durch Nachrichtendienste um eine geheimdienstliche Tätigkeit für eine fremde Macht nach § 3 Abs. 1 Nr. 2 VSG NRW handelt, hat der Verfassungsschutz NRW zur Bekämpfung dieses Phänomens die Aufgabe, entsprechende Informationen zu sammeln und auszuwerten. Die Bekämpfung von Industriespionage obliegt den Strafverfolgungsbehörden.

Nordrhein-Westfalen ist mit seiner Vielzahl an hochinnovativen Unternehmen, Universitäten, Fachhochschulen und Forschungseinrichtungen Ziel von Ausspähungen und ein interessanter Aktionsraum für Wirtschafts- sowie für Industriespionage. Dabei kann ein bekannt gewordener Angriff häufig weder als eindeutiger Fall nachrichtendienstlich gesteuerter Wirtschaftsspionage noch als eindeutiger Fall von Konkurrenzausspähung kategorisiert werden. Die Abgrenzung zwischen diesen beiden Formen der illegalen Know-how-Abschöpfung ist schwierig, weil sowohl Zielobjekt als auch Methoden weitgehend identisch sind. Die Herkunft und Verbindungswege der Ausspähmaßnahme werden regelmäßig mit hohem Aufwand verschleiert. Hinweise auf fremde Nachrichtendienste als mögliche Auftraggeber von Wirtschaftsspionage haben sich bisher nicht eindeutig klären lassen, so dass auch keine gerichtsfesten Erkenntnisse aus strafrechtlichen Ermittlungsverfahren vorliegen.

Gleichwohl gibt es Indikatoren, die nahe legen, dass Wirtschaftsspionage ein Betätigungsfeld für ausländische Nachrichtendienste ist. Es gibt Staaten, die ihren Nachrichtendiensten einen gesetzlichen Auftrag dafür gegeben haben. Nach dem Gesetz der russischen Föderation über die Auslandsaufklärung hat der russische Auslandsnachrichtendienst den Auftrag, „die wirtschaftliche Entwicklung und den wissenschaftlich-technische Fortschritt des Landes durch Beschaffung von wirtschaftlichen und wissenschaftlich-technischen Informationen durch die Organe der Auslandsaufklärung zu fördern.“ In anderen Staaten wie in der Volksrepublik China weisen bereits die Zahl der Angehörigen der Nachrichtendienste (mehrere 100.000) und der organisatorische Aufbau auf die Zielrichtung der Auslandsaufklärung hin. Es gibt jeweils eigene Arbeitsbereiche für die verschiedenen Aufklärungsbereiche und Wirtschaftsräume, zum Beispiel Westeuropa und damit auch Deutschland.

2. Ist die Sorge vor Wirtschaftsspionage durch befreundete Staaten begründet?

Die Verfassungsschutzbehörde des Landes Nordrhein-Westfalen hat keine eigenen Erkenntnisse, dass sogenannte befreundete Dienste Wirtschaftsspionage in Nordrhein-Westfalen betreiben. Auch dem Präsidenten des Bundesamtes für Verfassungsschutz liegen nach eigener Aussage „keinerlei Erkenntnisse vor, die die These einer Wirtschaftsspionage aus dem Westen stützen".

Dennoch muss davon ausgegangen werden, dass neben den klassischen Spionagezielen Politik und Militär auch Handelsstrategien, innovative Techniken oder Finanzströme für viele Staaten von hohem Interesse sind, weil eine stabile Volkswirtschaft Wachstum und Wohlstand des eigenen Landes bedeuten.

3. Wie hoch ist der jährliche wirtschaftliche Schaden durch Wirtschafts- und Industriespionage in NRW?

Nach Untersuchungen durch Befragungen von Unternehmen gehen Schätzungen davon aus, dass in der Bundesrepublik Deutschland jährlich Schäden zwischen 20 und 50 Milliarden Euro durch Wirtschaftsspionage und Wirtschaftskriminalität entstehen. Dabei gehen die Sicherheitsbehörden von einem erheblichen Dunkelfeld aus. Die Ursache liegt darin, dass betroffene Unternehmen in vielen Fällen versuchte wie auch erfolgreiche Angriffe entweder gar nicht feststellen oder aber aus Sorge vor Imageverlusten die von ihnen identifizierten Angriffe weder der Polizei noch dem Verfassungsschutz mitteilen. Belastbare absolute Zahlen zum wirtschaftlichen Schaden liegen deshalb nicht vor.

In Nordrhein-Westfalen mit seinen ca. 760.000 Unternehmen könnte der Schaden in Höhe eines zweistelligen Milliardenbetrags liegen. Es geht aber nicht allein um einen finanziellen Schaden in den Unternehmen. Das ausgespähte und gestohlene Know-how kann für die Konkurrenzfähigkeit des Unternehmens wesentlich sein. Beispielsweise kann der Diebstahl von Konstruktionsplänen für ein neues Bauteil im schlimmsten Fall die Insolvenz für das betroffene Unternehmen zur Folge haben, weil das Produkt vor dem „Erfinder" auf den Markt kommt, erwartete Gewinne

ausbleiben und jahrelange Entwicklungsarbeit mit entsprechend hohen Kosten nicht refinanziert werden können und das Kapital für zukünftige Investitionen fehlt.

