unternehmer nrw

Landesvereinigung der Unternehmensverbände Nordrhein-Westfalen e.V.

Die Landesvereinigung der Unternehmensverbände Nordrhein-Westfalen e.V. (unternehmer nrw) ist der Zusammenschluss von 129 Verbänden mit 80.000 Betrieben und drei Millionen Beschäftigten. unternehmer nrw ist Mitglied der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA) und vertritt die Interessen des Bundesverbandes der Deutschen Industrie e.V. (BDI) als dessen Landesvertretung.

STELLUNGNAHME

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 06. Februar 2014, um 12.00 Uhr, Plenarsaal

F R A G E N K A T A L O G

I. Situationsanalyse

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

Hierzu liegen uns keine Erkenntnisse vor.

2. **Ist die Sorge von Wirtschaftsspionage durch befreundete Staaten begründet?**

   In welchem Umfang Nachrichtendienste anderer Länder Daten von deutschen Unternehmen ausspähen, ist uns nicht bekannt. Das dies aber geschieht, scheint festzustehen. Dazu kommt Industriespionage durch Wettbewerber, die eine ernsthafte Bedrohung für einheimische Unternehmen darstellen.

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

   Hierzu liegen uns keine Erkenntnisse vor. Für die Bundesrepublik insgesamt geht die Bundesregierung von einem jährlichen Gesamtschaden von rund 50 Milliarden Euro aus.

4. **Welche Informationen werden nachrichtendienstlich abgeschöpft**?

   Aufgrund der hohen Dunkelziffer gibt es hierzu kaum gesicherte Erkenntnisse. Soweit Unternehmen betroffen sind, sind aber unter wirtschaftlichen Gesichtpunkten gerade Innovationen etwa bei Weltmarktführern in ihren jeweiligen Branchen von hohem Interesse, weil damit die Marktposition ganz erheblich verbessert werden kann.

5. **Welche Methoden wird sich hierbei bedient**?

   Grundsätzlich sind sowohl Fälle bekannt, in denen „konventionell" durch Personen – Eindringlinge in Unternehmen, Mitarbeiter oder Kunden – Informationen ausgespäht werden als auch Informationsgewinnung, die schwerpunktmäßig über technische Mittel (Online-Ausspähung etc.) erfolgt.

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

   Die Frage ist nicht primär an die Wirtschaft gerichtet. Gleichwohl möchten wir darauf hinweisen, dass das Innenministerium NRW als Landesverfassungsschutzbehörde eine Vielzahl von Informations- und Beratungsmöglichkeiten für Unternehmen bietet, die sehr hilfreich sind. Insbesondere der Gesichtspunkt der Vertraulichkeit bei diesen Angeboten ist für tatsächlich oder potentiell betroffene Unternehmen von elementarer Bedeutung weil das Bekanntwerden von „Sicherheitslecks" für die Unternehmen gravierende Folgen schon im Hinblick auf den Reputationsverlust haben kann.

7. **Wie ist die Aufklärungsquote?**

Die Frage ist nicht an die Vertreter der Wirtschaft gerichtet, hierzu liegen auch keine Erkenntnisse vor.

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

Weniger die Branchenzugehörigkeit ist entscheidend für die Attraktivität als „Ziel" einer Ausspähung als die konkreten Innovationen im Unternehmen. Je höher das Maß der Innovation im Unternehmen ist, desto höher das Risiko, in das Visier einer Ausspähung zu geraten.

9. Haben die Unternehmen in NRW ein ausreichendes Problembewusstsein?

Gerade größere Unternehmen beschäftigen sich regelmäßig seit längerem mit der Sicherung ihrer Betriebsgeheimnisse. Andererseits besteht vor allem bei kleineren Mittelständlern oft ein Nachholbedarf vor allem in der systematischen Erfassung der vorhandenen sicherheitsrelevanten Daten und des Umgangs damit. Hier können Beratungs- und Hilfsangebote öffentlicher Stellen eine gute Starthilfe darstellen (siehe hierzu Antwort Frage 6.).

II. Verbesserungsmöglichkeiten

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

a) Unternehmen sind in eigenem Interesse gut beraten, vor allem über ein stringentes Sicherheitskonzept zu verfügen, dass deutlich macht, wer im Unternehmen mit welchen sicherheitsrelevanten Informationen umgeht und welche Vorkehrungen gegen unbefugten Zugriff ergriffen wurden. Je nach Unternehmenstyp sind dafür unterschiedliche Sicherheitsmaßnahmen und Stufen einschlägig – hierfür gibt es keine pauschalisierten Hinweise. Wichtig in diesem Zusammenhang ist aber, ein Bewusstsein für eine echte IT-Sicherheitskultur stärker zu verankern.

b) Die Politik sollte – wie es auch aktuell auf Bundesebene erfolgt – gemeinsam mit der Wirtschaft ein „Nationales Gesamtkonzept für Wirtschaftsschutz" entwickeln. Dieses sollte beinhalten:

- Entwicklung eines gemeinsamen Grundverständnisses zu Inhalt und Umfang des Wirtschaftsschutzes bei Politik, Behörden und Industrie

- Intensivere Kooperation von Staat und Industrie bei der freiwilligen Lagebilderstellung, bei Prävention und Krisenmanagement

- Schaffung klarer rechtlicher Rahmenbedingungen für die freiwillige Kooperation und den Austausch von Staat und Industrie im Wirtschaftsschutz

- Harmonisierung gesetzlicher Sicherheitsbestimmungen zwischen den Ländern sowie zwischen den Mitgliedsstaaten der EU

- Schaffung klarer Zuständigkeiten und zentraler Ansprechpartner bei den Sicherheitsbehörden

- Ausweitung der Kapazitäten und Ressourcen staatlicher Sicherheitsbehörden zur Unterstützung der Sicherheit der deutschen Industrie

- Stärkung eines adäquaten Sicherheitsbewusstseins in Unternehmen und Gesellschaft

Dazu wäre es hilfreich, wenn ein Bundesbeauftragter für Wirtschaftsschutz als Koordinator der Sicherheitsbehörden und zentraler Ansprechpartner für die Industrie für Fragen des Wirtschaftsschutzes benannt würde.

Das Konzept sollte dabei auch offen sein für die maßgeblichen Akteure auf Länderebene und mit deren Aktivitäten abgestimmt sein.

Aus unserer Sicht werden auf Landesebene bereits eine Vielzahl von Maßnahmen ergriffen vor allem betreffend Kooperationen zwischen Behörden und Wirtschaft. Diese zu verstärken, ist beständige Aufgabe aller beteiligten Akteure.

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

Es gilt der Grundsatz: Sicherheitsschutz ist primär Aufgabe der betroffenen Unternehmen.

Hierbei können die zuständigen Behörden allerdings eine wichtige Beratungs- und Hinweisfunktion übernehmen. Von wesentlicher Bedeutung bei diesem hochsensiblen Bereich ist der Vertrauensschutz bei Gesprächen und Kontakten zwischen Unternehmen und Behörden. Vollkommen kontraproduktiv wäre daher eine Meldepflicht für betroffene Unternehmen. Dies kann dazu führen, dass Unternehmen doppelt

betroffen sind, nämlich zusätzlich zu dem erfolgten Eingriff durch drohenden Reputationsverlust.

Verstärkt werden sollte die vertrauensvolle Zusammenarbeit in freiwilligen gemeinsamen Initiativen wie der nationalen Cybersicherheitsstrategie, die unter anderem den gemeinsamen Cyber-Sicherheitsrat, die Allianz für Cybersicherheit und die Task-Force „IT-Sicherheit für die Wirtschaft“ beinhaltet.

12. Halten Sie die im Antrag aufgeführten Forderungen an die Bundesregierung für ausreichend? Wenn nein, welche Maßnahmen sollten noch auf Bundesebene ergriffen werden ?

Die Aktivitäten, die mit dem im Antrag unter II. aufgeführten Maßnahmen angeregt werden sollen, werden nach unserem Verständnis imWesentlichen bereits im Rahmen der Zuständigkeiten und Möglichkeiten von den nordrhein-westfälischen Behörden ergriffen. Weitergehende Maßnahmen, insbesondere die unter 3. b und c beschriebenen, sollten in Abstimmung mit entsprechenden Aktivitäten auf Bundesebene erfolgen.

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?

Siehe Antwort Frage 10.

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

Siehe Antwort Frage 6.

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

Siehe Antwort Frage 6.

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

Siehe Antwort Frage 6, 11. Eine Meldepflicht wird entschieden abgelehnt, weil zu dem Schaden für das Unternehmen durch den Eingriff selbst auch noch ein Reputationsschaden hinzukommen kann. Zudem würde auch die

langfristige vertrauensvolle Zusammenarbeit zwischen Behörden und Unternehmen ernsthaft geschädigt.

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 Internetdienste (Cloud-Storage, E-Mail-Provider etc.) US-amerikanischer Anbieter ein**

    Hierzu liegen uns keine konkreten Erkenntnisse vor.

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

    Zentraler Ansatz für eine Erhöhung der Sicherheit von Unternehmensdaten ist die Erstellung eines Konzepts, welche Daten des Unternehmens sicherheitsrelevant sind, wo im Unternehmen Zugriff dazugegeben ist und wie der Umgang damit stattfindet. Wie diese dann konkret geschützt werden, muss im Einzelfall beurteilt werden. Deshalb könnten technische Standards nur begrenzt die Sicherheit der Daten gewährleisten.

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

    Der deutschen IT-Wirtschaft bieten sich auf dem Feld des Datenschutzes sicherlich große Chancen.

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?**

    Es handelt sich hierbei um interessante Ansätze, die im Detail eingehend geprüft werden müssten.

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?

Die Bedrohungen, die sich aus etwaig missbräuchlichem Verhalten von ausländischen Nachrichtendiensten ergeben können, gelten natürlich ebenso hinsichtlich der von diesen beauftragten Unternehmen.