Bundesamt für Verfassungsschutz

ASW
Zentralorganisation der Wirtschaft

Braucht Ihr Sicherheits-bewusstsein ein Update?

3. Sicherheitstagung des BfV und der ASW am 11. Dezember 2008 in Köln

Tagungsband

„Braucht Ihr Sicherheitsbewusstsein ein Update?“

3. Sicherheitstagung des BfV und der ASW am 11. Dezember 2008 in Köln

Tagungsband

Impressum:

Herausgeber: Bundesamt für Verfassungsschutz
Merianstraße 100
50765 Köln

Tel.: 0221-792-0
Fax: 0221-792-2915
E-Mail: poststelle@bfv.bund.de / wirtschaftsschutz@bfv.bund.de
Internet: http://www.verfassungsschutz.de

Inhaltsverzeichnis Seite

3. Sicherheitstagung des BfV und der ASW am 11. Dezember 2008 in Köln

BfV-Präsident Heinz Fromm und Vorsitzender der ASW Dr. Thomas Menk

Die 3. Sicherheitstagung des Bundesamtes für Verfassungsschutz und der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V (ASW) fand unter dem Motto „Braucht Ihr Sicherheitsbewusstsein ein Update?“ statt. Zahlreiche Vertreter deutscher Konzerne, klein- und mittelständischer Unternehmen und Wirtschaftsverbände nahmen daran teil. Fachleute aus den Sicherheitsbehörden und der Wirtschaft referierten zu verschiedenen Aspekten der Wirtschaftsspionage und des Wirtschaftsschutzes. Behandelt wurden die Themen Industriespionage, Sicherheitsmanagement in den Unternehmen und die potenziellen Auswirkungen extremistischer Bestrebungen auf die Wirtschaft.

Die Resonanz auf die Tagung war durchweg positiv. Die 4. Sicherheitstagung ist für Anfang 2010 vorgesehen.

Die gemeinsamen Sicherheitstagungen sind Teil umfangreicher Maßnahmen im Bereich der Information und Sensibilisierung durch das BfV und seines Kooperationspartners der ASW. Ziel von Prävention durch Information ist der Schutz der Unternehmen und des Wirtschaftsstandortes Deutschland. Sie sind zugleich Ausdruck einer guten Zusammenarbeit von Staat und Wirtschaft.
Denn:

„Wirtschaftsschutz ist Teamwork!“

Grußwort des Präsidenten des BfV, Heinz Fromm

Meine sehr geehrten Damen und Herren,

ich begrüße Sie herzlich zu unserer 3. Sicherheitstagung, die auch in diesem Jahr gemeinsam von der Arbeitsgemeinschaft für Sicherheit der Wirtschaft und dem Bundesamt für Verfassungsschutz durchgeführt wird.

Ich freue mich besonders darüber, dass zahlreiche Vertreter aus der Wirtschaft unter uns sind. Nur gemeinsam können wir einen erfolgreichen und möglichst umfassenden Schutz der Wirtschaft erreichen. Eine Voraussetzung hierfür ist Vertrauen. Und dieses Vertrauen soll unter anderem durch die heutige Veranstaltung weiter ausgebaut werden.

Das BfV sieht in der ASW einen verlässlichen Partner für Sicherheitsfragen. Deshalb begrüße ich den Vorsitzenden der ASW, Herrn Dr. Thomas Menk, sehr herzlich.

Mein ganz besonderer Dank gilt den Referenten aus der Wirtschaft. Herr Rafael Schenz, Chef der Konzernsicherheit Deutsche Bank AG, wird das Informationsschutzkonzept eines Global Player erläutern. Herr Christian Schaaf, Geschäftsführer von „Corporate Trust“, referiert über die Schäden, die der deutschen Wirtschaft durch die Spionage entstehen.

Vor wenigen Tagen hat das BfV sein jährliches Symposium durchgeführt. Diesmal zum Thema „Terrorismusbekämpfung in Europa. Eine Herausforderung für die Nachrichtendienste“. Unter den Referenten dort herrschte Einigkeit, dass globale Gefährdungen nur durch ein transnationales Vorgehen eingedämmt werden können. Das ist im Bereich des Wirtschaftsschutzes nicht anders.

Ministerialrat Kaller wird den Wirtschaftsschutz aus der Sicht des Bundesministerium des Innern darstellen.

Selbstverständlich werden heute auch Mitarbeiter meines Hauses referieren.

Herr Dr. Even, Abteilungsleiter Spionageabwehr, wird das Bedrohungspotenzial für Unternehmen darstellen und Herr Klingelhöller wird die Wirtschaftsspionage via Internet erläutern.
Aus einer ganz anderen Warte wird Herr Selzner die Thematik beleuchten. Er beschäftigt sich mit den Auswirkungen des politischen Extremismus auf die Wirtschaft, eine Perspektive, die zeigt, dass der Verfassungsschutz neben der Wirtschaftsspionage auch andere Bedrohungen der Unternehmen im Blickfeld hat.
Nicht zuletzt gilt mein Dank denjenigen, die unsere heutige Veranstaltung vorbereitet haben und für den reibungslosen Ablauf Sorge tragen.

Meine Damen und Herren,

eine funktionierende Wirtschaft ist eine der Grundvoraussetzungen für die innere Stabilität von Staaten. Innovation und Anpassung an neue Gegebenheiten sind die Voraussetzung für Wohlstand und sozialen Frieden.
Mit der Globalisierung der Wirtschaft hat auch das Risiko des illegalen Know-how Transfers zugenommen. Dies gilt insbesondere für deutsche Unternehmen, nicht zuletzt aufgrund ihres hohen technologischen Standards. Gefährdet sind jedoch nicht nur international tätige Konzerne, sondern auch innovative klein- und mittelständische Unternehmen.
Wirtschaftsspionage schädigt darüber hinaus in hohem Maße unsere nationalen wirtschaftlichen Strukturen und volkswirtschaftlichen Interessen insgesamt.

Wie Sie wissen, ist die Zuständigkeit des Verfassungsschutzes auf die Abwehr staatlich gelenkter oder gestützter, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung beschränkt. Hierzu zählt die Industriespionage, die Ausspähung konkurrierender Unternehmen zwar nicht, gleichwohl ist eine Unterscheidung in der Regel wegen ähnlicher Vorgehensweisen der Täter schwierig. Deshalb sind die Verfassungsschutzbehörden auch nicht daran gehindert, diese Vorgänge für Präventionszwecke methodisch auszuwerten.

Die Abwehr illegaler Ausforschung im Wirtschaftsbereich ist schwieriger geworden, nicht zuletzt auch wegen der raffinierteren Methoden der Gegenseite.
Das Internet spielt mittlerweile eine herausgehobene Rolle. Und zwar nicht nur bei der Gewinnung offen verfügbarer Informationen, sondern auch im Zusammenhang mit neuartigen Angriffs- und Ausspähungstechniken.

Ein wirkungsvoller Schutz gegen derartige Angriffe ist aufwendig, schließlich reicht ein punktuelles Vorgehen nicht aus. Stattdessen muss ein ganzheitliches Schutzkonzept entwickelt werden, eine Kombination sorgfältig abgestufter und abgestimmter Entscheidungen personeller und materieller Art. Das Bundesamt für Verfassungsschutz steht dabei als koordinierende Zentralstelle für die Lagedarstellung und den gezielten Informationsrückfluss zur Verfügung. Wir sehen in der Abwehr der Wirtschaftsspionage einen Aufgabenschwerpunkt. In diesem Zusammenhang ist das methodische Wissen über politische und militärische Spionage von hohem Wert.

Wir haben zudem strukturelle und personelle Maßnahmen getroffen, um insbesondere den Präventionsbereich auszubauen und zu verstärken. Im Rahmen der im Juli verabschiedeten „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“ arbeitet das BfV intensiv an Konzepten zur Sensibilisierung der deutschen Unternehmen. Hierzu zählen Vortragsveranstaltungen und eine intensive Öffentlichkeitsarbeit.

Wir sind uns bewusst, dass die Sicherheit der deutschen Wirtschaft nur in enger Kooperation mit den Verantwortlichen in den Unternehmen gewährleistet werden kann. Schließlich basiert die Qualität der Beratungstätigkeit in hohem Maße auf der Mitwirkung derjenigen Unternehmen, die Opfer von Wirtschaftsspionage geworden sind. Deren – selbstverständlich anonymisierten – Erfahrungen aus Schadensfällen

können dazu genutzt werden, noch nicht betroffene Unternehmen zu warnen und zu beraten.

Die heutige Sicherheitstagung soll ein weiterer Baustein für diese notwendige Kooperation sein.
Ich wünsche Ihnen interessante Vorträge und einen schönen Aufenthalt hier in Köln.

„Wirtschaftsschutz – eine Herausforderung für Staat und Wirtschaft“

Referent: Stefan Kaller, Bundesministerium des Innern

In Zeiten eines starken internationalen Wettbewerbs hängt die strategische Position eines Unternehmens vorrangig von der Innovationsgeschwindigkeit ab. Immer kürzer werden Produktzyklen, immer schneller werden Technologien durch innovativere Produkte abgelöst. Der Wettbewerb intensiviert sich im Hinblick auf Zeit und Know-how.
Zur Sicherung der Wettbewerbsposition besteht deshalb ein Interesse von Großunternehmen wie auch klein- und mittelständischen Betrieben, das eigene wirtschaftlich wertvolle „geistige Eigentum“ vor Spionage und unbefugter Verwertung durch andere Unternehmen und Nachrichtendienste ausländischer Staaten zu schützen.

In der heutigen Zeit definieren sich Staaten über ihre wirtschaftliche Stärke. Führende Industrienationen kämpfen um die wirtschaftliche Vormachtstellung in zukunftsträchtigen Schlüsseltechnologien, während Schwellenländer Anschluss an die Industriestaaten suchen. In den Medien wird oft sogar von einem „Wirtschaftskrieg“ gesprochen. Neben legalen Methoden versuchen Unternehmen und Staaten in zunehmendem Maße unter Einsatz illegaler Methoden an wichtige Unternehmensinformationen zu gelangen. Wir wissen, dass diese Art der illegalen technologischen Informationsbeschaffung gerade in der Strategie einiger Schwellenländer eine zentrale Rolle spielt. In staatskapitalistischen Ländern sind zudem die personellen Verflechtungen zwischen Staat und Wirtschaft besonders eng, sodass von einer besonders hohen Schadenswirkung auszugehen ist.

Schädigungspotenzial der Wirtschaftsspionage
Das Thema der heutigen Sicherheitstagung lautet „Braucht Ihr Sicherheitsbewusstsein ein Update?“ Diese Frage zu stellen und kritisch im Hinblick auf das eigene Unternehmen zu beantworten, kann also von entscheidender Bedeutung für ein erfolgreiches Überleben in der heute vernetzten und globalisierten Wirtschaft sein. Mögliche Verluste durch illegalen Wissenstransfer sind hoch; sie können sogar Existenz vernichtend sein. Insgesamt wird das Schadenspotenzial durch Wirtschaftsspionage in Deutschland auf ein Volumen von bis zu rund 50 Milliarden € geschätzt. Allerdings ist davon auszugehen, dass das Dunkelfeld wesentlich höher ist. Diese Dimension allein verdeutlicht ein signifikantes Phänomen!

Alle Schutz-, Abwehr- und Gegenmaßnahmen gegen die Risiken des illegalen Know-how-Abflusses können – gerade dann, wenn diese Angriffe staatlicherseits flankiert werden – nicht von einzelnen Unternehmen oder Sicherheitsbehörden abgewehrt werden. Es bedarf vielmehr der branchenübergreifenden Abstimmung und der engen Zusammenarbeit zwischen öffentlichen und privaten Akteuren. Deshalb ist Wirtschaftsschutz – d.h. alle relevanten Maßnahmen, die geeignet sind, Angriffen und Bedrohungen für die Wirtschaft aus allen Phänomenbereichen von Spionage,

Extremismus und Terrorismus rechtzeitig zu begegnen – aus Sicht des BMI eine Herausforderung für Staat und Wirtschaft gemeinsam. Wirtschaftsschutz kann nur unter Bündelung aller Kräfte wirksam geleistet werden!

Zuständigkeiten / Initiativen des Staates
Die Abwehr und Bekämpfung der Wirtschaftsspionage ist vorrangiges Ziel des BMI und seiner nachgeordneten Behörden. Das BfV, das BKA und das BSI leisten hervorragende Arbeit, um den wachsenden Gefahren zu begegnen. Speziell im BfV wurde der personelle Kräfteansatz für den Bereich Wirtschaftsspionage / Wirtschaftsschutz verbessert und die Binnenstrukturen der aktuellen Bedrohungslage angepasst, um vor allem im Analyse- und Beratungsbereich optimal agieren zu können.

Wir halten es für erforderlich, dass auch die Verfassungsschutzbehörden der Bundesländer ihre personellen wie auch sachlichen Ressourcen bündeln, um eine optimale Vernetzung herbeizuführen. Gerade die Abwehr der Wirtschaftsspionage ist eine gemeinsame Aufgabe von Bund und Ländern. Die vorgenommene Ertüchtigung des Bundesamtes für Verfassungsschutz findet damit ihre Ergänzung in der derzeit laufenden Optimierung unserer Zusammenarbeit im Verfassungsschutzverbund. Unser Ziel ist vor allem die Stärkung der operativen Kompetenzen!

Rahmenregelung
Wir haben dieses Jahr unter Federführung meines Hauses die „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“ in enger Kooperation mit der Wirtschaft fortentwickelt. Die Rahmenregelung betrifft die Zusammenarbeit staatlicher Stellen mit der Wirtschaft bei vielfältigen Fragen des Wirtschaftsschutzes, zum Beispiel vor Organisierter und politisch motivierter Kriminalität. Die jüngste Fortentwicklung der Regelung galt insbesondere Maßnahmen zur Abwehr und Bekämpfung von Wirtschaftsspionage.

Unter anderem haben wir die Mitwirkung der Wirtschaftsunternehmen neu gestaltet. Dabei übernimmt die „Arbeitsgemeinschaft für Sicherheit der Wirtschaft“ (ASW) eine hohe Verantwortung für die Bündelung und Koordinierung sicherheitsrelevanter Informationen aus der Wirtschaft an die Behörden wie auch in umgekehrter Richtung. Diese Kooperation darf keine „Einbahnstraße“ werden. Auch deshalb wird zu gegebener Zeit eine Evaluierung der Rahmenregelung durchgeführt. Selbstverständlich bleibt der Schutz personenbezogener Daten voll gewahrt.

Auch die Zahl der beteiligten Behörden, die die Sicherheitspartnerschaft zwischen Staat und Wirtschaft bilden, hat sich vergrößert. Damit wird die Netzwerkbildung voran gebracht und der Notwendigkeit zum vernetzten Handeln besser Rechnung getragen.

„Ressortkreis Wirtschaftsschutz“
Das Kernstück der staatlichen Initiativen bildet der neu gegründete „Ressortkreis Wirtschaftsschutz“. Dieser aus Vertretern verschiedener Bundesministerien und

Bundesbehörden neu eingerichtete Kreis wird unter Vorsitz des BMI künftig die Umsetzung der „Rahmenregelung für die Zusammenarbeit mit der Wirtschaft in Sicherheitsfragen“ eng begleiten und notwendige Impulse geben. Der Ressortkreis soll die Erkenntnisse der Bundesregierung bündeln und bewerten. Auch soll erreicht werden – und das ist mir ein besonderes Anliegen – dass die Vielzahl an bereits existierenden Initiativen und Projekten verschiedener Behörden auf diesem Feld zusammengefasst werden.

Im Zusammenwirken mit der Wirtschaft sollen Gegenstrategien und -maßnahmen entwickelt werden. Vor allem sollen auch die Kommunikationswege und der Austausch zwischen den Sicherheitsbehörden und der Wirtschaft in diesem Phänomenbereich weiter verstetigt und optimiert werden. Mit der Einrichtung eines Ressortkreises Wirtschaftsschutz – die konstituierende Sitzung fand am 24. September 2008 unter Teilnahme von Herrn Staatssekretär Dr. Hanning statt – gibt es auf Bundesebene erstmalig ein übergeordnetes Gremium mit dem ein unmittelbarer und stetiger Austausch über grundsätzliche Fragen im Bereich des Wirtschaftsschutzes ermöglicht wird und eine Steuerung sämtlicher Aktivitäten erfolgen kann. Damit wird ein „echter Mehrwert“ zu den bislang auf unterschiedlichsten Ebenen stattfindenden Aktivitäten erreicht. Ich denke aber auch, dass ein solcher Kreis, mit konstant personeller Besetzung, zu mehr Wirkkraft in der Zusammenarbeit führt. Der „Ressortkreis Wirtschaftsschutz“ wird künftig halbjährlich tagen; die nächste Sitzung ist für Mitte März 2009 vorgesehen.