Darüber hinaus kann die Wettbewerbsfähigkeit einer ganzen Branche beeinträchtigt werden, so dass auch der Allgemeinheit durch den Wegfall von Arbeitsplätzen oder geringere Steuereinnahmen ein Schaden entsteht.

4. Welche Informationen werden nachrichtendienstlich abgeschöpft?

Im Fokus der Wirtschaftsspionage stehen neben innovativer Technik und Erkenntnissen aus Forschung und Entwicklung auch Kundendaten, Marketingplänen sowie sensible Betriebs- und Geschäftsdaten der Unternehmen nahezu sämtlicher Branchen. Dazu gehören zum Beispiel:

- Herstellungsverfahren, Konstruktionsunterlagen,
- Spezialwerkzeuge und Steuerungssysteme,
- Forschungsergebnisse, Produktideen,
- Personaldaten,
- Kunden- und Lieferantenbeziehungen, Lagerbestände,
- Verkaufsstrategien, Absatz- und Vertriebswege,
- Budgetplanungen, Kalkulationsunterlagen und Investitionsvorhaben,
- Unternehmensstrategien der nächsten Jahre.

5. Welcher Methoden wird sich hierbei bedient?

Wirtschaftsspionage erfolgt im Wesentlichen durch drei Methoden:

5.1 Open Source Intelligence (OSINT)

Die häufigste, weil einfachste Methode fremder Nachrichtendienste ist, die erforderlichen Informationen durch intensives Abschöpfen von offen zugänglichen

Quellen zu beschaffen (im nachrichtendienstlichen Sprachgebrauch: Open Source Intelligence -OSINT).

Auf diese Weise gelangen fremde Nachrichtendienste an wirtschaftlich wertvolle Daten, die in wachsender Anzahl offen zur Verfügung stehen, zum Beispiel über Internetauftritte der Unternehmen, über Preisgabe von Unternehmensinterna durch Mitarbeiterinnen und Mitarbeiter in sozialen Netzwerken, über Kontakte auf Messen, Symposien oder auf Empfängen in Botschaften und Konsulaten sowie über Angaben in Visaanträgen wie z. B. Funktion im Unternehmen oder Gehaltshöhe.

Der Wert dieser offen erhobenen Daten wird oftmals unterschätzt, weil eine Einzelinformation in der Regel nicht sehr aussagekräftig erscheint. In einer methodischen Verknüpfung ergibt sich für einen fremden Nachrichtendienst jedoch ein Gesamtbild, aus dem sich auch sensible Unternehmensdaten ablesen lassen.

5.2 Human Intelligence (HUMINT)

Des Weiteren werden menschliche Quellen zur Informationsbeschaffung genutzt (im nachrichtendienstlichen Sprachgebrauch: Human Intelligence- HUMINT).

Dabei setzen Nachrichtendienste gezielt Agenten ein. Hierzu zählen „statuswidrig abgetarnte" Diplomaten, die von ihren Botschaften und Konsulaten aus einer nachrichtendienstlichen Tätigkeit nachgehen. Der gezielte Einsatz von ausländischen Praktikanten oder Doktoranden ist eine weitere Möglichkeit, um unmittelbar an sensible Unternehmensdaten zu gelangen. Zu HUMINT zählt aber auch die klassische nachrichtendienstliche Methode des Kompromats. Kompromate werden beispielsweise durch den Einsatz von übermäßigen Alkohol, Drogen oder den Einsatz von Prostituierten geschaffen. Mit der Drohung, das kompromittierende Material zu veröffentlichen, werden Personen zur Kooperation genötigt.

5.3 Signal Intelligence (SIGINT)

Einen sehr hohen Stellenwert hat inzwischen die Informationsgewinnung durch Fernmelde- und elektronische Aufklärung (im nachrichtendienstlichen Sprachgebrauch: Signal Intelligence – SIGINT). Die Globalisierung der Kommunikation mit Hilfe des Internets bietet dabei für Nachrichtendienste zahlreiche Ansatzpunkte für ihre elektronische Aufklärung.

Netzwerkstrukturen und Netzknoten für die Kommunikation verlaufen zumeist über das Ausland; die einzelnen „Pakete“ werden von den Netzbetreibern oftmals über den billigsten Weg geleitet, auch wenn dieser geografisch länger ist und z.T. außerhalb Deutschlands liegt. Ein Abgreifen dieser Daten auf den Vermittlungsstellen, die im Ausland liegen, hinterlässt kaum Spuren. Eine Verschlüsselung bietet nur Schutz, wenn sie von Endgerät zu Endgerät (Ende-zu-Ende-Verschlüsselung) erfolgt und ein anerkannt sicheres Verschlüsselungsverfahren angewendet wird.

