ZVEI:
Die Elektroindustrie

Positionspapier

Cyber-Sicherheit und Schutz vor Wirtschaftsspionage

November 2013

Zentralverband Elektrotechnik- und Elektronikindustrie

Cyber-Sicherheit für Wirtschaft und Gesellschaft

Cyber-Sicherheit inkl. IT-Sicherheit steht im Zuge der bekannt gewordenen Abhörprogramme PRISM und Tempora im Mittelpunkt der Öffentlichkeit. Die intensive Nutzung moderner Informationstechnologien beinhaltet neben Chancen auch signifikante Sicherheitsrisiken. Allerdings ist sowohl von Seiten der Medien als auch der Politik, ein für den Standort Deutschland, aber auch für ganz Europa, wesentlicher Aspekt weitgehend unbeachtet geblieben. Durch die massiven Ausspähprogramme besteht für Unternehmen aus besonders innovativen industriellen Branchen, wie der Elektroindustrie, die Gefahr, dass abgegriffene Daten für Industriespionage missbraucht werden. Die Stärke des Wirtschaftsstandortes Deutschland liegt maßgeblich in seiner Innovationsfähigkeit. Dieses Wissen und diese Ideen gilt es zu schützen.

Gerade im Bereich automatisierter Steuerungs- und Produktionsanlagen geben zunehmende Fallzahlen von tatsächlichen oder versuchten nicht-autorisierten Zugriffen Grund zu großer Sorge. Das Ausspähen von Daten und Schwachstellen an solchen Anlagen, das letztlich zu einer Proliferation von Informationen über diese Schwachstellen und über deren Ausnutzung führen kann, stellt eine ernstzunehmende Bedrohung für die Industrie, aber auch die gesamte Gesellschaft dar. Angriffe auf solche Einrichtungen können zu gewaltigen wirtschaftlichen und auch infrastrukturellen Schäden führen. Die Einführung von Cyber-Physical Systems in Steuerungseinrichtungen für Produktionsanlagen und Infrastruktureinrichtungen wie Stromnetzen, bedeutet auch eine erhöhte Empfindlichkeit solcher Anlagen gegenüber böswilligen Eingriffen. Um also die Chancen, die mit dem Aufkommen Cyber-Physical Systems verbunden sind, nutzen zu können, ist eine verstärkte Aufmerksamkeit gegenüber den damit verbundenen Angriffsmöglichkeiten und eine vorausschauende Sicherheitsstrategie nötig. Dies bedeutet auch, dass es verhindert werden muss, dass Informationen über Schwachstellen in Informationsnetzwerken massenhaft abgegriffen werden. Sie dürfen weder in den Händen staatlicher Institutionen noch von Privatpersonen gelangen, auf welchem Wege auch immer, denn ein Missbrauch kann nicht sicher ausgeschlossen werden und hätte möglicherweise dramatisch Folgen.

Der ZVEI lehnt daher jedwede Ausspähung von Daten entschieden ab, die nicht der ordnungsgemäßen Wahrung der Sicherheit dienen. Die Tendenz, Daten massenhaft und nicht-autorisiert zu speichern und auszuwerten, betrachtet der ZVEI mit großer Sorge.

Die Politik ist gefordert, sich den Realitäten der Vernetzung zu stellen

Zunehmende Vernetzung – Zunehmende Wirtschaftsspionage

Die modernen Informations- und Kommunikationstechnologien (IKT) sind für den Standort Deutschland eine große Chance. Sie bieten vielseitige Möglichkeiten, die Betriebsabläufe von Unternehmen effizienter werden zu lassen. Auf diese Technologien kann nicht mehr verzichtet werden. Umso mehr muss sichergestellt sein, dass Wissen, Ideen und Innovationen nicht durch Ausspähung an Wettbewerber verlorengehen.

Wirtschaftsspionage ist ein Problem, das in den letzten Jahren massiv zugenommen hat. Die Anzahl von belegten Ereignisse und Indizienfällen von Ausspähungen ist drastisch gestiegen. Zudem ist von einer hohen Dunkelziffer von nicht erkannten oder nicht gemeldeten Fällen auszugehen. Während große Unternehmen und Konzerne ihre internen Bemühungen zum Schutz vor Spionageangriffen deutlich intensiviert haben, stehen kleine und mittlere Unternehmen vor einer schwierigen Aufgabe. Für den Standort Deutschland sind die hoch-innovativen kleinen und mittleren Unternehmen aber von zentraler Bedeutung. Daher muss es der Politik ein besonderes Anliegen sein, die hiesigen Unternehmen bei ihren Bemühungen zum Schutz von Unternehmensgeheimnissen zu unterstützen.