Personal- und Erfahrungsaustausch

Mit diesem gemeinsamen Netzwerk von Staat und Wirtschaft wollen wir den Gefährdungen durch illegalen Informationsabfluss begegnen. Eine optimierte zielorientierte Zusammenarbeit wird durch persönliches Kennen lernen forciert. Wir müssen daher Personal und Methoden austauschen. Denn die Komplexität der Aufgabe, Sicherheit für die Wirtschaft zu produzieren, erfordert von den Mitarbeiterinnen und Mitarbeitern auf staatlicher wie auch privater Seite die Fähigkeit, nicht nur die eigenen Aufgaben- und Verfahrensabläufe sicher beurteilen zu können. Vielmehr müssen übergreifende Fragestellungen beherrscht werden. Damit kann sich insbesondere ein Zugewinn an Erfahrungswissen einstellen.

Ein regelmäßiger und strukturierter Personalaustausch ist schon deshalb wichtig, damit sich beide Seiten besser kennen und verstehen. Die gegenseitige Kenntnis über Zuständigkeiten, Aufgaben und Handlungsmöglichkeiten ist wichtig und erleichtert die Kommunikation. Der Personalaustausch zwischen den staatlichen Stellen und der Wirtschaft ist im Rahmen von gegenseitigen Hospitationen bereits begonnen worden. Wir können hier aber noch optimieren. Daran müssen wir weiter engagiert arbeiten. Ich möchte in diesem Zusammenhang ausdrücklich Herrn Dr. Menk danken, der diesen Prozess als Leiter der Konzernsicherheit der Daimler AG sehr positiv begleitet, insbesondere hinsichtlich der Hospitationen von Mitarbeiterinnen und Mitarbeitern des Bundesamtes für Verfassungsschutz.

Fallzahlen / Praxis

Das Gefährdungsbild durch Wirtschaftsspionage wird durch die polizeilichen Fallzahlen nicht angemessen belegt. Signifikante Fallzahlen sind beispielsweise in den vergangenen zwei Jahren nicht vorhanden. Es liegen lediglich vereinzelte Verurteilungen vor. So hat beispielsweise der 6.Senat des OLG München einen deutschen Ingenieur im Sommer 2008 wegen geheimdienstlicher Tätigkeit nach § 99 Abs. 1 Nr. 1 StGB zu einer Freiheitsstrafe von 11 Monaten verurteilt, die zur Bewährung ausgesetzt wurde. Strafmildernd wertete das Gericht dabei das umfassende Geständnis des Angeklagten, der nach seiner Verhaftung mit den Sicherheitsbehörden zusammengearbeitet hat. Insbesondere hat der Senat zu seinen Gunsten berücksichtigt, dass dieser durch seine tätige Mithilfe den Sicherheitsbehörden ermöglicht hat, einen mutmaßlichen Angehörigen des russischen Geheimdienstes festzunehmen.

Es wäre jedoch ein Trugschluss, aus fehlendem Fallaufkommen in den polizeilichen Kriminalstatistiken die Brisanz der Situation im Phänomenbereich der Wirtschaftsspionage zu verkennen. Das Erscheinungsbild und die Methoden der Wirtschaftsspionage haben sich verändert. Neben dem herkömmlichen Muster der „klassischen“ Ausforschungsmethoden gibt es eine deutliche Zunahme von Angriffen unter Einsatz von IT gestützten Attacken auf Täterseite. Auch die Nutzung der so genannten „offenen Abschöpfung“ intensiviert sich, begünstigt gerade auch durch Globalisierung und intensive Nutzung der Möglichkeiten des Internets. Immer wieder liegen Hinweise und Berichte vor, dass überwiegend im Zusammenhang mit chinesischen Staatsangehörigen Verstöße gegen das UWG – Gesetz gegen den unlauteren Wettbewerb – oder Straftatvorschriften des StGB erfolgen.

Änderungen des „Selbstverständnisses“ auf Wirtschaftsseite / Anzeigeverhalten

Ich möchte nochmals betonen, dass die zielgerichtete Zusammenarbeit zwischen Staat und Wirtschaft ein zentraler Erfolgsfaktor ist, um im internationalen Wettbewerb bestehen und die steigenden Sicherheitsherausforderungen erfolgreich meistern zu können.

Die umfassende Sensibilisierung, Beratung sowie die effiziente Abwehr nachrichtendienstlicher und anderer Angriffe auf Wirtschaftsunternehmen und Betriebe kann aber nur gelingen, wenn die Unternehmen die Sicherheitsbehörden an ihren Erfahrungen mit Verdachts- bzw. Schadensfällen teilhaben lassen. Es ist erfreulich, dass in jüngerer Zeit ein gewisser Bewusstseinswandel zu verzeichnen ist. Ich will aber auch nicht verhehlen, dass es hier aus unserer Sicht noch entscheidenden Verbesserungsbedarf gibt! Wenn Wirtschaftsspionageangriffe den Sicherheitsbehörden nicht bekannt werden, entsteht kein geeignetes Lagebild und es können nur weniger zielgerichtete Maßnahmen zum Schutz der Wirtschaft eingeleitet werden. Das hohe Dunkelfeld wird zudem nicht weiter aufgeklärt. Ich appelliere deshalb an die Vertreter der Wirtschaftsunternehmen, Fälle von Wirtschaftsspionage und Konkurrenzausspähung zur Anzeige zu bringen. Je mehr wir über Verdachtsfälle, Straftaten, Täterstrukturen und - verhalten im Bereich des „illegalen

Informationsabflusses“ wissen, desto zielgenauer können wir eine grundlegende Abwehrstruktur und konkrete Gegenmaßnahmen für den Einzelfall entwickeln.

Die weit verbreitete Sorge vor dem Imageschaden oder Reputationsverlust dürfte eine maßgebliche Ursache für dieses Verhalten der Wirtschaft sein. Auch wenn wir diese Beweggründe natürlich respektieren, können wir den Unternehmen strikte Vertraulichkeit seitens der Verfassungsschutzbehörden zusichern. Bei der Erfüllung der Aufgabe der Wirtschaftsspionageabwehr unterliegen diese nicht dem Legalitätsprinzip, sondern für sie gilt das Opportunitätsprinzip. Das bedeutet, dass eingetretene Schadensfälle in der Wirtschaft sachgerecht aufgeklärt werden und nicht wie bei Maßnahmen der Strafverfolgung zugleich in die Öffentlichkeit gelangen. Genau dieser Aspekt erleichtert den Verfassungsschutzbehörden den Austausch und die Beratung der Wirtschaft! Kein Unternehmen, das sich wegen möglicher Ausforschungen an die Spionageabwehr wendet, muss befürchten, dass die zur Verfügung gestellten Informationen ohne Einverständnis publik gemacht werden und sich unter Umständen nachteilig auf das Unternehmensimage auswirken. Im Gegenteil – die Wirtschaft findet vertrauensvolle Ansprech- und Beratungspartner bei den Verfassungsschutzbehörden von Bund und Ländern.

Aufgabe der Wirtschaft ist es nunmehr, den „Teufelskreis“ aus Gefährdung, Informationsdefizit und Abschottung beim Schadenseintritt zu durchbrechen! Die engere Kooperation der Wirtschaft mit den Sicherheitsbehörden ist letztlich der Schlüssel, die Wirtschaftsspionage erfolgreich einzudämmen.

Prävention bei Wirtschaft und Staat

In erster Linie muss der Schutz vor Wirtschaftsspionage (Know-how-Schutz) in den Unternehmen seinen Anfang nehmen. Gegenmaßnahmen gestalten sich bei kleinen Unternehmen anders als bei Großunternehmen. Nach Ermittlung der Schutzbedürftigkeit, vor allem durch eine grundlegende Analyse der Bedrohungsszenarien und der Schwachstellen des Unternehmens mit anschließender Risikobewertung, muss ein entsprechendes Informations- und Sicherheitskonzept möglichst individuell entwickelt werden. Dieses sollte insbesondere die Aspekte von personellen, organisatorischen und technischen Maßnahmen umfassen. In den sog. Geheimschutz betreuten Unternehmen z.B. im Bereich der Verteidigungsindustrie liegen solche Konzepte umfassend vor. Diese wurden teilweise mit Hilfe der Verfassungsschutzbehörden erstellt. Gerade in kleinen und mittleren Betrieben fehlen diese jedoch häufig, obwohl gerade die dort geleistete innovative Forschungs- und Entwicklungsarbeit von besonderem Interesse für Konkurrenten respektive für fremde Nachrichtendienste sein kann.

Vor allem auch die Verfassungsschutzbehörden leisten mit ihrer präventiv ausgerichteten Arbeit im Bereich der Abwehr von Wirtschaftsspionage bzw. des Wirtschaftsschutzes „klassische Prävention“ einschließlich der notwendigen „Sensibilisierung“. Sämtliche Präventionsmaßnahmen auf staatlicher wie auch privater

Seite müssen aber auch regelmäßig und umfassend auf ihre Wirkkraft überprüft und ggf. neu justiert werden. Die heutige Veranstaltung ist Teil dieser Daueraufgabe!

Konzept einer öffentlich-privaten Sicherheitspartnerschaft
Die Ausspähungsmöglichkeiten in einer zunehmend global vernetzten Gesellschaft sind vielschichtiger geworden und bieten neue Ansatzpunkte für Spionageaktivitäten, insbesondere in der Wirtschaft.

Diese Entwicklung erfordert letztlich eine konzeptionelle Neuorientierung der Sicherheitspartnerschaft von Staat und Wirtschaft. Angesichts der bestehenden Gefährdungslage ist eine vertrauensvolle öffentlich-private Sicherheitspartnerschaft weiter auszubauen. Sie ist eine beiderseitige Strategie, Mangel an Ressourcen und Zugang zu Wissen im Sicherheitsbereich zu überwinden.

Außerdem bin ich davon überzeugt, dass sie zu einem zentralen Wettbewerbs- und Erfolgsfaktor für den Wirtschaftsstandort Deutschland führen wird. Wir brauchen ein Wissens- und Informationsnetzwerk – nicht nur zwischen den Sicherheitsbehörden, sondern auch zwischen Staat und Wirtschaft. Der bedarfsgerechte Informationsaustausch im Phänomenbereich Wirtschaftsspionage ist daher weiter auszubauen. Nur so wird es auf längere Sicht gelingen, „unfreundliche Informationsabflüsse“ einzudämmen und zu verhindern.

Für die Umsetzung viele dieser Dinge werden wir – auch das möchte ich nicht verschweigen – Ausdauer brauchen. Aber im Sinne des gemeinsamen Anliegens, die deutsche Wirtschaft umfassend zu schützen, wird sich dies lohnen!

Die Entwicklungen hin zu einer öffentlich-privaten Sicherheitspartnerschaft schreiten in Deutschland langsamer als im Ausland voran. Man denke nur an die Diskussion über die Gefahr einer Erosion des staatlichen Gewaltmonopols hinsichtlich des Aufwachsens von privaten Sicherheitsunternehmen in Deutschland. Daher ist ein Blick über die eigenen Grenzen stets von Nutzen, um Anregungen im Sinne von bestpractice zu erhalten.

Fazit / Schluss
Die Abwehr von Wirtschaftsspionage und damit einhergehender Phänomenbereiche ist eine gemeinsame Herausforderung für Staat und Wirtschaft! Der wirtschaftliche Erfolg der Exportnation Deutschland beruht auf Innovation und Wissensvorsprung seiner zahlreichen international tätigen Unternehmen. Gerade auch die Sicherheitsinteressen des Mittelstandes in Deutschland spielen eine große Rolle. Denn Dienstleistungs- und Wissensgesellschaften schöpfen ihre wirtschaftliche Kraft aus der Leistungsfähigkeit des Mittelstandes.

Wir müssen deshalb in besonderer Weise dafür Sorge tragen, dass es fremden Nachrichtendiensten, aber auch konkurrierenden Wirtschaftsunternehmen nicht gelingt,

mit illegalen Methoden das technologische Kernwissen und die -kompetenzen dieser Unternehmen abzuschöpfen und damit die deutsche Wirtschaft in ihrer Gesamtheit zu schädigen. Sicherheit in der Wirtschaft – gerade auch Schutz vor illegalem Know-how-Abzug – wird immer mehr zu einem entscheidenden Wettbewerbsfaktor.

„Wirtschaftsspionage – Bedrohungspotenzial für die Unternehmen“

Referent: Dr. Burkhard Even, Bundesamt für Verfassungsschutz

Die Bundesrepublik Deutschland ist wegen ihrer geopolitischen Lage in Europa, ihrer wichtigen Rolle in EU und NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie mit Weltmarktführung für fremde Nachrichtendienste sehr attraktiv. Die Globalisierung der Weltwirtschaft hat dazu geführt, dass neben großen Konzernen auch viele innovative klein- und mittelständische Unternehmen zur Erhaltung ihrer Wettbewerbsfähigkeit auf dem Weltmarkt präsent sein müssen. In diesem Kontext haben sich aber auch die Risiken im In- und Ausland erheblich vergrößert.

Bestimmendes Kriterium für den Erfolg im Wettbewerb von Staaten und Unternehmen ist das Streben nach einem Wissensvorsprung. Dieser Wissensvorsprung ist aber regelmäßig nur durch den Einsatz erheblicher finanzieller Mittel und personeller Ressourcen erreichbar. Durch Spionage und andere illegale Methoden ist dieses Ziel ungleich kostengünstiger zu erlangen.

Der Forschungs- und Industriestandort Deutschland steht daher seit Jahren im Fokus fremder Nachrichtendienste und konkurrierender ausländischer Unternehmen. Im Zusammenhang mit dem immer stärker werdenden globalen Verdrängungswettbewerb sind insbesondere die hoch innovativen Wirtschaftsunternehmen der Bundesrepublik einem harten Konkurrenzkampf ausgesetzt, der auch mit illegalen Mitteln ausgetragen wird.

Wer sind heute die Akteure und Hauptauftraggeber?
Nach Erkenntnissen des BfV sind seit Jahren die Nachrichten- und Sicherheitsdienste der Russischen Föderation und der Volksrepublik China die Hauptträger von Spionageaktivitäten in Deutschland, das gilt auch für den Bereich der Wirtschaftsspionage.
Ich möchte zunächst auf die Rolle der russischen Nachrichtendienste eingehen.

Die russischen Nachrichtendienste
Als fester Bestandteil der nationalen Sicherheitsstruktur und als Ausführungsorgane der staatlichen Auslandsaufklärung genießen die Dienste hohes Ansehen und Rückhalt bei der politischen Führung. Sie sollen die Erfüllung politischer Vorgaben gewährleisten sowie die politischen und wirtschaftlichen Interessen Russlands fördern.

Im wesentlichen sind drei Nachrichtendienste Russlands im Bereich Wirtschaftsspionage aktiv.
Dies sind:
- der SWR, dem die zivile Auslandsaufklärung in den Bereichen Politik, Wirtschaft sowie Wissenschaft und Technologie obliegt,

- die GRU, zuständig für die militärische Auslandsaufklärung einschließlich militärisch nutzbarer Technologien und
- der FSB, der zivile und militärische Abwehrdienst.

Unter wirtschaftlichen Aspekten arbeitet der FSB heute mit ausdrücklicher Unterstützung der Russischen Regierung im wesentlichen in zwei Richtungen und zwar ist

→ der Dienst an kommerziellen Tätigkeiten unterschiedlicher Art beteiligt
→ und er übt eine nachrichtendienstliche Kontrolle über Wirtschaftsstrukturen in Russland aus.

Der Schutz der Wirtschaft sowie des wissenschaftlichen und technischen Potenzials gehört zu den Hauptaufgaben des FSB. Darunter fällt auch die Kontrolle ausländischer Joint-Venture-Partner.