Neben solchen „passiven“ Ausspähungen durch Abgreifen setzen Staaten wie China auf „aktive Angriffe“, die entweder automatisiert erfolgen oder spezifiziert ein einzelnes Unternehmen oder eine einzelne Mitarbeiterin oder Mitarbeiter betreffen. Anders als die automatisierten Massenangriffe sind diese Einzelangriffe regelmäßig nicht mit herkömmlichen Methoden (Firewall, Virenscanner) zu erkennen. Wesentliches Ziel ist in diesen Fällen die Infizierung der Unternehmensnetzwerke mit Spionagesoftware, um illegal Firmen Know-how zu erlangen.

6. Was tut das Land NRW, um die Firmen im Land und damit den Wirtschaftsstandort zu schützen?

Der Verfassungsschutz des Landes Nordrhein-Westfalen informiert in seinen jährlichen Berichten über die Gefahren der Wirtschaftsspionage. Ebenso sensibilisiert er gerade kleine und mittlere Unternehmer in zahlreichen Veranstaltungen in den Unternehmen selbst, bei Veranstaltungen von Wirtschaftsverbänden und Industrie- und Handelskammern sowie anderen öffentlichen Veranstaltungen über die Gefahren der Wirtschaftsspionage. Im Jahr 2012 hielten Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes NRW 210 Vorträge vor ca. 6.500 Multiplikatoren, davon 30 Vorträge bei Industrie- und Handelskammern sowie bei größeren Unternehmerverbänden. Einer der hier ansässigen DAX 30-Konzerne wurde bei einer hausinternen „Awareness-Kampagne“ unterstützt.

Unternehmen und Verbände finden zudem auf der Homepage des Ministeriums für Inneres und Kommunales unter der Adresse
http://www.mik.nrw.de/verfassungsschutz/spionageabwehr/abwehr-von-wirtschaftsspionage.html
ein umfangreiches Informations- und Beratungsangebot, darunter auch einen „On-

line-Test", der es in kurzer Zeit erlaubt, in einem ersten Schritt festzustellen, ob ein Unternehmen durch Wirtschaftsspionage gefährdet ist.

Darüber hinaus geht der Verfassungsschutz des Landes Nordrhein-Westfalen jedem konkreten Verdachtsfall konsequent nach und ermittelt dazu auch vor Ort. Er sichert dabei auf Wunsch Vertraulichkeit zu. Er berät in diesem Zusammenhang Unternehmen auch bei der Presse- und Öffentlichkeitsarbeit. Beim Verfassungsschutz gehen pro Woche durchschnittlich zwei Anfragen/Hinweise ein. Das sind Anfragen beispielsweise dazu, wie ein Unternehmen sich allgemein vor Ausspähung schützen kann. Des Weiteren geht es um konkrete Verdachtsfälle, wenn das Unternehmen Anhaltspunkte für einen Angriff vermutet, oder beispielsweise den Verdacht hat, ein ausländischer Praktikant habe ggf. Unterlagen entwendet.

Bereits 2001 wurde in Nordrhein-Westfalen eine Sicherheitspartnerschaft gegen Wirtschaftsspionage und Wirtschaftskriminalität in Nordrhein-Westfalen als Public Private Partnership gegründet. In dieser Partnerschaft haben sich das Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen (Abteilung für Verfassungsschutz und Polizeiabteilung), das Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk, der Verband für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V. und die Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen e.V. zusammengeschlossen, um gemeinsam gegen Wirtschaftsspionage und Wirtschaftskriminalität vorzugehen. Die Sicherheitspartnerschaft hat z.B. 2013 gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vier öffentliche Veranstaltungen in wirtschaftlichen Schwerpunkt-regionen durchgeführt. Dabei wurde über die aktuelle Bedrohungslage und über Angriffstechnologien informiert. Gleichzeitig wurden Empfehlungen zum Schutz der eigenen Wettbewerbsvorteile und zur planvollen und erfolgreichen Sicherung von Spuren digitaler Angriffe auf die Unternehmensnetzwerke weitergereicht.

7. Wie ist die Aufklärungsquote?

Aufklärungsquoten liegen für den Bereich der staatlich gelenkten Wirtschaftsspionage nicht vor. Wird den Sicherheitsbehörden ein Angriff auf ein Unternehmen bekannt, so bleibt häufig offen, ob der Fall der nachrichtendienstlich

gesteuerten Wirtschaftsspionage zuzuordnen ist oder ob eine der Konkurrenzausspähung ohne nachrichtendienstliche Beteiligung vorliegt. Die Abgrenzung zwischen diesen beiden Formen des Know-how-Diebstahls ist schwierig, weil sowohl Zielobjekt als auch Methoden weitgehend identisch sind.

8. Welche Wirtschaftsbranchen sind in besonderem Maße auf politische Hilfe gegen Wirtschaftsspionage angewiesen?

Grundsätzlich sind alle deutschen Wirtschaftsbereiche, Unternehmen und Branchen von Wirtschaftsspionage bedroht, die erfolgreich im nationalen und vor allem internationalen/globalen Wettbewerb stehen. Besonders betroffen sind dabei bundesweit die Forschungs- und Entwicklungsabteilungen von Unternehmen aus den Bereichen Rüstung, Luft- und Raumfahrt, Satellitentechnik, Maschinenbau, Medizin- und Mikrotechnologie, erneuerbare Energien wie Windkraftanlagen und Sonnenkollektoren, Biotechnologie und Chemie. Neben den großen Unternehmen kommen in Nordrhein-Westfalen und in den Regionen hinzu die sog. "Hidden Champions", also kleine und mittlere Unternehmen mit hoch innovativer Technik und Produkten, die häufig auf dem Weltmarkt an der Spitze, in der Öffentlichkeit aber weniger bekannt sind und zum Beispiel elektronische Bauteile wie Steckverbindungen, Zubehörteile für Autos oder für Rüstungsgüter herstellen.