Forderungen an die Politik

Vor diesem Hintergrund fordert der ZVEI die Umsetzung folgender Maßnahmen:

1. Nationale Ebene:

a. Die Bundesregierung muss verstärkt Personen und Unternehmen vor staatlicher wie privater Ausspähungen im In- und Ausland schützen. In beiden Fällen ist das Verhalten der jeweiligen Mitarbeiter von entscheidender Bedeutung. Daher sind Maßnahmen zur Sensibilisierung von Unternehmen für Fragen der Daten- und Kommunikationssicherheit deutlich auszuweiten. Die Allianz für Cybersicherheit ist hier ein sehr guter Ansatz und wird vom ZVEI nachdrücklich unterstützt.

b. Die Kommunikationsinfrastruktur sollte weiterentwickelt werden. Auf nationaler Ebene sollten Kommunikationswege vorgehalten werden, auf denen eine Nutzung des Internets (zum Beispiel für Cloud- oder E-Mail-Dienste) ohne Umwege über das Ausland möglich ist. Ob dies über Routinglösungen oder andere Maßnahmen gewährleistet wird, ist unerheblich. Die Politik sollte darauf achten, dass eine derartige Infrastruktur auf Grund ihrer Kritikalität für die Unternehmen diskriminierungsfrei zugänglich ist und keinem nachteiligen Geschäftsmodell Vorschub leistet.

c. Das Ausspähen von Daten ist mit Nachdruck strafrechtlich zu verfolgen. Dies schließt die Verfolgung von Unternehmen ein, die gesammelte Daten nicht gemäß gültiger Rechtsvorschriften an Dritte weitergeben.

d. Die amtlichen Zuständigkeiten bei Spionagevorfällen müssen einheitlicher strukturiert werden. Für Unternehmen ist es schwierig in der Frühphase eines Vorfalles, wenn der Täterhintergrund noch im Dunkeln liegt, Unterstützung von Amtsseite einzuholen. So liegt z. B. die Wirtschaftsspionage oft im Zuständigkeitsbereich des Verfassungsschutzes, während bei einer Ausspähung durch einen Konkurrenten gewöhnlich die Polizei hinzugezogen werden muss. Gleichzeitig muss dafür gesorgt werden, dass im Zuge der ‚Föderalisierung' der Cyber-Sicherheitsstellen auf Landesebene eine effektive Koordinierung und Einheitlichkeit gewährleistet wird.

e. Vor diesem Hintergrund begrüßt der ZVEI die Etablierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als die zentrale Anlaufstellte ausdrücklich. Seine Kapazitäten im Rahmen der Allianz für Cybersicherheit sind daher zu stärken. Im Umgang mit Meldungen ist besonders auf Vertraulichkeit zu achten. Oft sehen Unternehmen von einer Meldung ab, da sie einen Imageschaden fürchten und Prozesse noch unklar sind.

2. Europäische Ebene:

a. Es ist notwendig, einen einheitlichen europäischen Rechtsraum zu etablieren, in dem Wirtschaftsspionage konsequent verfolgt wird. Es ist festzuschreiben, dass die EU-Mitgliedsstaaten andere Mitgliedsstaaten nicht ausspionieren. Solche Handlungen widersprechen dem Geist der EU als Wertegemeinschaft. Entsprechend sollte angestrebt werden, unter den EU-Staaten ein No-Spy-Abkommen zu schließen.

b. Für eine solide Sicherung von Daten- und Kommunikationsinfrastrukturen besteht Forschungsbedarf im Bereich technischer und algorithmischer Lösungen. Im Rahmen ihrer Forschungsrahmenprogramme sollte die EU mehr in die Erforschung von Sicherheitslösungen investieren, beispielsweise über das Instrument der Public-Private-Partnerships.

c. Die Novellierung der EU-Datenschutzrichtlinie sieht der ZVEI als geboten an. Allerdings ist hierbei auf Ausgewogenheit zu achten. Ferner ist zu bedenken, dass Datenschutz nicht mit Datensicherheit gleichzusetzen ist. Die EU-Datenschutzrichtlinie ist für die Datenschutzinteressen der Wirtschaft wenig geeignet. Die aktuell von der Kommission und dem Parlament bearbeitete Richtlinie zum Schutz von Netzwerken und Informationen (NIS-Richtlinie) geht in die richtige Richtung. Weitere Maßnahmen im Sinne des Subsidiaritätsprinzips zur Unterstützung des Know-how-Schutzes in den Mitgliedsstaaten sind jedoch notwendig. Vor diesem Hintergrund ist von der EU zu fordern, die Maßnahmen unter Punkt 1 auf europäischer Ebene umzusetzen.