Bei der Vorbereitung von Wirtschaftsverträgen mit ausländischen Partnern ist immer eine Abstimmung mit der FSB-Verwaltung erforderlich. Dabei bietet sich eine hervorragende Möglichkeit, weitreichende Kontrolle über ausländische Investoren und mögliche Geschäftspartner auszuüben.

Im Rahmen seiner Abwehraktivitäten in Russland betreibt der FSB eine intensive Internetüberwachung. Zu diesem Zweck müssen alle russischen Anbieter von Internetzugängen dem FSB einen ständigen Zugriff auf den Datenverkehr ermöglichen, der in oder über Russland abgewickelt wird. Auch die Telefongesellschaften des Landes sind verpflichtet, dem FSB einen permanenten Zugang zu Informationen über Telefonkunden und deren Ferngespräche zu gewähren. Dadurch erhält der FSB die Möglichkeit, telefonische Kontakte, deren Intensität sowie den Aufenthalt der Gesprächsteilnehmer zum Zeitpunkt der Telefonate festzustellen. Daher müssen auch ausländische Staatsangehörige in Russland damit rechnen, bei der Nutzung des Internet oder durch Telefongespräche in das Blickfeld des FSB zu geraten und gezielt geheimdienstlich überwacht zu werden.

Die im Oktober 2007 erfolgte Ernennung des früheren russischen Ministerpräsidenten und ausgewiesenen Wirtschaftsfachmanns Fradkow zum neuen Leiter der Auslandsaufklärung SWR lässt den Schluss zu, dass der Dienst seine Aktivitäten im Bereich Wirtschaftsspionage weiter verstärken soll. Gestützt wird diese Annahme durch eine Äußerung des damaligen Präsidenten Putin anlässlich der offiziellen Amtseinführung Fradkows, wonach eine Aufgabe der Auslandsaufklärung darin bestehe, den Wandel der weltweiten Wirtschaftskonjunktur frühzeitig zu erkennen und dessen Auswirkungen auf das heimische Industrie- und Verteidigungspotenzial abzuschätzen. Auch müsse der SWR die Interessen der russischen Unternehmen im Ausland verstärkt schützen.

Auch der frühere Leiter des SWR Lebedew hatte in mehreren Interviews den volkswirtschaftlichen Wert offensiver Wirtschaftsspionage beschrieben.

Er bezeichnete die Informationen aus der Aufklärung an sich schon als unbezahlbar. So hätten wissenschaftlich-technische Informationen und Know-how einen Effekt, den man in Ziffern mit vielen Nullen messen müsse. Er bemerkte weiter, dass die vom Nachrichtendienst im Ausland gewonnenen Informationen auch der Wirtschaft und Wissenschaft in Russland zur Verfügung gestellt werden.

Die Spionageabwehr stellt entsprechend intensive Bemühungen russischer Nachrichtendienste fest, auf offenen und geheimen Wegen Informationen aus Politik, Militär, und verstärkt auch aus Wirtschaft und Wissenschaft zu gewinnen.

Ein Beleg dafür ist der Spionagefall um einen ehemaligen Ingenieur des EADS-Konzerns, der im Juni 2008 wegen geheimdienstlicher Tätigkeiten zu einer Freiheitsstrafe verurteilt wurde. Ihm konnte nachgewiesen werden, Unterlagen über zivile Hubschrauber an einen russischen Agenten geliefert zu haben. Vor einer höheren Strafe bewahrte ihn insbesondere seine Weigerung, auch Materialien über militärische Hubschrauber zu beschaffen.

Die Nachrichtendienste der Volksrepublik China.
Die VR China ist auf dem Wege zur führenden Wirtschaftsmacht. In wichtigen Sparten ist China mittlerweile der weltgrößte Produzent. China gehört zu den weltweit führenden Exporteuren von Informationstechnologie, darunter Notebooks, PCs, Handys und digitale Kameras. Der chinesische Mobilfunkmarkt ist der weltweit Größte. China kauft sich in westliche Unternehmen ein oder übernimmt sie ganz, um so in den Besitz fortschrittlicher Technologien und des Marketingnetzes zu gelangen.

Diese Entwicklung ist kein Zufall, sie verläuft vielmehr nach einem strikten Plan auf der Basis der wirtschaftlichen Ordnung des Landes aufgestellt vor 30 Jahren durch Deng Xiaoping. Die chinesischen Nachrichten- und Sicherheitsdienste haben mit ihren speziellen Instrumenten und Möglichkeiten das strategische Vorhaben – zügig die Technologielücke zu den hochentwickelten Industriestaaten zu schließen – umfassend zu unterstützen.

Spätestens seit dem Beitritt der Volksrepublik China zur Welthandelsorganisation WTO 2001 hat eine neue Phase der Wirtschaftsexpansion begonnen. Es geht um die endgültige Platzierung als Wirtschaftsmacht ersten Ranges bis 2020. Dieses ehrgeizige Ziel wird nur mit massivem – auch illegalem – Transfer von Spitzentechnologie aus den hoch entwickelten Industriestaaten zu meistern sein.

Das MSS – Ministerium für Staatssicherheit – überwacht u.a. auch die im eigenen Land lebenden Ausländer, einschließlich der Angehörigen diplomatischer Vertretungen.

Das MÖS – Ministerium für Öffentliche Sicherheit – ist die nationale Polizeibehörde der VR China mit einem breitgefächerten Aufgabenspektrum im Bereich der öffentlichen Sicherheit und Ordnung sowie der Bekämpfung von Korruption und organisierter Kriminalität.

Das MID – Military Intelligence Department – ist traditionell für die nachrichtendienstliche Aufklärung mit menschlichen Quellen (HUMINT) im Ausland zuständig.

Hauptaufgabe des MID ist das Beschaffen von jeglichen Informationen mit militärischem Bezug. Besonders interessieren Informationen, die für die Modernisierung der chinesischen Militär- und Rüstungstechnik benötigt werden.

Die neu gegründete Internetpolizei ist eine Zivilbehörde mit weitreichenden Exekutivbefugnissen, die nicht nur den „normalen“ Internet-User sondern auch die Provider scharf kontrolliert.

Deutschlands Stellung in der Welt beruht primär auf seiner wirtschaftlichen Leistungskraft und dem hohen Niveau von Forschung und Technik. Die Leistungsfähigkeit der deutschen Wirtschaft wird durch verschiedene Faktoren bedroht. Dazu zählen insbesondere auch Wirtschaftsspionage und Konkurrenzausspähung.

Die Verfassungsschutzbehörden bezeichnen mit dem Begriff Wirtschaftsspionage die Ausforschung von Wirtschaftsunternehmen und Betrieben durch Nachrichtendienste fremder Staaten. Im Gegensatz dazu ist Konkurrenzausspähung, oft auch als Konkurrenzspionage bezeichnet, die Ausforschung durch ein konkurrierendes Unternehmen. Für letzteres ist der Verfassungsschutz zwar nicht zuständig. In der Praxis wirkt sich das allerdings oft nicht aus, da wir zumindest solange tätig werden können, wie der nachrichtendienstliche Hintergrund nicht definitiv ausgeschlossen ist.

Die zum klassischen Aufgabenbereich fremder Nachrichtendienste gehörende Wirtschaftsspionage gewinnt im Rahmen des globalen Ringens um Marktanteile immer mehr an Bedeutung. Wirtschaftsspionage schädigt nicht nur nationale wirtschaftliche Strukturen, sie vernichtet darüber hinaus auch Arbeitsplätze. Von daher ist es eine zentrale Aufgabe der Spionageabwehr über die Gefahren durch Wirtschaftsspionage aufzuklären, Beratung anzubieten und zu leisten und operative Abwehrmaßnahmen durchzuführen.

Die gegnerische Informationsbeschaffung vollzieht sich nicht nach einheitlichen Regeln. Fremde Staaten betreiben sie in Abhängigkeit von ihren spezifischen Bedürfnissen und Möglichkeiten.

So richtet sich das Interesse hochindustrialisierter Länder eher – aber nicht nur – auf den strategischen Bereich, d.h. auf die wirtschaftliche Infrastruktur der Bundesrepublik im ganzen, auf energiewirtschaftliche Informationen sowie auf Unternehmens-, Wettbewerbs- und Marktstrategien. Aber auch Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen sind in diesem Zusammenhang Aufklärungsziele, genauso wie Informationen über firmeninterne Entscheidungsprozesse.

In technologisch weniger entwickelten Staaten (Schwellenländer) basiert wirtschaftliches Wachstum vor allem auf arbeitsintensiver Produktion sowie der Förderung und Verarbeitung von Rohstoffen. Technologisches Wissen wird meistens importiert, entweder über Güter und Dienstleistungen oder durch Direktinvestitionen ausländischer Unternehmen. Fortschritt basiert in diesen Ländern oftmals nicht auf eigenen Innovationen, sondern auf Modifikation und Imitation. Diese Länder versuchen vor allem, sich technisches Know-how zu beschaffen, um Kosten für eigene Entwicklungen oder Lizenzgebühren zu sparen.

Wesentliche Ausspähungsziele sind zukunftssichernde und strategisch bedeutsame Technologien. Neben der Rüstungstechnologie sind insbesondere die Technologiebereiche aus Umwelt und Energie, fast alle Sparten der elektronischen und chemischen Industrie und der Maschinen- und Anlagenbau in allen seinen Facetten betroffen.

Für den illegalen Wissensabfluss gibt es vielfältige Ansatzpunkte. Die Informationsbeschaffung erfolgt sowohl durch den Einsatz klassischer Agenten als auch durch so genannte Non-Professionals, also Studenten, Gastwissenschaftler und Praktikanten aus anderen Staaten, die sich zu Studien- oder Ausbildungszwecken zeitweilig in Deutschland aufhalten und die sich ihren Heimatländern ganz besonders verpflichtet fühlen. Insbesondere chinesische Nachrichtendienste bedienen sich dieser Beschaffungsmethode.

Neben dem Einsatz menschlicher Quellen gewinnt die technische Informationsbeschaffung deutlich an Bedeutung. Die aktuell wohl gefährlichste Bedrohung stellen internetgebundene Angriffe auf Netzwerke und Computersysteme von Wirtschaftsunternehmen, Forschungseinrichtungen und Regierungsstellen dar.

Die „Global Player“ unter den deutschen Unternehmen sind sich der Gefahren der Ausspähung durch fremde Nachrichtendienste oder Konkurrenten meistens bewusst. Ihre Sicherheitsabteilungen haben Konzepte und Programme entwickelt, um bereits vor Eintritt eines Schadensfalles erfolgreich gegensteuern zu können. Kleinen und mittleren Unternehmen fehlen dagegen sehr oft die Erfahrungen sowie die personellen und finanziellen Ressourcen, um auf Bedrohungen entsprechend zu reagieren.

Die Gefährdungssituation in Deutschland ist vielfältig
Mögliche Einfallstore für eine Ausspähung können sein:
- Joint Ventures mit ausländischen Firmen
- Partnerschaften von Institutionen, Forschungseinrichtungen, Regionen und Städten
- Delegationen bei Messen und Firmenbesuchen
- Elektronische Angriffe über das Internet
- eigene Mitarbeiter

Im Bereich der chinesischen – wie auch der russischen – Nachrichtendienste stellen die diplomatischen Vertretungen und die Agenturen von Medien in Deutschland eine bekannte Plattform für Spionage dar. Gleiches gilt auch für die russischen Nachrichtendienste. Als Diplomaten oder Journalisten getarnt werden sie von ihren deutschen Kontaktpersonen kaum als Angehörige eines Nachrichtendienstes wahrgenommen und können so ihr Interesse an sensiblen Informationen unauffällig mit ihrer offiziellen Funktion begründen.

Sie halten gezielt und geschickt Kontakte zu wichtigen Informationsträgern in Verbänden, wissenschaftlichen Instituten, zu Unternehmen und anderen Einrichtungen. Sie besuchen Messen, Fachveranstaltungen, um dort Kontakt zu interessanten Personen aufzunehmen. Durch wiederholte Einladungen werden die Kontakte zielstrebig ausgebaut und durch kleine Gefälligkeiten gefestigt. Es entsteht somit eine aus dem Gedanken der Freundschaft heraus verpflichtende Beziehung, bei dem die verdeckt arbeitenden Nachrichtendienstler ihre Gesprächspartner über ihre wahren Absichten im Unklaren lassen.

Schlüsseltechnologien und Grundlagenforschung stehen im besonderen Aufklärungsinteresse der chinesischen Nachrichtendienste. Beschafft werden Know-how und High-End-Produkte auf breiter Front – nach dem Staubsaugerprinzip – auf allen staatlichen und privaten Ebenen durch legales aber auch illegales Handeln. Die Steuerung und Koordinierung der Beschaffungsaufträge erfolgt in China über die Staatskommission für Wissenschaft und Technik. Eine beabsichtigte Maßnahme kann in beliebige Teilaufträge gegliedert und auch durch Personen, die nicht dem Nachrichtendienst zugehörig sind, ausgeführt werden, z.B. die von mir bereits erwähnten Non-Professionals.

Auch wenn sich daraus kein Generalverdacht gegen alle chinesischen Mitarbeiter in deutschen Unternehmen und Forschungsanstalten ableiten lässt, gibt es doch zahlreiche Hinweise aus Wirtschaft und Forschung auf auffälliges Verhalten von Personen dieses Kreises, das jeweils in einen ungewollten, nicht autorisierten Know-how-Abfluss nach China münden kann.

So musste im Sommer 2008 ein Maschinenbauunternehmen in Süddeutschland feststellen, dass ein aus China stammender Konstruktionstechniker sich in größerem Umfang Firmenunterlagen, die nicht aus seinem Arbeitsbereich stammten, elektronisch

verschafft hatte. Wiederholt war er während seiner mehrjährigen Anstellung nach China gereist. Nach Bekannt werden dieses Vorfalls erschien der Mitarbeiter nicht mehr an seinem Arbeitsplatz, sein Aufenthalt ließ sich nicht mehr ermitteln.

Ein anderer Fall möglicher chinesischer Wirtschaftsspionage betrifft eine Firma, die im Maschinen- und Anlagenbau weltweit tätig ist. Zusammen mit einer chinesischen Firma wurde in den späten 90er Jahren ein Joint-Venture gegründet. Vor zwei Jahren wurde die Firma durch ein Landesamt für Verfassungsschutz sensibilisiert. Hierbei wurde u.a. festgestellt, dass die Firma kein eigenes IT-Schutzkonzept besaß.
In diesem Zusammenhang überprüfte das Unternehmen auch den E-Mail-Verkehr einer chinesischen Mitarbeiterin. Dabei wurde festgestellt, dass diese umfangreiche Firmendaten (Preiskalkulationen, Betriebsanleitungen, Konstruktionszeichnungen u.v.m) von ihrem Firmen E-Mail-Account an zwei E-Mail-Adressen weiterleitete, wobei eine Adresse den Anschein hatte, als sei es eine offizielle E-Mail-Adresse des Unternehmens. Dem IT-Administrator der Firma war diese jedoch nicht bekannt.

Obwohl ein nachrichtendienstlicher Hintergrund sich in solchen Fällen meistens nicht nachweisen lässt, zeigen die Sachverhalte exemplarisch die Notwendigkeit präventiver Maßnahmen zum Schutz vor unerwünschtem Know-how-Klau.

Dem fundamentalen Sicherheitsgedanken „Kenntnis nur wenn nötig“ wird offenbar allzu oft nicht genug Beachtung geschenkt.

China hat in den letzten zwei Jahrzehnten verschiedene umfassende Entwicklungsprogramme aufgestellt, die der Intensivierung des Technologie- und Wissenstransfers nach China zum Ziel haben. Dazu gehört u.a. ein Programm zur Unterstützung der Rückkehr von im Ausland ausgebildeten Fachleuten. Dieses Programm bezweckt die Förderung chinesischer Fachleute mit dem Ziel der Modernisierung des Landes und der Erreichung internationaler Standards.

Die Entwicklung neuer Werkstoffe wird von China im Hinblick auf die vielfältigen wichtigen Anwendungsbereiche wie beispielsweise Automobilbau, Luft- und Raumfahrttechnik und Kraftwerksbau gefördert.