Aber auch kleine Unternehmen mit neuen Marktideen („Start Ups") und einem Potenzial für große Marktchancen sind für Wirtschaftsspionage von Interesse. Genauso sind auch Verfahren zur Lebensmittelproduktion und Produkte für die Landwirtschaft von Ausspähungen betroffen.

Neben den Unternehmen sind auch Universitäten und Fachhochschulen, Forschungseinrichtungen, Technologie- und Gründerzentren, wie sie in Nordrhein-Westfalen zahlreich zu finden sind, von nachrichtendienstlichen Angriffen bedroht.

9. Haben die Unternehmen in NRW ein ausreichendes Problembewusstsein?

Angesichts der zunehmenden Zahl gerade von elektronischen Attacken, des gesamtwirtschaftlichen Schadens von Wirtschaftsspionage und der Folgen für

einzelne Unternehmen bis hin zur Insolvenz kann das Problembewusstsein nicht hoch genug sein. Gleichwohl ist es nicht in allen Unternehmen gleich ausgeprägt. Gerade kleine Unternehmen unterschätzen häufig die Gefahr, Ziel von Wirtschaftsspionage zu werden. Die hohe Anzahl von Anfragen durch Verbände und Unternehmen an den nordrhein-westfälischen Verfassungsschutz nach Referenten für Präventionsveranstaltungen, deutet jedoch darauf hin, dass das Interesse an Informationen zum Schutz vor Wirtschaftsspionage stetig wächst.

10. Welche Maßnahmen sollten a) Unternehmen und b) Politik ergreifen, um Wirtschaftsspionage einzudämmen? Welche zusätzlichen Bemühungen sollte die Landespolitik in diesem Bereich kurz- und langfristig unternehmen?

Ganz wesentlich ist, dass sich die Unternehmen klar darüber sind, jederzeit Ziel von Wirtschafts- oder Konkurrenzausspähung sein zu können und dass es in Anbetracht der vielfältigen Angriffsmethoden keinen hundertprozentigen Schutz gibt, schon gar nicht durch Standardlösungen. Unternehmen müssen deshalb zunächst ihre existenziellen Betriebs- und Geschäftsgeheimnisse, die sogenannten Kronjuwelen, identifizieren. Dies sind in der Regel nicht mehr als 5 % aller Unternehmensdaten. In einem zweiten Schritt muss festgestellt werden, wie diese Daten geschützt sind, insbesondere wer im Unternehmen oder von außen Zugriff darauf hat. Zum Schutz des Know- how gilt es anschließend, ein ganzheitliches Sicherheitskonzept zu entwickeln und umzusetzen, das organisatorische und technische Maßnahmen sowie solche der Aufmerksamkeits- und Bewusstseinsschärfung („Awareness") umfasst. Unternehmenssicherheit ist mehr als lediglich IT-Sicherheit. Eine geeignete Basis für einen umfassenden Unternehmensschutz können die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie internationale Standards wie ISO 27001 ff. sein.

Es empfiehlt sich, den sensibelsten Bereich des IT-Netzwerks in einem Unternehmen vom Internet zu entkoppeln. Ohne eine Verbindung zum Internet können keine elektronischen Angriffe von außen erfolgen. Zudem muss die „Sicherheitslücke Mensch" geschlossen werden. Zum Sicherheitskonzept gehört deshalb zwingend, das Sicherheitsbewusstsein aller Angehörigen eines Unternehmens ständig zu schärfen. Ergänzend müssen die bestehenden Sicherheitsvorkehrungen und deren

Einhaltung auf ihre Wirksamkeit fortlaufend überprüft werden. Im Einzelfall kann es sich auch empfehlen, sensible IT-gestützte Verfahren einem Penetrationstest zu unterziehen, bei dem denkbare Angriffe simuliert und deren Folgen zur Fortentwicklung des Sicherheitskonzeptes genutzt werden.

11. Ergänzend: Wie müsste die Zusammenarbeit zwischen Staat (z. B. Verfassungsschutz, Zoll) und den Unternehmen gestaltet werden, um Wirtschaftsspionage effektiv abwehren zu können?