3. Internationale Ebene:

a. Die Europäische Union sollte auf No-Spy-Abkommen mit ihren internationalen Partnern hinwirken. Die UN sollten bemüht sein, institutionalisierte Wirtschaftsspionage international zu ächten.

b. In internationalen Wirtschaftsabkommen, sollten Datenschutz, Kommunikationsschutz, der Schutz von Patenten und Intellectual Property stets berücksichtigt werden. Die Durchsetzung von EU-Datenschutz- und Kommunikationsstandards sollte angestrebt werden.

c. Im Internet (bzw. im Darknet) existieren zahlreiche Plattformen, die gezielt Informationen über Sicherheitsschwachstellen in Netzwerken sammeln und diese kostenlos bereitstellen oder verkaufen. Ähnlich wie es bei illegalen Film- und Musik-Streamingdiensten und Tauschbörsen der Fall ist, sind diese international zu ächten und konsequent zu bekämpfen.

Sicherheit muss ganzheitlich betrachtet werden

Schaffung einer neuen Sicherheitskultur

Die grundsätzliche Verantwortung für die Know-how- und Cyber-Sicherheit liegt bei den Unternehmen selbst. Vor dem Hintergrund der 4. Industriellen Revolution und der zunehmenden autonomen Kommunikation zwischen Maschinen untereinander und Akteuren außerhalb des Unternehmens (Zulieferer, Kunden) sind die Unternehmen umso dringlicher gefordert. Ein umfassendes Sicherheitskonzept für die gesamte Industrie muss entwickelt werden. Ganzheitliche Ansätze müssen von Beginn im täglichen Unternehmensbetrieb einbezogen werden. Eine flächendeckende Nutzung von Verschlüsselungen, die technisch keinerlei Schwierigkeit darstellt, würde bereits zu einer deutlichen Verbesserung des Schutzes führen.

Sicherheit von interdependenten Kritischen Infrastrukturen zum Schutz von Gesellschaft und Wirtschaft

Systeme und Infrastrukturen werden miteinander verbunden, die früher vollkommen unabhängig voneinander existierten. Dennoch sieht die Politik die immer stärker vernetzten Infrastrukturen noch sehr sektoral auf die Bereiche Energie, Kommunikation, Transport und Gesundheit beschränkt. Künftig ist jedoch eher von wenigen bzw. einer einzigen interdependenten Infrastruktur auszugehen. Politik und Wirtschaft sind daher gefordert, neue Ansätze zu entwickeln. Das Szenario des ‚Großen Stromausfalls' verdeutlicht dies eindrücklich. Der Aufbau und die Vorhaltung von Redundanzen, der Fähigkeit des Lastabwurfs und Inselbetriebs sowie einer Art ‚Schwarzstartfähigkeit' in den Teilsektoren sind besonders relevant. Fest steht, dass der zunehmende Vernetzungsgrad kein Risiko an sich ist. Vielmehr birgt er wertvolle Entwicklungschancen für die deutsche Industrie. Der ZVEI spricht sich daher für eine ganzheitliche Betrachtung des sich gegenseitig bedingenden Wirtschafts- und Infrastrukturschutzes aus.

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Der ZVEI vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland und auf internationaler Ebene. Rund 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Sie beschäftigen rund 80 Prozent der Mitarbeiterinnen und Mitarbeiter der Elektroindustrie in Deutschland. Der ZVEI repräsentiert eine Branche mit 170 Milliarden Euro Umsatz im Jahr 2012 und mehr als 845.000 Beschäftigten. Mit den noch einmal 665.000 Mitarbeitern außerhalb Deutschlands ist die Wertschöpfung der Elektroindustrie am stärksten von allen Branchen global vernetzt.

Die Elektroindustrie ist eine der innovativsten Industriezweige Deutschland. Die Aufwendungen für Forschung und Entwicklung beliefen sich im Jahr 2012 auf 13,5 Milliarden Euro. Rund 40 Prozent des Umsatzes der Unternehmen der Elektroindustrie entfällt auf Produktneuheiten.

Mehr Informationen über den ZVEI unter www.zvei.org.

Ansprechpartner im ZVEI:

Peter Krapp
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Geschäftsführer Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main
Tel.: +49 69 6302-272
E-Mail: krapp@zvei.org
www.zvei.org

ZVEI:
Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org

www.zvei.org