Den deutschen Unternehmen, die in der Volksrepublik China investieren, müssen die damit zusammenhängenden Risiken der nachrichtendienstlichen Ausspähung bewusst sein.

Der Verfassungsschutz wird deswegen auch zukünftig auf die Firmen zugehen, die bekanntermaßen das Ziel von Angriffen waren oder sind. Nach unserer Erfahrung ist das ein für beide Seiten sinnvoller Weg, da dann auch in die Tiefe gehende Sachverhalte angesprochen sowie das Ausspähungsziel und der potenzielle Angreifer eingegrenzt werden können.

Umgekehrt ist es unabdingbar, dass sich Unternehmen, die von ungewollten Technologieabfluss betroffen sind, an den Verfassungsschutz wenden.

Das Bundesamt und die Verfassungsschutzbehörden der Länder stehen als kompetente Ansprechpartner für Beratung und Abwehrmaßnahmen zur Verfügung.

Nachrichtendienste westlicher Länder
In den Medien wird zuweilen berichtet, dass auch westliche Industrienationen Wirtschaftsspionage gegen Deutschland betreiben könnten.

Dazu ist anzumerken, dass dem BfV zur Zeit keine konkreten Anhaltspunkte für eine systematische Wirtschaftsspionage anderer Länder gegen Deutschland vorliegen. Das ist aber kein Grund zur Entwarnung, weil zumindest die Gefahr von Ausspähung durch andere Unternehmen (also Konkurrenzausspähung) sehr real ist und deshalb die gleichen Schutzvorkehrungen angezeigt sind.

Handlungsoptionen des Bundesamtes für Verfassungsschutz zum Schutz des Wirtschaftsstandortes Deutschland
Wirtschaftsspionage und Konkurrenzausspähung können für die Unternehmen gleichermaßen existenzbedrohend sein.

Die Ausgangssituation für beide Arten von Ausspähung ist nahezu identisch. Unternehmen produzieren Güter und Dienstleistungen, die sie am Markt anbieten und von deren Verkauf sie angemessene Erträge für das investierte Kapital erwarten. Dabei stehen sie in einer stetigen Konkurrenz mit anderen Unternehmen. Wirtschaftlicher Erfolg und präventives Sicherheitsmanagement, also der präventive Schutz der substantiellen Werte eines Unternehmens, sind deshalb in einem engen Zusammenhang zu sehen.

Die Bundesregierung und das Bundesamt für Verfassungsschutz (BfV) räumen dem Schutz der Wirtschaft einen hohen Stellenwert ein.

Die überarbeitete Rahmenregelung ist die Basis der Kooperation zwischen der „Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW)“, dem BfV und anderen staatlichen Institutionen.

So übermittelt das BfV der ASW fortlaufend Beiträge, die für die Sicherheit der Wirtschaft relevant sind und stellt Analysen, Referenten und Hilfsmittel zur Verfügung. Besonders wichtig sind auch gemeinsame Veranstaltungen zu unterschiedlichen Themenschwerpunkten. Die heutige Veranstaltung ist ein gutes Beispiel dafür.

Im Bundesamt für Verfassungsschutz sind die Ressourcen in der Spionageabwehr, die

sich qua gesetzlichem Auftrag mit der Abwehr von Wirtschaftsspionage befasst, durch ein eigenständiges Referat verstärkt worden, um insbesondere die Analyse- und Beratungstätigkeit weiter zu optimieren.

Darüber hinaus haben wir den bisherigen Aufgabenkatalog im Bereich des Wirtschaftsschutzes erweitert.

Bislang standen die
- Analyse und methodische Aufarbeitung nachrichtendienstlicher Sachverhalte und präventiver Aspekte,
- die Herausgabe von Informationsschriften und
- eine umfangreiche Vortragstätigkeit bei einschlägigen Veranstaltungen im Mittelpunkt.

Dieses breite Informationsangebot wurde ergänzt durch eine erheblich gesteigerte Internetpräsenz zu den Themen Wirtschaftsspionage und Wirtschaftsschutz. Unser Newsletter unterrichtet zeitnah über aktuell bekannt gewordene neue Gefahrenmomente. Daneben wird an dem Aufbau eines Infoboards (mit Zugangsberechtigung) gearbeitet, auf dem geschützte Informationen mit Unternehmen der geheimschutzbetreuten Industrie ausgetauscht werden sollen.

Gerade die Erarbeitung von wirksamen Sensibilisierungskonzepten verlangten nach einem engen Schulterschluss zwischen den Wirtschaftsunternehmen und den sie vertretenden Organisationen und Verbänden und dem Bundesamt für Verfassungsschutz.

Erwähnen möchte ich auch in diesem Zusammenhang unser Hospitationsprogramm, in dessen Rahmen Mitarbeiter des Bundesamtes die Arbeitsweise der Sicherheitsabteilungen in Firmen kennen lernen. Es trägt maßgeblich zum besseren Verständnis der jeweiligen Aufgaben und Probleme bei.

Der Schwerpunkt unseres Konzeptes beruht im wesentlichen auf dem Gedanken der „Prävention durch Information“.

Alleine in diesem Jahr konnten wir in zahlreichen Vorträgen, Sensibilisierungs- und Informationsgesprächen Interessierte aus den Unternehmen und Wirtschaftsverbänden erreichen. Sowohl die durchweg positive Resonanz als auch die rege Nachfrage nach unserem „Service“ zeigt uns, dass wir den richtigen Weg gehen und damit einen konstruktiven Beitrag zum Wirtschaftsschutz leisten.

Die Qualität der Beratungstätigkeit durch den Verfassungsschutz basiert allerdings in starkem Maße auf der Mitwirkung der durch Wirtschaftsspionage betroffenen Unternehmen. Die Erfahrungen aus Schadensfällen müssen genutzt werden, um künftige Fälle zu verhindern.

Dabei legen wir besonderen Wert auf den Quellenschutz. Keine Firma, die sich wegen möglicher Verdachtsfälle an die Spionageabwehr wendet, muss befürchten, dass diese ohne ihr Wissen und Wollen publik und sie „als Opfer an den Pranger“ gestellt wird. Verfassungsschutzbehörden unterliegen nicht dem Strafverfolgungszwang und sind insoweit flexibler als z.B. Polizeibehörden. Ein intensiver vertrauensvoller Erfahrungs- und Erkenntnisaustausch zwischen betroffenen Unternehmen und dem Verfassungsschutz ist die Grundlage für die künftige Verhinderung oder zumindest Erschwerung von Wirtschaftsspionage.

Abschließend möchte ich noch einmal betonen:
Wirtschaftsspionage schädigt unsere volkswirtschaftlichen Interessen in hohem Maße. Zwar ist die Abwehr von illegaler Ausforschung im Wirtschaftsbereich durch verfeinerte Methoden, speziell im Bereich Internet schwieriger geworden, doch sie ist nicht aussichtslos.

Voraussetzungen einer erfolgreichen Abwehr sind: Sensibilität gegenüber den Angriffsgefahren, Kenntnisse über die Methoden und Ziele der Nachrichtendienste, der Einsatz geeigneter Schutzmaßnahmen und die Einsicht in deren Notwendigkeit.

Eine wesentliche Voraussetzung der erfolgreichen Zusammenarbeit zwischen Staat und zu schützender Wirtschaft ist der Informationsfluss. Dieser darf nicht einseitig sein, sondern muss in beide Richtungen laufen. Hier sind in erster Linie die Unternehmen selbst gefordert. Erforderlich sind entsprechende Sicherheitskonzepte und deren konsequente Umsetzung.

Die Verfassungsschutzbehörden des Bundes und der Länder bieten hierbei kompetente Hilfe im Rahmen ihres Sensibilisierungsprogramms „Prävention durch Information“ an. Die Qualität dieser Hilfe hängt aber u.a. auch wesentlich davon ab, welche Informationen die durch Wirtschaftsspionage betroffenen Unternehmen dem Verfassungsschutz übermitteln. Nur wenn über Verdachts- und Schadensfälle gesprochen wird, können daraus qualifizierte Schlussfolgerungen gezogen und Erfahrungen zur Warnung und vor künftigen Gefahren genutzt werden.

Wichtig ist:
Die Verfassungsschutzbehörden stehen für Informationsgespräche, insbesondere auch bei fragwürdigen Kontakten und Vorkommnissen zur Verfügung. Entsprechende Angaben werden vertraulich behandelt.

Nur eine enge und vertrauensvolle Kooperation von Unternehmen und Sicherheitsbehörden verspricht Erfolg.

Wir sind dazu bereit, unseren Teil beizutragen.

„Wirtschaftsspionage via Internet“

Referent: Wolf Klingelhöller, Bundesamt für Verfassungsschutz

Einem WDR 4-Beitrag der Reihe „Auf ein Wort“ vom 10. November 2008 zufolge, kam vor 25 Jahren der erste Computervirus in Umlauf und sorgt seither für großen Ärger. Der Computervirus war von dem Informatiker Fred Cohen geschrieben worden, um die Gefahren von feindlicher Übernahme ganzer Computersysteme aufzuzeigen.

Inzwischen haben sich die Vorhersagen von Fred Cohen bewahrheitet. Wegen der Durchdringung nahezu aller Lebensbereiche mit der Computertechnik wächst der Lebensraum für Viren ständig. Damit wächst auch die Bedeutung des Themas “Wirtschaftsspionage via Internet", mit dem man sich nicht erst neuerdings beschäftigt.

Viele berufene Autoren und Experten haben sich damit befasst und dabei verschiedene Aspekte betrachtet :

- z.B die technischen Aspekte, die beschreiben, auf welche Weise es gelingt, angegriffene Rechnersysteme zum "Plaudern" (Stichwort "Spionage") oder zum Absturz zu bringen bzw. Daten zu verändern (Stichwort "Sabotage"), oder
- die Aspekte, die sich mit Möglichkeiten und Schwächen von Bedienern und Nutzern der Opfersysteme befasst, oder
- mit der Angreiferseite, Angreifergruppierungen und deren jeweiligen Motivation.

Dabei wird der Begriff „Wirtschaftsspionage“ oftmals weiter gefasst als es der Verfassungsschutz aus guten Gründen tut. Da dieses am heutigen Tage bereits mehrmals angesprochen wurde, will ich die von uns für wichtig gehaltene Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung nicht erneut ausbreiten und als bekannt voraussetzen. Ich werde mich im weiteren Verlauf des Vortrags mit Vorkommnissen befassen, die nach unserer Meinung einen nachrichtendienstlichen Hintergrund besitzen bzw. bei denen ein solcher nicht ausgeschlossen werden kann und bei denen es sich dann, wenn sie gegen die Wirtschaft gerichtet sind, um Fälle von Wirtschaftsspionage handelt.

Ich werde in meinem Vortrag auch nur wenig in die Technik eintauchen. Ich verstehe zwar ein bisschen was vom Internet; aber nicht ausreichend, um Ihnen in verständlicher Form alle Angriffsformen und Abwehrtechniken darzustellen, die mit großer Kreativität auf Angreifer und Verteidigerseite entwickelt werden. Mein Ziel ist es vielmehr, Sie mit der Darstellung von Erkenntnissen und Einschätzungen des Verfassungsschutzes so betroffen zu machen, dass Ihre sicherlich schon hohe Einschätzung der Bedeutung der IT-Sicherheit eine weitere Bestätigung erhält und Sie dieses weitervermitteln wollen.

Es ist keine Neuigkeit, dass ein Rechner, der an ein Datennetz angebunden ist, grundsätzlich über dieses Netz angegriffen und dann ausgespäht werden kann. Daten können verändert und elektronische Identitäten übernommen werden. Grundsätzlich ist

daher jede auf einem Rechner am Netz gespeicherte Information gefährdet.
Auf den Aspekt, dass eine gekaperte IT-Infrastruktur und Identitäten für Angriffe gegen weitere Rechner missbraucht werden können, will ich hier nicht weiter eingehen.

Rechner am Netz können Schadprogramme – Viren mittels entsprechend kompromittierter E-Mail-Anhänge empfangen oder auch durch das bloße Ansurfen von verseuchten Web-Sites, zum Beispiel branchenorientierten Sites.

Das Infizieren mit einem Virus kann aber auch ohne eine Netzanbindung eines Rechners erfolgen. Kommt ein so infizierter Rechner später ans Netz, kann die Schadsoftware in Aktion treten.

Wir wissen, dass Datenträger (USB-Sticks, FlashKarten, CD's, etc.), zum Beispiel als Werbemittel verteilt, zum Einschleusen von Schadsoftware genutzt werden. Also Vorsicht !!

Verweigern Sie auch die Bitte, auf Ihrem Laptop befindliche Dateien z.B. eine sehr gelobte Power-Point Präsentation, auf einen Ihnen zur Verfügung gestellten USB-Stick zu überspielen. Auf diesem könnte sich bösartige Software befinden. Auch für dieses Beispiel liegen Erkenntnisse vor.

Immer wieder sprechen auch wir die Empfehlung aus, mitgeführte Rechner nicht aus dem Auge zu lassen. Das beinhaltet auch den Rat, hoteleigene Schließfächer nicht als sicheren Aufbewahrungsort zu betrachten. Wir sind immer wieder überrascht, dass diese Empfehlung nur eingeschränkt zur Kenntnis genommen wird.

Neben der Schadsoftware in Form von Viren, die sich im angegriffenen Rechner "breit machen", wird auch über so genannte Würmer gesprochen, die gleichermaßen unappetitlich sind. Das sind Programme, die sich selbstständig über ein Netz verbreiten und auf andere Rechner vervielfältigen können. Eine Nutzung von Würmern für Zwecke der Spionage / Wirtschaftsspionage ist uns bisher nicht bekannt geworden.

Die zur Zeit wohl populärste Methode, um flächenwirksam und mit geringem Aufwand Schadprogramme zu verbreiten, ist die Verbreitung mittels verseuchter Anhänge an E-Mails. Daneben gibt es mit natürlich auch weitere Methoden, die weniger „öffentlich" sind, eher konspirativ genutzt werden, daher noch schwieriger zu detektieren sind und vom Angreifer auch größeren Aufwand erfordern. Sie dienen wahrscheinlich auch eher für Angriffe auf sehr wertige, handverlesene Einzelziele.

Seit dem Jahre 2003 wird in den Medien, insbesondere auch dem Internet selbst immer wieder über elektronische Angriffe mit E-Mails, die Schadsoftware behaftete Anhänge (.doc,.ppt,.pdf) besitzen, berichtet. Untersuchungen dieser Angriffe führten zu der Einschätzung, dass sie ihren Ursprung mit hoher Wahrscheinlichkeit in der Volksrepublik China haben und von dort mit Ausdauer und breitflächig gegen Regierungsstellen und Firmen im jeweiligen Zielland vorgetragen werden.

Seit 2005 werden solche E-Mail-Angriffe auch in Deutschland festgestellt und mit dem gleichen Ergebnis ausgewertet, was in enger Zusammenarbeit von BfV und BSI erfolgt. Die Erstfeststellungen im Jahre 2005 waren Beginn einer systematischen Beobachtung und Analyse derartiger Angriffe gegen Bundesbehörden in Deutschland.