Basis für einen effektiven Schutz der Unternehmen ist eine vertrauensvolle Zusammenarbeit mit den Sicherheitsbehörden. Viele Unternehmen wenden sich jedoch nicht an die Sicherheitsbehörden, weil sie fürchten, dass gegen sie gerichtete versuchte oder erfolgreiche Angriffe zum Beispiel durch Cyberattacken, in der Öffentlichkeit bekannt werden und ihr Image und ihre Reputation Schaden nehmen. Dies ist insbesondere dann der Fall, wenn ihnen „anvertraute" Informationen, wie z.B. personenbezogene Daten von Kunden oder Zulieferern, abhanden gekommen sind. Zudem haften Geschäftsführungen unter bestimmten Voraussetzungen für die eingetretenen Schäden persönlich. Die Unternehmen müssen derartige Folgen jedoch nicht befürchten, wenn sie sich an den Verfassungsschutz NRW wenden. Dieser behandelt die ihm gemeldeten Fälle und die damit verbundenen Gespräche absolut vertraulich. Zwischen dem nordrhein-westfälischen Verfassungsschutz und den hier ansässigen Verbänden und vielen Unternehmen besteht bereits seit geraumer Zeit eine verantwortungsvolle und vertrauensvolle Zusammenarbeit

12. Halten Sie die im Antrag aufgeführten Forderungen an die Bundesregierung für ausreichend? Wenn nein, welche Maßnahmen sollten noch auf Bundesebene ergriffen werden, um die Unternehmen in Deutschland besser zu schützen?

Die Entscheidung, welche Maßnahmen auf Bundesebene zur Verhinderung von Wirtschaftsspionage getroffen werden, liegt bei der Bundesregierung. CDU und SPD haben in ihrem Koalitionsvertrag vom 27.11.2013 hierzu vereinbart: „Wir wollen unsere Unternehmen vor Wirtschafts- und Konkurrenzspionage aus aller Welt

schützen und eine nationale Strategie für den Wirtschaftsschutz erarbeiten". Sie haben damit einen Rahmen vorgegeben, den es unter Beteiligung der Länder auszufüllen gilt.

13. Sind Sie der Auffassung, dass die Aktivitäten deutscher Behörden zur Abwehr von Wirtschaftsspionage auf den verschiedenen politischen Ebenen ausreichend koordiniert sind? Brauchen wir eine "nationale Sicherheitsstrategie", wie sie etwa der Präsident des Bundesverbandes der Deutschen Industrie (BDI), Ulrich Grillo, forderte?

Die Landesbehörden für Verfassungsschutz sowie das Bundesamt für Verfassungsschutz tauschen ihre Information zum Thema Wirtschaftsspionage regelmäßig oder aus besonderem Anlass aus. Hierzu dient auch die sogenannte AG Wirtschaftsschutz, in der die Verfassungsschutzbehörden von Bund und Ländern vertreten sind.

Das Bundesministerium des Innern (BMI), der Bundesverband der Deutschen Industrie e.V. (BDI) sowie der Deutsche Industrie- und Handelskammertag (DIHK) haben mit anliegender Erklärung vom 28. August 2013 zum Thema „Wirtschaftsschutz in Deutschland 2015 – Vertrauen, Information, Prävention" ihre Absicht bekundet, gemeinsam einen zukunftsweisenden Wirtschaftsschutz in Deutschland auszugestalten. Die darin formulierten Handlungsziele können dazu beitragen, die vorhandene Koordination weiter auszubauen. Eine „nationale Sicherheitsstrategie" unter Einbeziehung der Länder kann dabei helfen, die Maßnahmen von Bund und Länder noch stärker zu koordinieren.

14. Wie bewerten Sie die Zusammenarbeit öffentlicher Institutionen mit den Unternehmen zum Thema Wirtschaftsspionage?

Die Zusammenarbeit zwischen öffentlichen Institutionen wie Behörden und Verbänden und den Unternehmen ist ein wichtiges und geeignetes Mittel zum Unternehmensschutz. Bereits 2001 wurde eine Sicherheitspartnerschaft gegen Wirtschaftsspionage und Wirtschaftskriminalität in Nordrhein-Westfalen gegründet. In dieser Partnerschaft haben sich das Ministerium für Inneres und Kommunales des

Landes Nordrhein-Westfalen (Abteilungen für Verfassungsschutz und Polizeiabteilung), das Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk, der Verband für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V. und die Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen e.V. zusammengeschlossen, um gemeinsam gegen Wirtschaftsspionage und Wirtschaftskriminalität vorzugehen Die Zusammenarbeit des nordrhein-westfälischen Verfassungsschutzes mit öffentlichen Instituten sowie mit den Unternehmen selbst ist traditionell gut und vertrauensvoll.

15. Welche Aufklärungsangebote sind bereits heute vorhanden oder sind vorstellbar, um die Unternehmen bzw. die Mitarbeiterinnen und Mitarbeiter von potentiell betroffenen Unternehmen zu sensibilisieren?

Der Verfassungsschutz des Landes Nordrhein-Westfalen informiert in seinen jährlichen Berichten über die Gefahren der Wirtschaftsspionage. Ebenso sensibilisiert er gerade kleine und mittlere Unternehmer in zahlreichen Veranstaltungen in den Unternehmen selbst, bei Veranstaltungen von Wirtschaftsverbänden und Industrie- und Handelskammern sowie anderen öffentlichen Veranstaltungen über die Gefahren der Wirtschaftsspionage. Im Jahr 2012 hielten Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes NRW 210 Vorträge vor ca. 6.500 Multiplikatoren, davon wurden 30 Vorträge bei Industrie- und Handelskammern sowie größeren Unternehmerverbänden gehalten. Einer der hier ansässigen DAX 30-Konzerne wurde bei einer hausinternen „Awareness-Kampagne“ unterstützt.