Die in Rede stehenden Angriff-Mails zeichnen sich durch mehrere Eigenschaften aus:

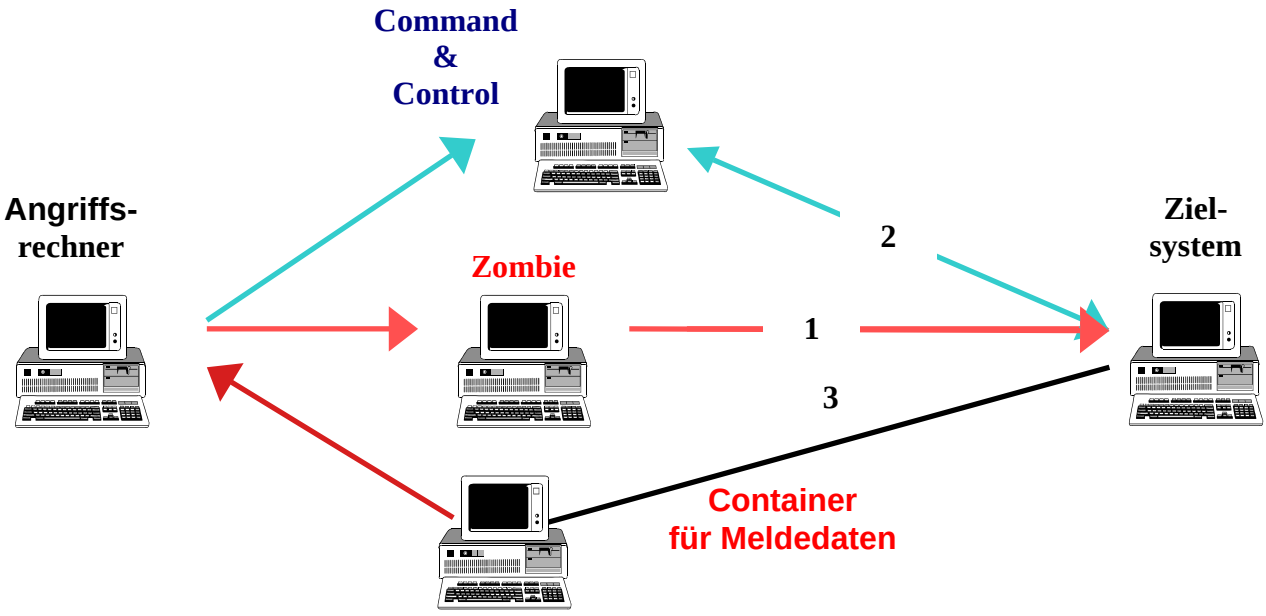
- sie sind an existente Personen / Personengruppen oder Arbeitsbereiche gerichtet. Das zeugt von einer gezielten Auswahl der "Opfer“, deren E-Mail-Adresse auf irgendeine Weise bekannt geworden ist, z.B. Messebesuchen, Geschäftskontakte, bei Empfängen, Hotelbuchungen usw.. Gelegentlich ist auch festgestellt worden, dass die angemailten Personen zwar existieren, aber nicht erreicht werden konnten, weil entweder die Adresse falsch geschrieben war oder die Person inzwischen über eine andere Adresse verfügt
- in den Betreffzeilen der E-Mails werden Themen oder Ereignisse angesprochen, die für den angemailten Empfänger aufgrund seiner Funktion / Tätigkeit / Hobbys /... von Interesse sein sollten.
  Wir sind sicher, dass den Angriffen ein sorgfältiges "social Engineering" vorausgeht mit dem Zweck, dass der Empfänger den mitgeführten Anhang der E-Mail öffnet, wodurch der Schadsoftware die Möglichkeit für eine Installationsversuch gegeben wird. Dem Empfänger wird es erschwert, in der Praxis nahezu unmöglich gemacht, vor dem Öffnen der Mail zu erkennen, dass er Opfer eines E-Mail-Angriffs zu werden droht.
- die schädlichen E-Mails sind signaturarm,
  sie werden von kommerzieller AntiViren-Software in den wenigsten Fällen erkannt
- viele der schädlichen E-Mails sind an mehrere Empfänger gerichtet,
  die alle über den gleichen Betreff-Köder angesprochen werden sollen. Dadurch wird die Wirkung natürlich bei geringem zusätzlichen Aufwand auf Angreiferseite vervielfältigt.
- einmal genutzte Empfängerlisten werden mit leichten Modifizierungen wieder genutzt.
  Daran ist eindeutig erkennbar, dass sie überarbeitet werden. Das spricht gegen einen amateurhaften Hintergrund der Versendung solcher E-Mails. Dass dabei auch der "Betreff' zwar geändert wird aber trotzdem noch zur Zielgruppe passt, legt einen professionellen Hintergrund sehr nahe. Außerdem lässt das Nachbessern darauf schließen, dass der Angreifer die Reaktionen auf seine Angriffe auswertet und auf dieser Basis seine Angriffe optimiert.

Die gezielte Auswahl von Empfängern bzw. Empfängergruppen, deren Tätigkeitsfelder (Regierungsstellen / Politik / Wirtschaft) in Verbindung mit dem erkannten "social Engineering“ sowie der lange Atem der Angriffstätigkeit legen die Vermutung nahe, dass hinter den Angriffen ein staatliches Interesse steht. Die Nachrichtengewinnung in staatlichem Auftrag ist typischerweise die Aufgabe von Nachrichtendiensten.
Wir schätzen, dass im Laufe eines Jahres mehrere Hundert E-Mail-Angriffe stattfinden.

Inhaber von E-Mail-Accounts in Organisationen wie Behörden oder Wirtschaftunternehmen sind wohl in der Regel über ein - hoffentlich - wohl konfiguriertes und mit Sicherheitsmaßnahmen gehärtetes "Hausnetz" an das Internet angeschlossen. Unsere Feststellungen zeigen jedoch, dass die oben beschriebenen

Angriff-E-Mails trotzdem durch allzu viele Schalen zum End-User durchkommen. Dann ist der Mensch die letzte Filterstelle, die das Einbringen von Schadsoftware verhindern könnte. Praktisch ist das aber nicht zu leisten. Die Erfahrung zeigt, dass eine gut gemachte Angriffs-Mail ohne offensichtliche Fehler z.B. Schreibfehler in Absender- oder Empfängeradresse und einem guten „social Engineering“ in den meisten Fällen geöffnet wird. Meistens sind auch die Zeit oder die IT-Mittel gar nicht vorhanden, jede einlaufende E-Mail zu prüfen.

Die festgestellten E-Mail-Angriffe werden in einer Art und Weise durchgeführt, die aus einschlägiger Literatur seit langem bekannt ist. Grundsätzlich erfolgt ein solcher Angriff in drei Phasen:



Der Verfassungsschutz sieht es als eine seiner präventiven Pflichten an, betroffene Stellen in Deutschland auf der Basis seiner Erfahrungen zu unterrichten und zu sensibilisieren.

An dieser Stelle möchte ich klarstellen, dass es mir nicht darum geht, die besondere Gefährlichkeit von E-Mail-Angriffen gerade aus der Volksrepublik China aufzuzeigen. Die besondere Bedeutung Chinas für unsere Wirtschaft ist bekannt.
Der Schutz gegen ein bestimmtes Land ist nicht mein Ziel; es geht vielmehr darum, auf zu zeigen, dass Informationen in unserem Land geschützt müssen weil sie gefährdet sind, von welchem Land auch immer.

Bei diesen Unterrichtungen und Sensibilisierungen müssen wir einen Spagat zwischen einerseits einer für konkrete Schutzmaßnahmen geeigneten Unterrichtung und andererseits der Gewährleistung auch zukünftigen Erkenntnisgewinns leisten. Das widerspricht sich. Eine Verbreitung allen Wissens würde das Erkennen zukünftiger Angriffe erschweren. Im Übrigen besitzen konkrete Angriffsparameter nach unseren Erfahrungen nur eine begrenzte zeitliche Gültigkeit, sodass durch deren Verbreitung ein falsches Gefühl der Sicherheit suggeriert würde.

Daraus resultiert die Notwendigkeit für ein abgestuftes Sensibilisierungsverfahren:

- In geeigneten Runden stellen wir Erkenntnisse und Gefahrenbewertungen dar. Wir wollen damit die seit langem bekannte abstrakte Gefahr konkreter und den Verantwortlichen die Gefahren bewusster machen.
- Aus solchen Veranstaltungen entstehen weitergehende Kontakte, in denen auch konkrete technische Sachverhalte diskutiert werden können. Das setzt voraus, dass die Firmen mit uns bei der Detektion von Angriff-Mails zusammenarbeiten und auch bereit sind, uns in Fällen, in denen sie sich angegriffen sehen, zu unterrichten. Letzteres hilft uns bei der Verbreiterung der Bewertungsbasis als Grundlage für weitere aktuelle Sensibilisierungen.

Solche weitergehenden Kontakte werden von uns dann eingegangen, wenn auch der Verfassungsschutz einen Mehrwert erzielt. Wir benötigen einschlägige Rückmeldungen betroffener Firmen, die zu unserer Gesamtbewertung beitragen. Es sind nämlich die angegriffenen Unternehmen selbst, die über die Sensoren zur Feststellung solcher Angriffe verfügen. Der Verfassungsschutz betreibt keine Sensoren im privaten Bereich. Sie können versichert sein, dass solche Rückmeldungen nie 1-zu-1 in Sensibilisierungsgesprächen mit anderen Firmen genutzt werden. Die Anonymität ist gewährleistet. Wir werden auch nie die gelegentlich gestellte Frage beantworten, bei welcher Firma durch einschlägige E-Mail-Angriffe denn welcher Schaden eingetreten sei. Auch nicht wenn eine solche Aussage angeblich benötigt werde, um die Konsequenzen anhand eines konkreten Schadenfalles richtig einschätzen und das Management überzeugen zu können.

Bei allen Sensibilisierungsgesprächen kommt es uns darauf an, nicht nur Feststellungen, Erfahrungen und Bewertungen abzugeben, sondern letztlich die reale Bedrohung so zu vermitteln, dass betroffene oder potenziell betroffene Firmen zu der Einsicht gelangen, dass sie mehr für ihre IT-Sicherheit tun müssen, wenn der Schutz der gesteigerten Anforderung stand halten soll. Eigeninitiatives und eigenverantwortliches Handeln ist erforderlich. Wir versuchen mit unseren Erkenntnissen, dazu Anstöße zu geben.

Ich möchte an dieser Stelle darauf hinweisen, dass wir keine IT-Sicherheitsberatung bieten. Das ist nicht unsere Aufgabe und würde auch bei kommerziellen IT-Sicherheitsberatungsunternehmen gar nicht gut ankommen.

Da alle Maßnahmen zur Sicherstellung der IT-Sicherheit Kosten mit sich bringen und möglicherweise bisher praktizierte Schutzmaßnahmen in Frage stellen, ist es nur zu verständlich, dass unsere Bewertungen und Empfehlungen hinterfragt werden. Gelegentlich hören wir bei Firmenkontakten (aber auch Behörden), dass die jeweilige Firma über ein mehrstufiges Virenschutzkonzept verfüge und nahezu 100% aller unerwünschten E-Mails heraus fische. Das sei doch ein hohes Maß an Sicherheit. Dazu zwei Anmerkungen: Der Weg, trojanisierte E-Mail-Anhänge auf einem Zielrechner zu platzieren, wird nicht nur von Nachrichtendiensten begangen, sondern kann auch einen kriminellen Hintergrund besitzen. Außerdem gibt es bekanntermaßen in großer Zahl E-Mail-Spams. Es ist gut, wenn diese herausgefiltert werden und dazu sind die Produkte

der Anti-Viren-Software-Hersteller sicherlich geeignet. Die E-Mails, über die ich hier heute rede, werden aber nicht so sicher detektiert. Sie sind - wie oben schon erwähnt - bewusst signaturarm gestaltet, um gerade die kommerzielle Anti-Viren-Software zu unterlaufen. Das heißt, die nachrichtendienstlich relevante Software gelangt ans Ziel. Das nahezu 100% ige Herausfischen von unerwünschten E-Mails bringt nicht die erhoffte Sicherheit gegen den starken Gegner. Ähnlich wie das Argument des mehrstufigen Virenschutzkonzepts sehen wir die Sicherheit, die durch hintereinander geschaltete Firewalls gegeben sein soll. Der Angreifer hackt sich nicht durch Firewalls. Er nutzt vielmehr erlaubte Protokolle wie E-Mails und WEB (HTTP). Die hierzu benötigte Mitwirkung des Opfers wird durch Köder-Techniken des „social Engineerings“ erreicht.

An der zunehmenden Bedeutung der Computertechnologie bestehen keine Zweifel. Das gleiche wird allerdings auch für die Bedrohung durch elektronische Angriffe gelten. Ihre Effektivität wird mit dem Wachstum des Internets und der Komplexität der Computer-Software steigen. Sie sind

- vergleichsweise billig,
- für den Angreifer wenig risiko-behaftet,
- sehr effektiv,
- einfach und weltweit zu platzieren,
- in Real-Zeit durchführbar,
- für viele Zwecke verwendbar,
- Mittel einer asymmetrischen Auseinandersetzung, d.h. der Schutz-Aufwand eines Angegriffenen ist deutlich höher als der Aufwand des Angreifers.

Viele Aktivitäten zur Detektierung von elektronischen Angriffen sowie zu ihrer Abwehr sind Reaktionen auf aktuelle Situationen. So wie sich die Computertechnologie und Angriffstechnik weiter entwickelt, müssen sich auch Schutzmaßnahmen weiter entwickeln.

Abschließend einige Merkposten :

- Jeder Rechner am Internet ist gefährdet.
- Die Elektronische Bedrohung wird zunehmen.
- Ergriffene Maßnahmen zur IT-Sicherheit sind nicht für die Ewigkeit geeignet, sondern bedürfen einer permanenten Evaluierung und Nachjustierung.
- Jede potenziell gefährdete Stelle (Unternehmen / Behörde) trägt selbst die Verantwortung für alle ergriffenen oder nicht-ergriffenen Maßnahmen zur Abwehr von elektronischen Angriffen.
- Lassen Sie Ihre Mitarbeiter nicht alleine; sorgen Sie für Ihre IT-Sicherheit.

Die Schäden durch Spionage in der deutschen Wirtschaft

11. Dezember 2008

CORPORATE TRUST
business risk & crisis management

Ergebnisse der Studie

Vorfälle

CORPORATE TRUST
business risk & crisis management

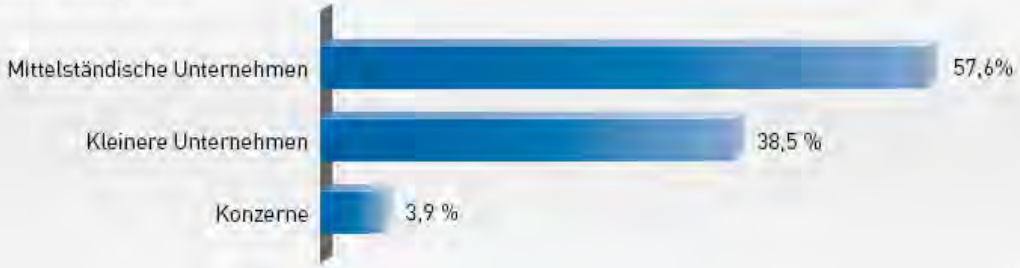
Gab es in ihrem Unternehmen bereits konkrete Hinweise auf Spionage bzw. einen Informationsabfluss?

GRAFIK 2 Quelle: Corporate Trust 2007

Gab es in Ihrem Unternehmen einen Verdacht auf Spionage bzw. Informationsabfluss, der nicht näher belegt werden konnte?

GRAFIK 3 Quelle: Corporate Trust 2007

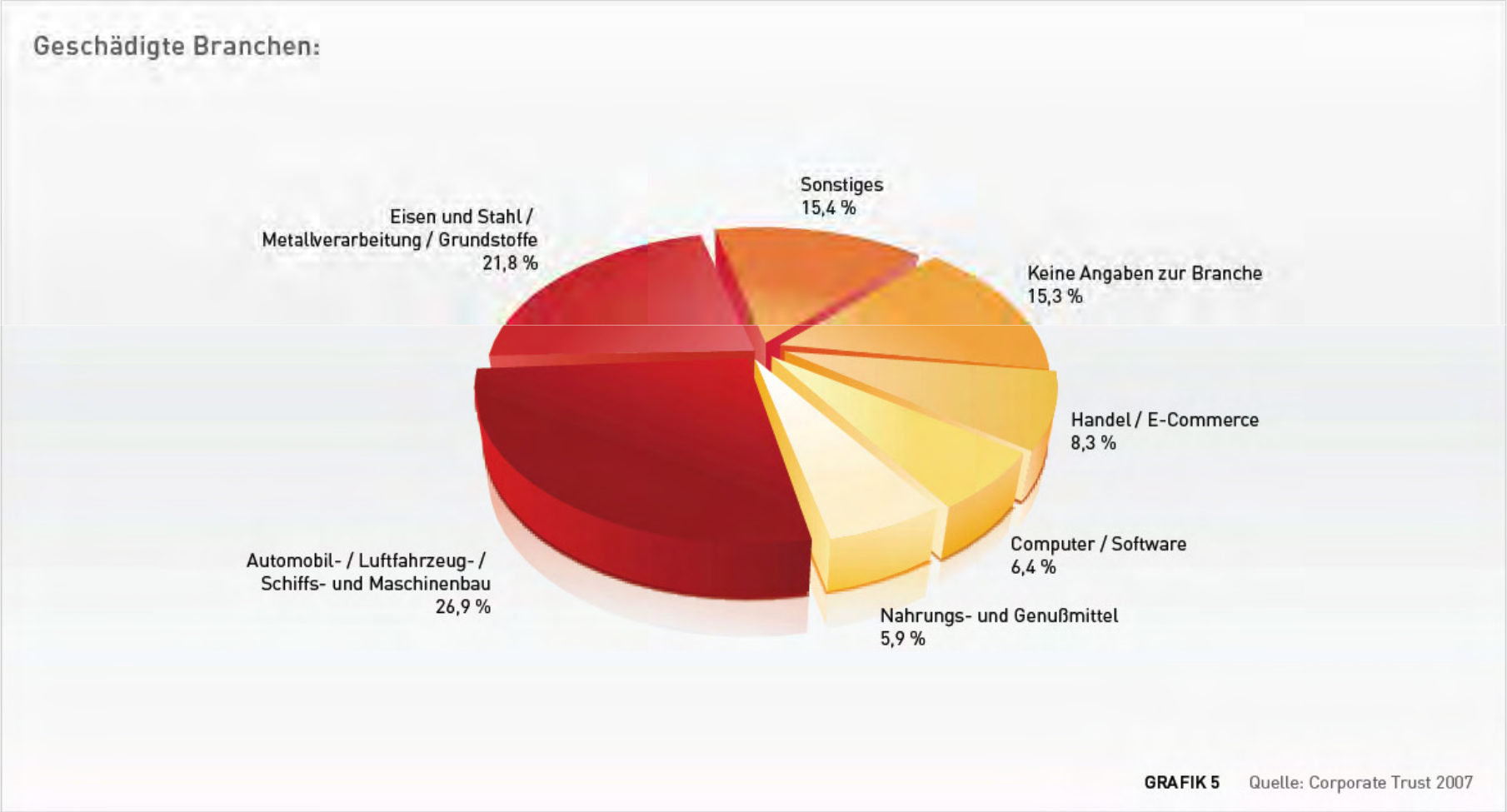
Schäden nach Unternehmensgröße:



GRAFIK 4 Quelle: Corporate Trust 2007

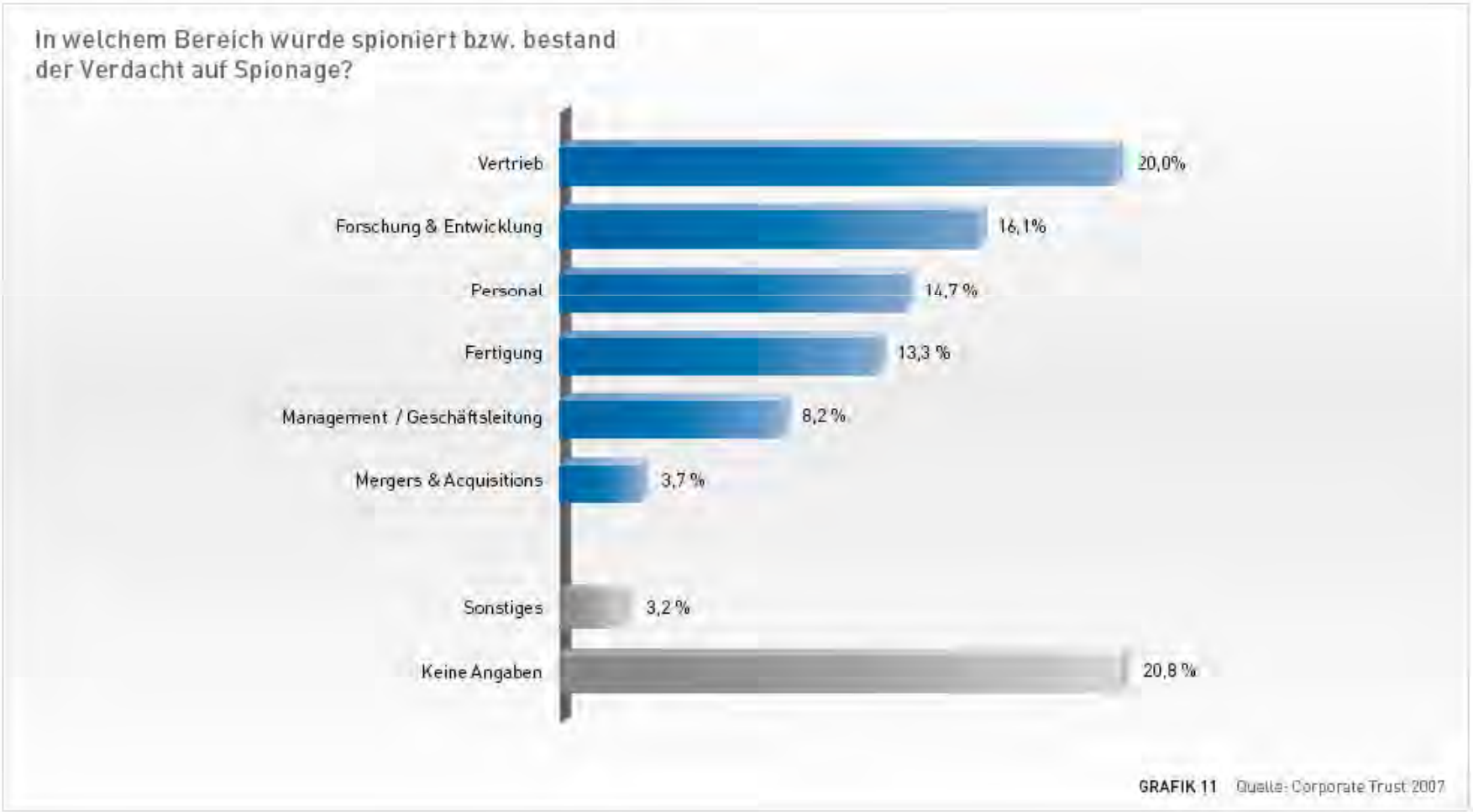
Geschädigte Branchen

CORPORATE TRUST
business risk & crisis management



In welchem Bereich wurde spioniert

CORPORATE TRUST
business risk & crisis management

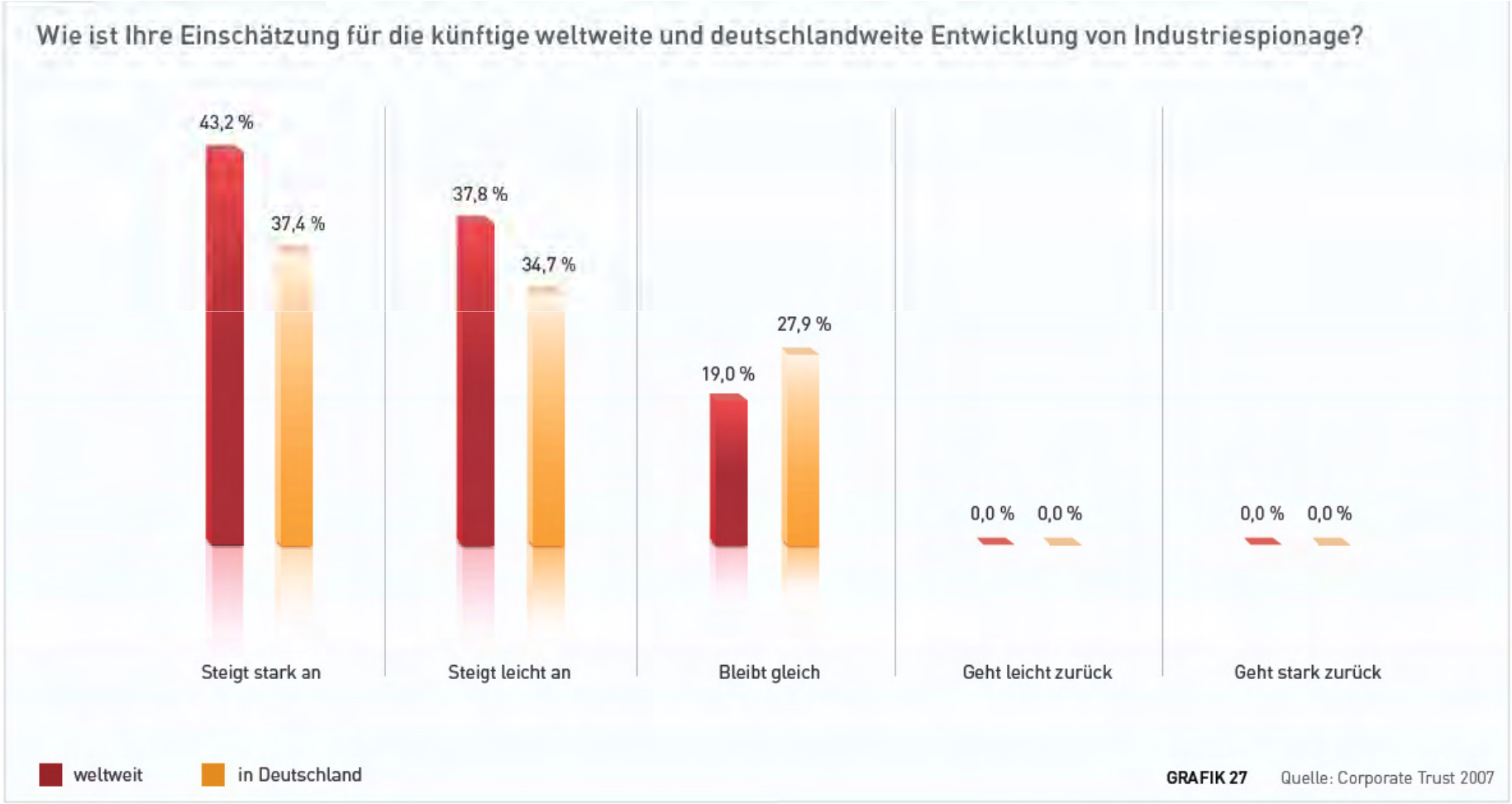


Spionage - Handlungen

CORPORATE TRUST
business risk & crisis management

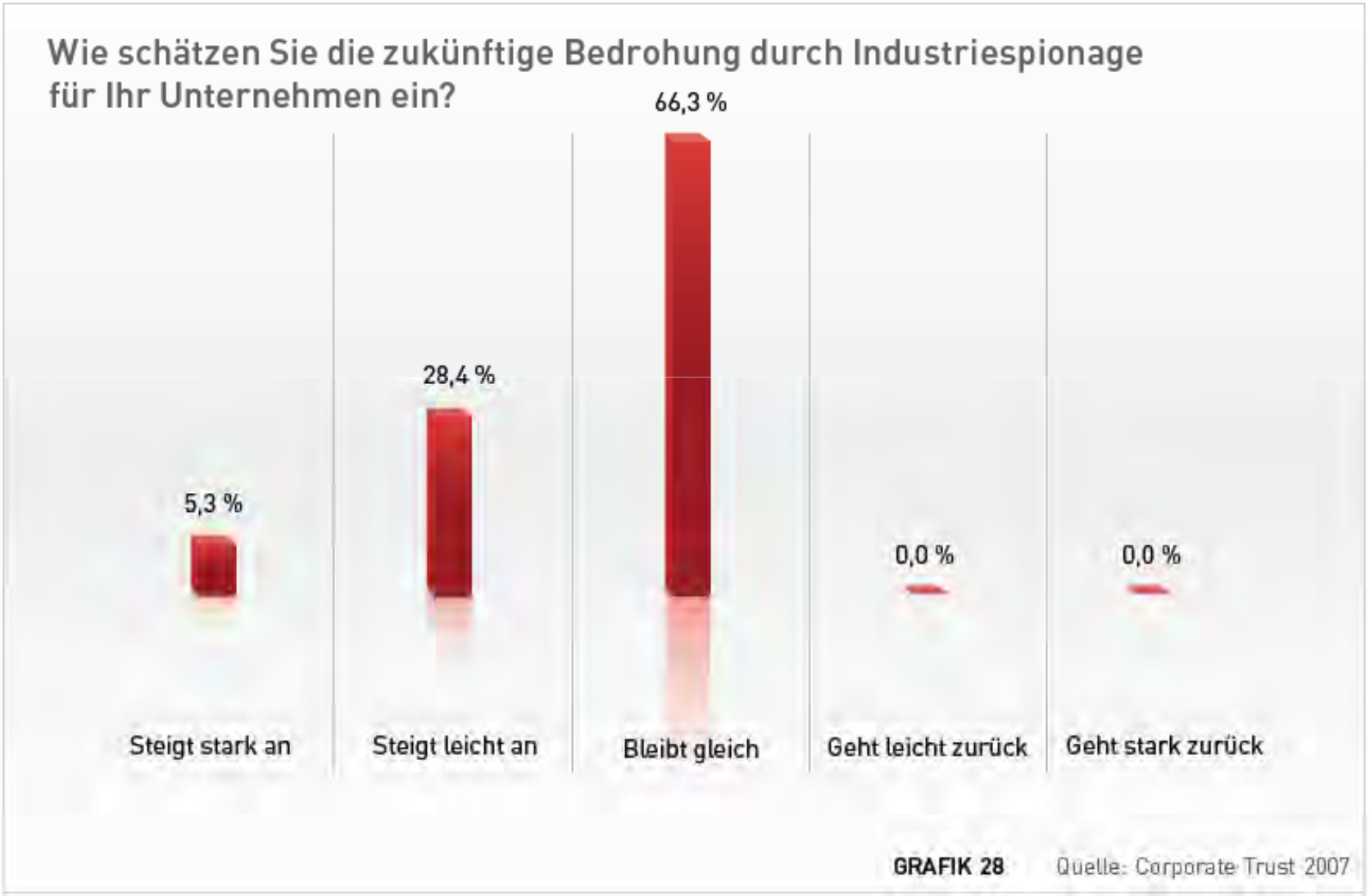
Zukünftige Entwicklung von Spionage

CORPORATE TRUST
business risk & crisis management



Zukünftige Entwicklung von Spionage

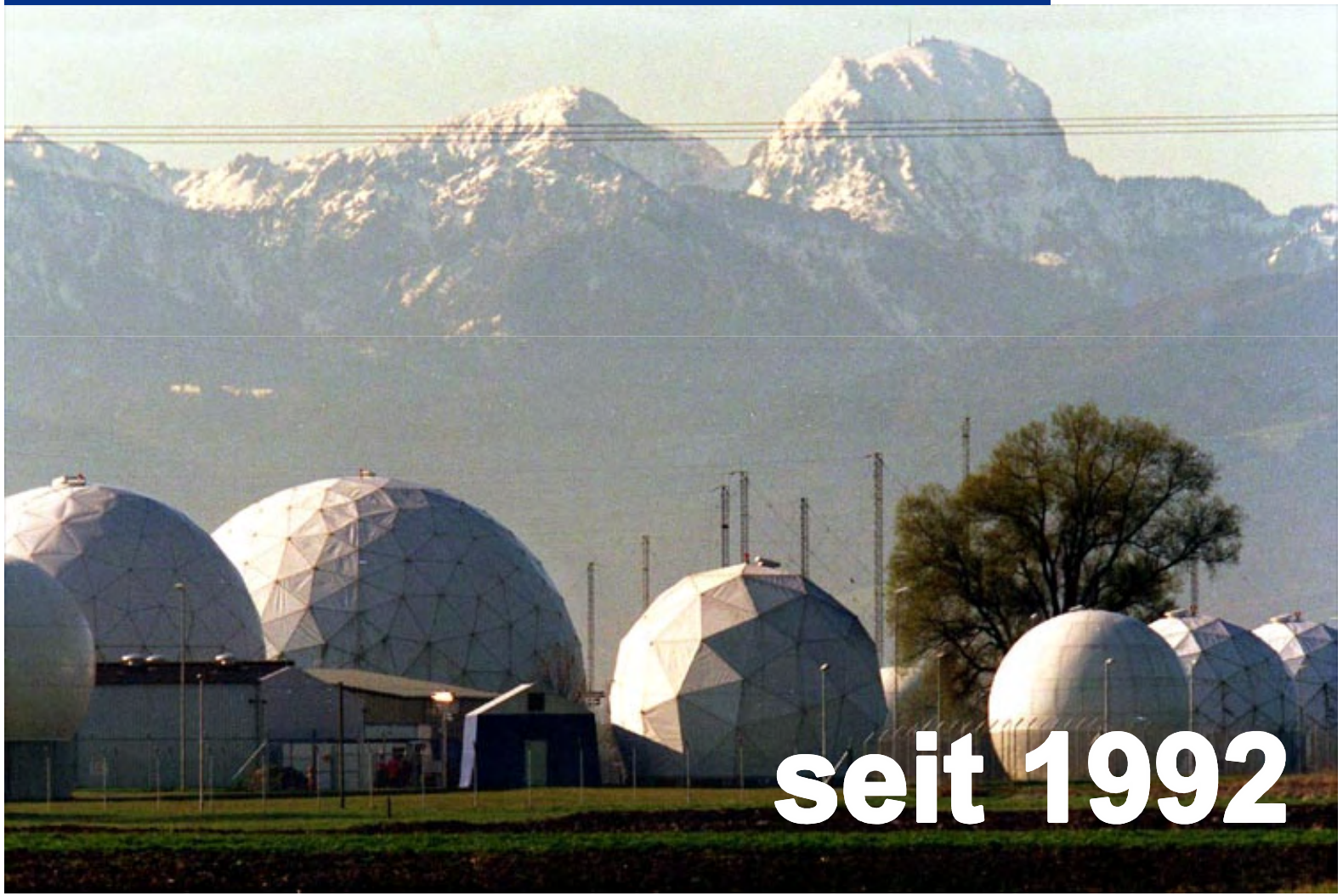
CORPORATE TRUST
business risk & crisis management



CORPORATE TRUST
business risk & crisis management

Ein neues Thema?