Unternehmen und Verbände finden zudem auf der Homepage des Ministeriums für Inneres und Kommunales unter der Adresse

http://www.mik.nrw.de/verfassungsschutz/spionageabwehr/abwehr-von-wirtschaftsspionage.html

ein umfangreiches Informations- und Beratungsangebot, darunter einen „Online-Test“, der es dem User in kurzer Zeit erlaubt, in einem ersten Schritt festzustellen, ob ein Unternehmen durch Wirtschaftsspionage gefährdet sein kann.

Darüber hinaus geht der Verfassungsschutz des Landes Nordrhein-Westfalen jedem konkreten Verdachtsfall konsequent nach und ermittelt dazu auch vor Ort. Er steht dazu allen Unternehmen als Ansprechpartner zur Verfügung, zum Beispiel bei

- Verdacht eines Angriffs auf Informations- und Kommunikationstechnik,
- Anhaltspunkten für Know-how-Verlust,
- Sicherheitsvorfällen in Auslandsniederlassungen und auf Geschäftsreisen,
- untypischen Einbruchsdelikten,
- Spionageverdacht gegen Mitarbeiter und Fremdpersonal,
- unerklärlichen Auftragsrückgängen oder unerklärlichem Verlust von Marktanteilen.

Die unter Frage 14 angesprochene Sicherheitspartnerschaft gegen Wirtschaftsspionage und Wirtschaftskriminalität hat 2013 gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vier öffentliche Veranstaltungen in wirtschaftlichen Schwerpunktregionen durchgeführt. Dabei wurde über die aktuelle Bedrohungslage und über Angriffstechnologien informiert. Gleichzeitig wurden fachliche Empfehlungen zum Schutz der eigenen Wettbewerbsvorteile und zur planvollen und erfolgreichen Sicherung von Spuren digitaler Angriffe auf die Unternehmensnetzwerke gegeben.

Die Informationsangebote des nordrhein-westfälischen Verfassungsschutzes werden unter Berücksichtigung neuer Erkenntnisse zur Wirtschaftsspionage kontinuierlich fortentwickelt und fließen in die Veranstaltungsreihen und Veröffentlichungen für die hier ansässige Wirtschaft ein.

16. Sind Sie der Meinung, dass es eine gesetzliche Verpflichtung für Unternehmen geben sollte, elektronische Angriffe an eine staatliche Zentralstelle zu melden?

Untersuchungsergebnisse zu der Frage, ob eine gesetzliche Verpflichtung für eine Meldung elektronischer Angriffe an eine staatliche Stelle dazu beitragen kann, eine bessere Vorsorge vor Angriffen treffen zu können, sind bisher nicht bekannt. Der Vorteil solcher Meldungen wäre, dass die Sicherheitsbehörden zeitnah zu Methoden und Ausspähziele informiert werden und damit für die Sicherheitskonzepte zusätzliche Informationen an die Unternehmen zurückspiegeln könnten. Zudem ist

nicht ausgeschlossen, dass nach einem Ausspähversuch weitere erfolgen, die ohne Ermittlungen möglicherweise unentdeckt bleiben. Aus zahlreichen Veranstaltungen ist dem Verfassungsschutz des Landes Nordrhein-Westfalen jedoch bekannt, dass ein Teil der Unternehmen eine derartige Verpflichtung eher kritisch sieht. Zudem gibt es bereits eine entsprechende Regelung für eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten in § 42a BDSG, die zunächst ausreichend erscheint.

17. Nach Informationen des Whistleblowers Edward Snowden haben sich US-Geheimdienste Zugriff auf die (Kunden-)Daten US-amerikanischer Internet- und Softwareunternehmen verschafft. Auch Verschlüsselungsdienste sollen betroffen sein. Zum Teil geschieht dies über eine (erzwungene) Kooperation mit den Unternehmen. Wie bewerten Sie vor diesem Hintergrund den Einsatz von IT-Produkten US-amerikanischer Anbieter? Bitte gehen sie jeweils gesondert auf (a) Hardware (Router etc.), (b) Sicherheits- und Systemsoftware (Betriebssysteme, Antivirenprogramme) sowie (c) Cloud- und Internet-dienste (Cloud-Storage, E-Mail-Provider etc.) US-amerikanischer Anbieter ein.

Der Verfassungsschutz des Landes Nordrhein-Westfalen verfügt über keine eigenen Informationen zu den in den Medien gegenüber der NSA und anderen Nachrichtendiensten erhobenen Vorwürfen, insbesondere über technische Details zu den Angriffen. Eine Bewertung von IT-Produkten US-amerikanischer Anbieter ist deshalb für den Verfassungsschutz des Landes Nordrhein-Westfalen nicht möglich.