Echelon - Geheimdienst NSA aus USA



CORPORATE TRUST
business risk & crisis management

Französischer Geheimdienst

Echelon - Geheimdienst NSA aus USA

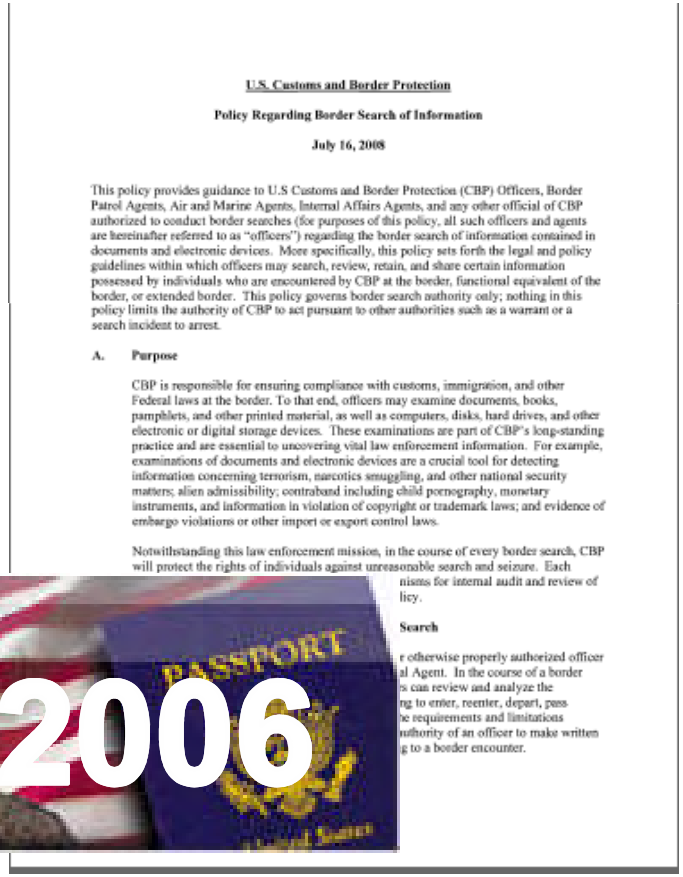
Chinesische Werkstudentin

Valeo

2005

CORPORATE TRUST
business risk & crisis management

Laptopkontrolle bei der Einreise



U.S. Customs and Border Protection

Policy Regarding Border Search of Information

July 16, 2008

This policy provides guidance to U.S Customs and Border Protection (CBP) Officers, Border Patrol Agents, Air and Marine Agents, Internal Affairs Agents, and any other official of CBP authorized to conduct border searches (for purposes of this policy, all such officers and agents are hereinafter referred to as "officers") regarding the border search of information contained in documents and electronic devices. More specifically, this policy sets forth the legal and policy guidelines within which officers may search, review, retain, and share certain information possessed by individuals who are encountered by CBP at the border, functional equivalent of the border, or extended border. This policy governs border search authority only; nothing in this policy limits the authority of CBP to act pursuant to other authorities such as a warrant or a search incident to arrest.

A. **Purpose**

CBP is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, officers may examine documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices. These examinations are part of CBP's long-standing practice and are essential to uncovering vital law enforcement information. For example, examinations of documents and electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography, monetary instruments, and information in violation of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

Notwithstanding this law enforcement mission, in the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure. Each
nisms for internal audit and review of
licy.

Search

e otherwise properly authorized officer
al Agent. In the course of a border
s can review and analyze the
g to enter, reenter, depart, pass
e requirements and limitations
uthority of an officer to make written
g to a border encounter.

Chinesische Hacker - Social Engineering

CORPORATE TRUST
business risk & crisis management

Von wem droht die Gefahr?

Täter

CORPORATE TRUST
business risk & crisis management

1 Staatliche Stellen

2 Innentäter

3 Konkurrenz

4 Hacker

5 OK

6 Medien

CORPORATE TRUST
business risk & crisis management

Schwachstelle Mensch

Internes Risiko

CORPORATE TRUST
business risk & crisis management

Personen mit einer hohen Vertrauensstellung

Internes Risiko

CORPORATE TRUST
business risk & crisis management

1 Interne Täter
(Eigene Mitarbeiter / Externe)

- Eigenaktiv
- Angeworben
- Eingeschleust

2 Social Engineering

- Als vorbereitende oder direkte Informationsgewinnung

3 Leichtfertig

- Abfluss von Information ohne böse Absicht
- Angeberei

CORPORATE TRUST
business risk & crisis management

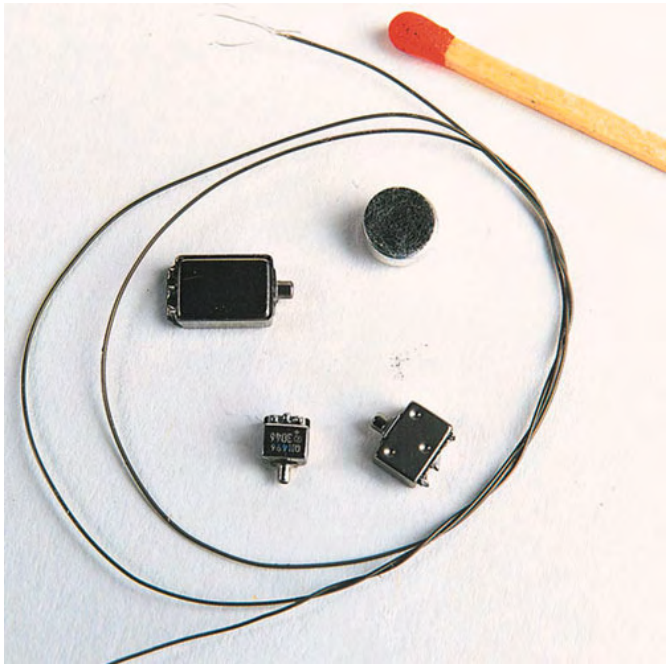
Technische Möglichkeiten

Key Ghost – Key Logger

CORPORATE TRUST
business risk & crisis management

Wanzen

CORPORATE TRUST
business risk & crisis management

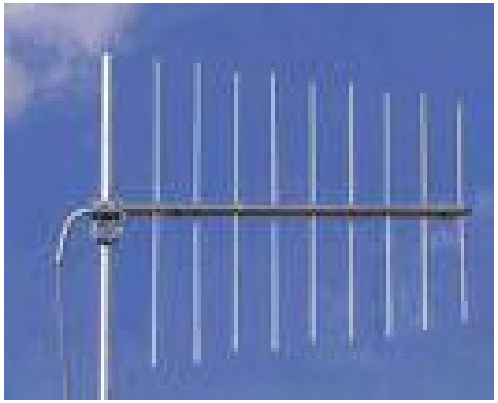


Versteckte Kameras und Mikrofone

CORPORATE TRUST
business risk & crisis management

Kompromittierende Strahlung

CORPORATE TRUST
business risk & crisis management



CORPORATE TRUST
business risk & crisis management

Informationsschutz im Ausland

Hotel

CORPORATE TRUST
business risk & crisis management

No´s:

- **Unterlagen im Safe**
- **WLAN nutzen**
- **Vertrauliche Informationen**
  - bei vermeintlich privater Kontaktaufnahme
  - über das Hoteltelefon
  - in ungesicherten Bereichen

Meeting

CORPORATE TRUST
business risk & crisis management

No´s:

- Herausgabe vertraulicher Unterlagen
- Laptop unbeaufsichtigt
- Speichermedien aushändigen

Kommunikation

CORPORATE TRUST
business risk & crisis management

No´s:

- **Netzwerkzugang über Fremd-Firmen-PC / -WLAN**
- **Bluetooth oder Head-Set**
- **Hotelinternet oder WLAN**
  - Passwortschutz
  - Vertraulichkeit

Socializing

No´s:

- **Prostituierte**
- **Übermäßiger Alkoholkonsum**
- **Annahme teurer Gastgeschenke**

CORPORATE TRUST
business risk & crisis management

Danke für Ihre Aufmerksamkeit!

„Politischer Extremismus und seine Auswirkungen auf die Wirtschaft“

Referent: Guido Selzner, Bundesamt für Verfassungsschutz

Wenngleich der Titel dieses Vortrages allgemeingehalten „Politischer Extremismus und seine Auswirkungen auf die Wirtschaft“ lautet, so wird man bei Sichtung der gegen die Wirtschaft gerichteten extremistisch motivierten Aktionen schnell feststellen, dass eine konkrete Bedrohung derzeit ausschließlich von Linksextremisten ausgeht.

D.h. das Propagieren von militanten Aktionen gegen die Wirtschaft oder gar deren Umsetzung finden in Deutschland lediglich im Linksextremismus statt – dafür allerdings umso manifester.

Entgegen dem Trend der letzten Jahre, der den deutschen linksextremistischen Phänomenbereich in der veröffentlichten Meinung allenfalls marginal verortete, erfuhr die Thematik „Gefährdung durch Linksextremisten“ zuletzt wieder wachsende Aufmerksamkeit.

Anlass dafür bot eine Reihe militanter Aktionen im Vorfeld und während des G8-Gipfels in Heiligendamm im Juni 2007. Und mit dem NATO-Jubiläumsgipfel Anfang April des kommenden Jahres taucht ein ähnlich „attraktives“ Ereignis bereits am zeitlichen Horizont auf. So untersucht der Vortrag die von Linksextremisten ausgehenden Bedrohungen

- in theoretisch – abstrakter Hinsicht – was deren ideologische Legitimation angeht,
- in einer Rückschau auf die „militante Kampagne“ gegen den G8-Gipfel.
- Und im Verweis auf aktuelle Beispiele linksextremistischer Anschläge auf Wirtschaftsunternehmen.

Linksextremistisches Personenpotenzial

Vorab ein Blick auf die Statistik, die einen Eindruck vom Potenzial der gewaltbereiten Linksextremisten liefert.

Zu dieser Gruppe zählen wir bundesweit ca. 6.300 Personen. Der weit überwiegende Teil davon – ca. 5.800 – sind sog. Autonome.

Ein Blick in die vom BKA erhobenen Zahlen zur „politisch motivierten Kriminalität links“ belegt für das Jahr 2007 insgesamt 2.765 Straftaten mit linksextremistischem Hintergrund, davon 833 Gewalttaten.

Im Bereich dieser 833 Gewalttaten sind besonders auffallend 384 Körperverletzungen, 51 Brandstiftungen und 215 Landfriedensbrüche.

Dies sind – absolut betrachtet – schon bemerkenswerte Größenordnungen, die den allgemeinen Aufwärtstrend der letzten Jahre bestätigen. So stieg die Zahl der politisch motivierten linksextremistischen Straftaten gegenüber dem Jahr 2006 um fast 17%.

Zu Beginn möchte ich darlegen, warum Wirtschaftsunternehmen das Feindbild für Linksextremisten sind und warum Wirtschaftsunternehmen gerade im Visier gewaltbereiter Linksextremisten stehen.

Wirtschaftsunternehmen sind Teil des marktwirtschaftlichen Systems. Sie sind sogar elementarer Bestandteil, sie sind – aus linksextremistischer Sicht – der Motor des Kapitalismus, d.h. eines Systems, das es - mit Blick auf die zu erringende herrschafts- und ausbeutungsfreie Gesellschaft - zu bekämpfen und zu überwinden gilt.

Vor diesem ideologischen Konstrukt weisen Linksextremisten Wirtschaftsunternehmen die zentrale Verantwortung für alle unterstellten sozialen und politischen Missstände zu. Diese Zuordnung gilt für die Wirtschaft insgesamt genauso wie für jedes einzelne Wirtschaftsunternehmen.

Darüber hinaus erstreckt sich der Schuldverweis auf die Mitarbeiter dieser Unternehmen und in Sonderheit auf jene, die dort Verantwortung tragen.

Der Vorwurf lautet, dass es Unternehmen ausschließlich darum zu tun ist, Gewinne zu maximieren und ihren wirtschaftlichen und politischen Einfluss zu sichern.

Dafür werden – nach linksextremistischer Lesart – zum einen Menschen unterdrückt und ausgebeutet und zum anderen Natur und Umwelt beschädigt oder nachhaltig zerstört.

Gefährdete Wirtschaftsbereiche

Wenn man nun versucht, diese – ideologisch abgeleitete – abstrakte Gefährdungsbeschreibung zu konkretisieren, ist es sinnvoll, die Risikofelder mit Hilfe der „klassischen“ Themen linksextremistischer Agitation zu markieren.

Der **„antifaschistische Kampf“** ist das Aktionsfeld Nummer 1.
Besonders gefährdet sind folglich Unternehmen, die aus linksextremistischer Perspektive den – unserem politischen System zwangsläufig innewohnenden – Faschismus tolerieren oder fördern. Dies sind in erster Linie

- Transport- und Reiseunternehmen, die (vermeintliche) Rechtsextremisten zu Veranstaltungen bringen
- Betriebe aus dem Hotel- und Gaststättengewerbe, die diesen Personen oder Vereinigungen Räume zur Verfügung stellen sowie Militaria-Händler und bestimmte Bekleidungsgeschäfte.

Mit dem Stichwort „Asylpolitik“ geht es um das Aktionsfeld **„Antirassismus“.**
Besonders betroffen sind in diesem Bereich Firmen, die mit der Unterbringung, Versorgung und Rückführung von Asylbewerbern beauftragt sind.
Im Mittelpunkt stehen also Hotelketten, Fluggesellschaften oder Lebensmittellieferanten sowie die Betreiber von Unterbringungsheimen.

Ferner sind zu nennen die privaten Wach- und Sicherheitsdienste von sog. Abschiebe-Haftanstalten oder die entsprechenden Dienste von so genannten „Abschiebe“-Flughäfen.

Bei **„Profiteure des Sozialabbaus“** stehen solche Unternehmen oder Einrichtungen im Fokus, die aus Sicht von Linksextremisten besonders von den Sozialreformen oder von der zunehmenden Deregulierung des Arbeitsmarktes profitieren.

Stichworte sind „Hartz IV“ und „1-Euro-Jobs“. Betroffen bzw. in Taterklärungen exemplarisch genannt werden jene Discounter, die angeblich „Billigjobber“ einstellen oder etwa keine Betriebsräte duldeten.

Hinzu kommen Zeitarbeitsfirmen, Wohlfahrtsverbände oder Umzugsunternehmen, die ihren Gewinn aus Zwangsräumungen im Kontext mit „Hartz IV“ ziehen.

Unter dem Aspekt **„Globalisierung“** wird die internationale Dimension des Stichwortes „Sozialabbau“ thematisiert.
Es geraten solche Unternehmen ins Fadenkreuz, die ihre Geschäftspolitik auf die Globalisierung ausgerichtet haben, etwa durch die Verlagerung von Fertigungsprozessen in Billiglohnländer.
Die mit „Atomgeschäft“ bezeichnete Branche der Nukleartechnologie gehört zu den bevorzugten Angriffspunkten militanter Linksextremisten. Ziel sind regelmäßig Firmen und Einrichtungen, die

- in den Bereichen Nutzung von Kernenergie
- oder Lagerung und Transport von Atommüll

tätig sind. Das gilt vor allem in zeitlicher Nähe zu Castor-Transporten.

In Erweiterung des emotional aufgeladenen Themas richtet sich die Agitation zunehmend auch gegen andere so genannt „unsaubere“ Formen der Energieerzeugung, wie z.B. Braunkohleverstromung – so gegen das Kraftwerk Moorburg in Hamburg.

Unter dem Schlagwort **„Umstrukturierung“** wenden sich militante Linksextremisten jenen Firmen und Banken bzw. Investoren zu, die in Großstädten und Ballungszentren an Projekten zur Stadtsanierung und Strukturverbesserung beteiligt sind. Gemeint ist die Umwandlung ehemaliger „linker“ Stadtteile oder auch sogenannter „Kieze“ in ein Areal teurer Altbauwohnungen, Rechtsanwaltskanzleien und Werbeagenturen.
Die linksextremistischen Aktionsschwerpunkte liegen seit langem in Berlin und in Hamburg. Im Visier erscheinen Immobilienfirmen, Architekturbüros, Banken sowie beteiligte Baufirmen.

Anschlagsziele im Bereich der **Bio- und Gentechnologie** sind hier insbesondere Freilandversuchsanlagen, aber auch US-Agrarmultis oder Futterproduzenten.

Das Thema **Rüstungsbetriebe und deren Zulieferer** bedarf zunächst einmal – so denke ich – keiner weiteren Kommentierung.

Es wird niemanden verwundern, dass der „G8 - Gipfel“ als Treffen der acht wichtigsten Wirtschaftsnationen in besonderer Weise das Lager der Linksextremisten herausfordert.

In ihren Augen handelt es sich um die Zusammenkunft selbsternannter Eliten, die über das Schicksal der Welt und das Wohlergehen von Milliarden Menschen bestimmen,

- ohne dafür demokratisch legitimiert zu sein,
- ohne dass der größte Teil der Weltbevölkerung repräsentiert wäre und ein Mitspracherecht besäße
- und mit dem ausschließlichen Ziel der Sicherung oder gar Vermehrung des eigenen Wohlstands – auf Kosten der Armen und Unterdrückten in der Dritten Welt.

Der jährliche G8-Gipfel gilt somit als Symbol des weltweiten Neoliberalismus, der „Macht des globalen Kapitalismus“ und dessen „politischer und militärischer Gewalt“.

An diesen Deutungen ist zu erkennen, dass die Globalisierung das ideologische Motiv für linksextremistische Agitation in geradezu idealer Weise bietet.

Nahezu alle linksextremistischen Themen- und Aktionsfelder lassen sich unter diesen Begriff subsumieren. Sei es Rassismus, Imperialismus, Militarismus, Faschismus, staatliche Repression, Umweltzerstörung.

Für sämtliche Phänomene trage der Neoliberalismus als globalisierte Form des Kapitalismus Verantwortung – und somit auch die in diesem System agierenden Wirtschaftsunternehmen.

Nachvollziehbar war der G8-Gipfel in Heiligendamm für Linksextremisten das Ereignis, auf das man sich seit dem Gipfel 2005 im schottischen Gleneagles intensiv vorbereitet hatte.

Eine zentrale Rolle spielte hierbei die sog. **„Militante Kampagne“**.
So gab es insgesamt 29 Brandanschläge auf Kraftfahrzeuge bzw. auf Gebäude mit zum Teil beträchtlichen Sachschäden. Von den insgesamt 29 Anschlägen richteten sich 19 gegen Wirtschaftsunternehmen, die übrigen 10 Anschläge gegen staatliche Einrichtungen bzw. gegen Institute, die jedoch allesamt mit dem Thema Wirtschaft in Verbindung stehen oder aus Sicht der Täter für die grundsätzlich negativen Folgen der Globalisierung in Haftung genommen werden.

Darüber hinaus wurden von 2005 bis zum Sommer 2007 über 600 weitere Straftaten mit G8/EU-Bezug verübt, oft handelte es sich um Farbschmierereien.

Im Vergleich zu Brandanschlägen sind Farbattacken zwar strafrechtlich von minderer Bedeutung und verursachen in der Regel auch einen erheblich geringeren Schaden.

Doch darf man das politische Signal nicht unterschätzen, das gerade von solchen Aktionen ausgehen kann.

Dies wurde etwa deutlich an der Farbattacke auf das Wohnhaus des damaligen Ministerpräsidenten von Mecklenburg-Vorpommern, Harald Ringstorff, - im August 2006 - oder auf das Kempinski Hotel in Heiligendamm, also auf den Tagungsort des G8-Treffens, das mit der Farbe – wie es in der Bekennung heißt – als „Ziel markiert" wurde.

Ich möchte Ihnen anhand exemplarischer Anschläge gegen Wirtschaftsunternehmen die Praxis der militanten Kampagne darstellen.

- Das Startsignal der bereits erwähnten „militanten Kampagne" wurde in der Nacht zum 28.Juli 2005 gegeben: Unbekannte verübten einen Brandanschlag auf das Dienstfahrzeug des damaligen Vorstandsvorsitzenden der Norddeutschen Affinerie AG Hamburg. Der Sachschaden belief sich auf etwa 70.000 Euro.
  In der (immerhin) sechsseitigen - anonymen Taterklärung hieß es :
  Der Vorstandsvorsitzende vereinige in seiner Person mehrere Funktionen, die geeignet seien, *„unterschiedliche Facetten imperialistischer Herrschaft aufzuzeigen und anzugreifen."* Er repräsentiere Organisationen, die wesentlich für Privatisierung gesellschaftlichen Eigentums, Verschärfung sozialer Repression und die bedingungslose Unterordnung sozialer Fragen unter die Wettbewerbslogik stünden.
- In der Nacht zum 27.März 2006 brannten bei der Gleis- und Schienenbaufirma Thormählen in Bad Oldesloe fünf Werkstattwagen sowie ein Spezialtraktor aus. Die enorme Schadenssumme belief sich auf ca. 250.000 Euro.
- Die Täter beriefen sich auf das Engagement der TST beim Bau eines Eisenbahnnetzes im Südsudan und brandmarkte die – wie es hieß – ökonomische Ausbeutung des von jahrzehntelangem Bürgerkrieg heimgesuchten Landes durch imperialistische Kräfte.
- Bereits zu Anfang hatte ich die so genannten Profiteure der „Asylpolitik" als Ziel militanter linksextremistischer Aktionen genannt. Im Rahmen dieser „militanten Kampagne" gegen den G8 - Gipfel war die Firma „Dussmann" im Februar und März 2007 gleich zweifach betroffen: Zunächst brannten vier Unternehmensfahrzeuge in Hamburg, dann folgte ein Brandanschlag auf ein von Dussmann genutztes Gebäude in Berlin.
  In ihrer Selbstbezichtigung führten die Autoren aus, das Unternehmen sei in der Vergangenheit - und mit entsprechenden Aktionen - wiederholt aufgefordert worden, *„sich aus der Zwangsverpflegung von Flüchtlingen mit miesem Essen zurückzuziehen, was die Konzernverantwortlichen jedoch ganz offensichtlich nicht zur Kenntnis"* nähmen.

Ein anderer Aspekt:

- Seit jeher bietet die „Bild"- Zeitung das klassische linksextremistische Feindbild. Betroffen war deren Chefredakteur am 22.Mai 2007: Unmittelbar vor seinem Wohnhaus wurde sein Privat-PKW angezündet und vollständig zerstört.

Die Tatbegründung – mit Bezug auf die „militante Kampagne“ – ist eindeutig: „Bild“-Zeitung sowie der Springer-Konzern *zögen „den emanzipatorischen Widerstand“* gegen den G8-Gipfel *„durch den Dreck“*. Zudem stelle die „Bild“-Zeitung eine *„bedeutende Säule für den Erhalt des kapitalistischen Systems in der BRD“* dar.

- Der letzte Brandanschlag mit ausdrücklichem Bezug auf die „militante Kampagne“ fand statt am 25.Juni 2007 in Berlin. Betroffen waren zwei Fahrzeuge der Deutschen Post AG bzw. deren Tochtergesellschaft DHL.
  Die DHL, so war zu lesen - unterstütze den US-amerikanischen Krieg im Irak, indem sie die dortigen US-Truppen mit Post und Gütern aller Art beliefere. Man habe die Fahrzeuge in Brand gesetzt, um *„ein wenig Sand in die Kriegsmaschinerie zu streuen und auf die Beteiligung Deutschlands auch in diesem Krieg aufmerksam zu machen“*.

Aber auch die vergangenen Monate belegen, dass die ideologisch bedingte Gewaltaffinität von Linksextremisten angesichts klarer Feindbilder aus sich heraus trägt und auch ohne konkrete Impulse eine hohe Intensität besitzt.

Einige Beispiele:

- Am 7.April 2008 verübten unbekannte Täter einen Brandanschlag auf das Gebäude des Rüstungszulieferers HAKO/Multicar.

- Am 27.Mai begingen anonyme Personen auf der Baustelle eines Berliner Wohnprojekts einen Brandanschlag auf einen 60 Tonnen schweren Teleskop-Autokran. Es entstand Sachschaden von etwa 200.000 Euro.

- Am 28.Mai gingen am Gebäude der Softwareentwicklungsfirma SAP in Berlin-Mitte 18 Schaufensterscheiben zu Bruch. Zur Begründung hieß es, die Firma entwickele Software für Sicherheitsbehörden und militärische Organisationen.

- Am 29.Mai zerstörten Unbekannte auf dem Firmengelände der Berliner Autovermietung Robben & Wientjes zwölf Transporter durch Brandsätze. Weitere 24 – in der Nähe stehende – Fahrzeuge wurden erheblich beschädigt.
  Allein hier entstand Sachschaden von über 1,1 Mio. Euro. In einem Selbstbezichtigungsschreiben warfen die Täter dem Unternehmen vor, an Räumungen und Zwangsumzügen beteiligt zu sein und sich damit zum „Teil der Verdrängung alternativer Lebensformen durch ‚Stadtteilveredelung‘“ zu machen.

Die drei letztgenannten Anschläge standen im Zusammenhang mit den so genannten autonomen „Freiräume-Aktionstagen“. Insgesamt kam es in dieser Woche zu 21 Brandanschlägen, 9 weiteren Sachbeschädigungen und 3 Hausbesetzungen.

Es folgten:

- Am 5.August ein Brandanschlag auf Fahrzeuge des Lebensmittelgroßhandels Schaper in Oranienburg. In einer kurzen Taterklärung hieß es, das Unternehmen verkaufe „ungenießbare Nahrungsmittel zu sehr hohen Preisen“; die Aktion sei

mithin Ausdruck des „Protests gegen ein System, in dem private Firmen mit Hilfe der Inhaftierung von Menschen Profite erwirtschaften“.

- Mit einer ähnlichen Begründung wurden in der Nacht zum 8.August in Berlin Fahrzeuge der Firma Siemens in Brand gesetzt. Die Taterklärung war gezeichnet mit „flammende grüsse“
- Am Beispiel der Firma K&S - Dr. Krantz Sozialbau und Betreuung im schleswig-holsteinischen Pinneberg wird besonders deutlich, auf welche Weise ein Unternehmen in das Zielspektrum militanter Aktivisten gerät. So wurde gegen K&S seit Monaten vor allem als Betreiber einer Gemeinschaftsunterkunft agitiert. Zunächst berichtete die „taz“ in einer Mai-Ausgabe über angeblich unhaltbare Zustände in dem Wohnheim. Später erschienen ähnliche Artikel in der marxistischen Tageszeitung „junge Welt“ sowie in der linksextremistischen Wochenzeitung „Jungle World“. Ganze Wohneinheiten – so heißt es in den Beiträgen – seien von Schimmel befallen und Gemeinschaftseinrichtungen defekt oder nicht zugänglich; zudem schikaniere das Personal die Bewohner. Zuvor hatte bereits das linksextremistische Szeneblatt „INTERIM“ entsprechend gegen K&S agitiert. Anfang Juni schließlich demonstrierten Flüchtlinge und Aktivisten vor der Firmenzentrale von K&S im niedersächsischen Sottrum. Am 13.August gipfelte die Kampagne dann in einem Brandanschlag mit erheblichem Sachschaden.

Bewertung und zum Ausblick

Nach unserer Einschätzung werden Wirtschaftsunternehmen auch künftig im Zielspektrum militanter Linksextremisten stehen.

Nach wie vor gibt es einige, wenn auch wenige, klandestine Strukturen im Linksextremismus, die die militante Intervention propagieren und in der Lage sind, sie gegen Wirtschaftsunternehmen umzusetzen.

Dies gilt generell, d.h. unabhängig von Sondersituationen wie etwa Heiligendamm 2007, dem bevorstehenden NATO-Gipfel 2009 oder dem G8 - Treffen 2009 in Italien.

Wenngleich solche Anlässe stets zu einer quantitativen wie qualitativen Verdichtung militanter Aktivitäten führen.

So gibt es ganz aktuell einen Aufruf antimilitaristischer Gruppen,
„am Beispiel des zivil-militärischen Unternehmens DHL die Kritik an der NATO … praktisch werden zu lassen“ sowie „Aktionstage gegen Rüstungsbetriebe und die Commerzbank“ zu organisieren.

Während die Commerzbank „im Bereich der Wirtschaft mit an vorderster Front im Bereich der Akzeptanzbeschaffung für die Bundeswehr“ stehe, habe sich die DHL als „Deutsche Heeres Logistik“ entpuppt und biete sich daher für eine „aktionsbezogene Mobilisierung im Vorfeld der NATO-Feierlichkeiten“ an.

Die Analyse zeigt, dass es bei der anhaltenden Bedrohung durch politische Fanatiker bleibt, die willens sind, dass ihnen verhasste Wirtschaftssystem in jeder Weise zu

schädigen.
Allerdings: Mit vorsätzlichen Personenschäden ist gegenwärtig nicht zurechnen. D.h., das militante Aktionsniveau geht derzeit nicht über die Ebene der Sachbeschädigungen - also nicht über „ … das kurzfristige ERSCHRECKEN DER ETABLIERTEN“ - hinaus. Und damit wird die Gewaltaffinität absehbar nicht in Terrorismus umschlagen.

Dies ist natürlich keine Gewähr für alle Zeit. Szeneintern sieht man aber, dass Personenschäden dem eigenen Milieu – grundsätzlich – nicht vermittelbar sind. Man würde sich politisch isolieren und auch jegliches Verständnis bei den zu gewinnenden Bevölkerungsgruppen verlieren. Gleichwohl ist an dieser Stelle größte Aufmerksamkeit geboten.

Eine regionale oder thematische Zieleingrenzung militanter Aktionen ist indessen kaum möglich und somit bleibt eine darauf aufbauende umfassende Prävention nahezu ausgeschlossen.

Ebenso ist nicht exakt prognostizierbar, wer wann Opfer werden kann. Eine solche Analyse ist aufgrund der Breite denkbarer politischer Begründungszusammenhänge sowie der daraus resultierenden Anzahl potentieller Anschlagsziele nicht zu erreichen.

Ungeachtet bleibt es das nachdrückliche Bemühen der Verfassungsschutzbehörden, den Tätern auf der Spur zu bleiben und auch klandestine Strukturen aufzuklären. Nur so kann der präventive Verfolgungsdruck auf die Szene erhalten bleiben.

Man muss allerdings deutlich machen, dass diese Aufgabe Kontinuität und vor allem einen langen Atem verlangt.