18. Welche technischen Standards zur Gewährleistung der Sicherheit vor Wirtschaftsspionage sind denkbar?

Ein hundertprozentiger Schutz vor Wirtschaftsspionage lässt sich auch durch umfangreiche technische Maßnahmen nicht gewährleisten. Die erfolgversprechendste Methode ist, sensible Bereiche eines IT-Netzwerkes, die die sogenannten Kronjuwelen (exklusives besonders sensibles Know-how) eines Unternehmens beinhalten, vom Internet zu trennen. Außerdem empfiehlt der Verfassungsschutz die Erstellung eines Sicherheitskonzeptes. Grundlage dafür können die

Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie internationale Standards wie ISO 27001 ff. sein.

19. Wie bewerten Sie die Chancen für die deutsche IT-Wirtschaft bezüglich eines Datenschutzes „Made in Germany"?

Antworten auf Fragen zu wirtschaftlichen Chancen bezüglich eines Datenschutzes „Made in Germany" kann der Verfassungsschutz aus seiner Aufgabenstellung heraus nicht bewerten.

20. Wie bewerten Sie den Vorschlag, eine eigene europäische bzw. deutsche Infrastruktur für Datennetze aufzubauen bzw. durch entsprechendes Routing dafür zu sorgen, dass Datenpakete nur innerhalb eines bestimmten geografischen Raumes versandt werden (so etwa der Plan des sogenannten "Schengen-Routing"), um deutsche Unternehmen vor Abhörmaßnahmen ausländischer Geheimdienste zu schützen?

Ob eine eigene deutsche oder europäische Infrastruktur der Datennetze umfassend vor elektronischer Ausspähung durch fremde Nachrichtendienste schützt, lässt sich ohne konkrete Kenntnis der dazu geplanten technischen Lösungen und der rechtlichen Vorgaben nicht beantworten.

CDU und SPD haben in ihrem Koalitionsvertrag vom 27.11.2013 dazu Folgendes vereinbart: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft-und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings".

Es wurde außerdem in der Antwort auf Frage 5 darauf hingewiesen, dass einem fremden Nachrichtendienst vielfältige Methoden zur Verfügung stehen, um an sensible Informationen zu gelangen.

21. Als Edward Snowden Zugriff auf die jetzt veröffentlichten Geheimdokumente hatte, war er nicht bei der NSA direkt, sondern bei einem privatwirtschaftlichen Unternehmen angestellt, das als Dienstleister für die NSA arbeitet. Wie schätzen Sie die Gefahr ein, dass solche Unternehmen, die als NSA-Dienstleister Zugriff auf die NSA-Überwachungstechnologie besitzen, wirtschaftlich bedeutende Informationen anderen US-amerikanischen Unternehmen zur Verfügung stellen bzw. verkaufen könnten? Wie schätzen Sie weiterhin die Gefahr ein, dass Mitarbeiter solcher NSA-Dienstleister, die wie Edward Snowden Zugriff auf die NSA-Überwachungstechnologie besitzen, wirtschaftlich bedeutende Informationen auf eigene Rechnung verkaufen könnten?

Herr Snowden soll ein ehemaliger Mitarbeiter US-amerikanischer Nachrichtendienste sowie einer der NSA nahestehenden Beratungsfirma gewesen sein. Er soll zeitweise als Administrator gearbeitet haben. Administratoren von IT-System haben häufig uneingeschränkten Zugriff auf sämtliche Anwendungen und Daten eines IT-Systems. Die Gefahr, dass Personen diese Zugriffsrechte benutzen, um illegal in den Besitz von Daten zu kommen und diese an Dritte weitergeben, lässt sich deshalb nicht ausschließen. Das gilt unabhängig davon, ob sie dem eigenen Unternehmen angehören oder bei einer Fremdfirma beschäftigt sind. Angesichts ihrer legalen Zugangsmöglichkeiten zu IT-System und ihres Insiderwissens über innerbetriebliche Schwachstellen stellen Personen, die ihre Zugriffberechtigungen missbrauchen und zum Kreis der sogenannten Innentäter gezählt werden, eine besondere Gefahr dar.

Unabhängig von der persönlichen Motivation des Herrn Snowden sind Gründe, im Unternehmen legal erworbenes Wissen illegal weiterzugeben, häufig Unzufriedenheit am Arbeitsplatz, fehlende Identifikation mit dem Unternehmen, aber auch die eigene wirtschaftliche Bereicherung, um einen aufwändigen Lebensstil, Überschuldung oder Drogenabhängigkeit, Alkohol- oder Spielsucht zu finanzieren.

Der Verfassungsschutz empfiehlt den Unternehmen, zur Vermeidung von Schäden durch Innentäterinnen oder -täter ein umfassendes Sicherheitskonzept zu erstellen. Dazu gehört zum Beispiel:

- Erstellen einer Risiko- und Schwachstellenanalyse,

- kontinuierliche Sensibilisierung aller Unternehmensangehörigen,
- Kompetenz und Motivation der eigenen Mitarbeiter für das Sicherheits-konzept zu nutzen,
- Benennung eines Sicherheitsverantwortlichen,
- Sicherheitsregelungen für Besucher und Fremdfirmen,
- klare Unternehmensleitlinien.

Anlage

BDI | Bundesministerium des Innern | DIHK

Erklärung

„Wirtschaftsschutz in Deutschland 2015 - Vertrauen, Information, Prävention"

Das Bundesministerium des Innern (BMI) und die Spitzenorganisationen der deutschen Wirtschaft, die Bundesvereinigung der Deutschen Industrie BDI und der Deutsche Industrie- und Handelskammertag DIHK, bekunden einvernehmlich ihre Absicht, gemeinsam einen zukunftsweisenden Wirtschaftsschutz in Deutschland auszugestalten.

Der Bundesminister des Innern und die Präsidenten des BDI und des DIHK geben folgende gemeinsame Erklärung ab:

Erwägungsgründe

Der Wirtschaftsstandort Deutschland ist maßgeblich von innovativen Unternehmen und Forschungseinrichtungen gekennzeichnet. Know-how und Innovationsfähigkeit deutscher Unternehmen sind Schlüsselfaktoren der Wettbewerbsfähigkeit unserer Volkswirtschaft. Wir betrachten den Schutz dieser elementaren Ressourcen als eine Aufgabe von gesamtstaatlichem Interesse und als einen wichtigen Wettbewerbs- und Erfolgsfaktor für die deutsche Wirtschaft.

Ziel von Sicherheitsbehörden und Wirtschaft muss ein bestmöglicher Wirtschaftsschutz sein. Darunter verstehen wir die Summe aller Maßnahmen von Sicherheitsbehörden und Wirtschaft zum Schutz der deutschen Unternehmen vor Wirtschaftsspionage und Wirtschaftskriminalität.

Die vorliegende Erklärung versteht sich auch als Ergänzung zur Cyber-Sicherheitsstrategie für Deutschland, insbesondere der Allianz für Cyber-Sicherheit, an der BDI und DIHK ebenfalls beteiligt sind.

Die Aufgabe Wirtschaftsschutz erfordert ein konzertiertes Vorgehen aller Kräfte. Weder Sicherheitsbehörden noch Wirtschaftsverbände und Unternehmen können eine effektive Abwehr alleine leisten.

Wir setzen uns daher das Ziel, gemeinsam eine nationale Strategie für den Wirtschaftsschutz zu entwickeln. Die von den Sicherheitsbehörden des Bundes und die von der deutschen Wirtschaft angestoßenen Aktivitäten sollen vernetzt, abgestimmt und harmonisiert werden.

Hauptzielgruppe der Maßnahmen zum Wirtschaftsschutz werden kleine und mittelständische Unternehmen sein. Diese benötigen bei ihren Anstrengungen zum Wirtschaftsschutz besondere Unterstützung, weil ihnen dazu oftmals die notwendigen Ressourcen fehlen.

Im Vordergrund aller Maßnahmen stehen Information, Sensibilisierung sowie Prävention. Gegenseitiges Vertrauen ist hierfür eine notwendige Voraussetzung. Der offene und freiwillige Austausch über Bedrohungen soll gefördert werden.
Wir wollen den Wirtschaftsschutz durch Maßnahmen staatlichen, privatwirtschaftlichen und gemeinsamen Handelns im Rahmen einer nationalen Strategie weiterentwickeln.

Handlungsziele

Hierzu vereinbaren das BMI, der DIHK und der BDI folgende gemeinsame Handlungsziele:

- Wir wollen eine **Sicherheitsplattform** mit zentralen Ansprechpartnern der Wirtschaft und der Sicherheitsbehörden schaffen
- Wir wollen eine **Sensibilisierung in der Wirtschaft** schaffen hinsichtlich der Gefährdungslage und Risiken durch Wirtschaftsspionage und Wirtschaftskriminalität sowie der Qualität und Schutzbedürftigkeit der in ihrem Besitz befindlichen Informationen. Die Sicherheitsbehörden sollen für die spezifischen Belange der Wirtschaft in einer freiheitlich verfassten Wirtschaftsordnung sensibilisiert werden.
- Wir streben daher **eine stärkere Vertrauenskultur** durch vertrauensbildende Maßnahmen an, um die Kooperation von Sicherheitsbehörden und Wirtschaft zur Abwehr von Risiken zu befördern sowie den Informations- und Erfahrungsaustausch zu stärken.
- Wir wollen in diesem Rahmen gemeinsam zu einer **neuen Qualität des wechselseitigen Informationsaustausches** beitragen. Hierzu soll der freiwillige, risikobasierte Informationsfluss zwischen Wirtschaft und Sicherheitsbehörden verbessert werden.
- Wir halten eine **Schaffung einer gemeinsamen Internetplattform Wirtschaftsschutz** von Staat und Wirtschaft für erforderlich.
- Wir halten im **Bundesministerium des Innern** die Schaffung eines **Beauftragten für Wirtschaftsschutz** für zielführend, der zentraler Ansprechpartner des Bundesministeriums des Innern und seiner Sicherheitsbehörden für die Wirtschaft ist und die Zusammenarbeit koordiniert.

Berlin, den 28. August 2013

Der Bundesminister des Innern	Der Präsident des Bundesverbandes der Deutschen Industrie	Der Präsident des Deutschen Industrie- und Handelskammertages
Dr. Hans-Peter Friedrich	**Ulrich Grillo**	**Dr. Eric Schweitzer**