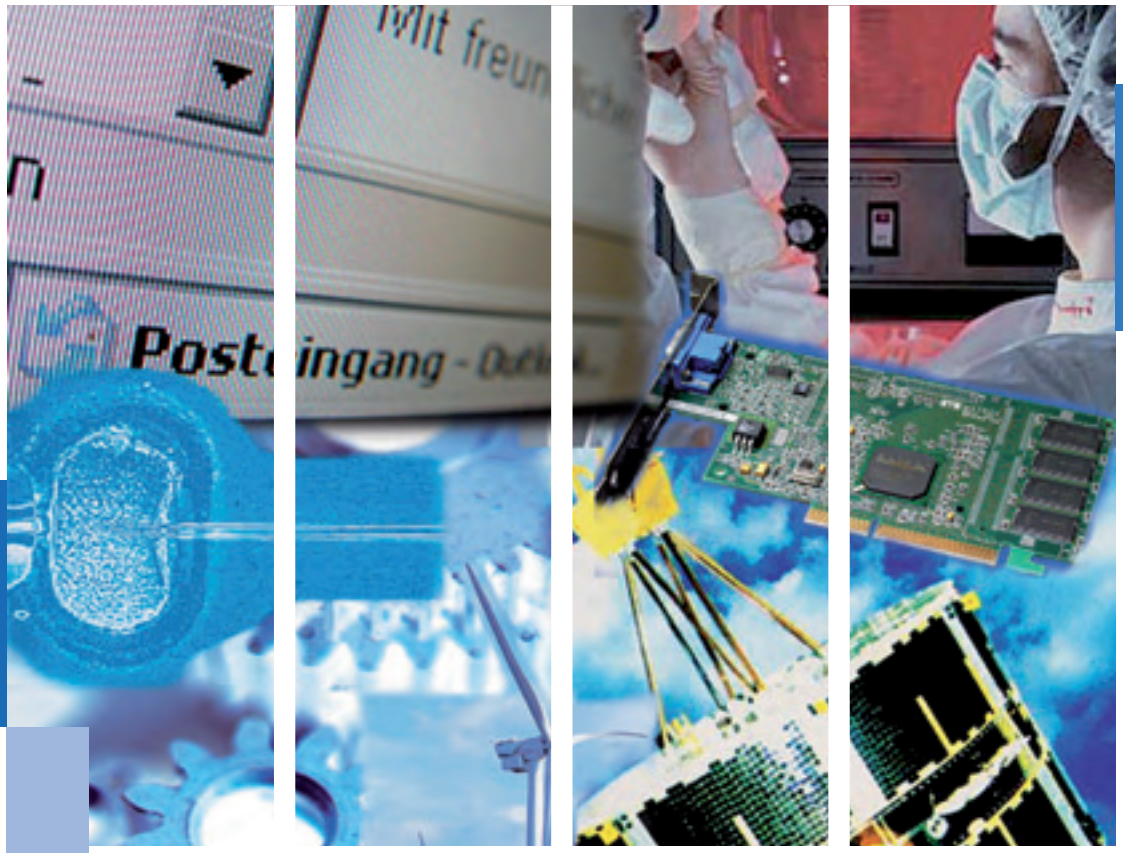
Bundesamt für
Verfassungsschutz

ASW
Zentralorganisation der Wirtschaft

Wirtschaftsschutz: Prävention durch Information

5. Sicherheitstagung des BfV und der ASW am 30. Juni 2011 in Köln



Tagungsband

„Proaktiver Wirtschaftsschutz: Prävention durch Information“

5. Sicherheitstagung des BfV und der ASW am 30. Juni 2011 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

5. Sicherheitstagung des BfV und der ASW am 30. Juni 2011 in Köln

Vizepräsident des BfV Dr. Alexander Eisvogel und der Vorsitzende der ASW Jörg Peter

Die 5. Sicherheitstagung des Bundesamtes für Verfassungsschutz und der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V (ASW) fand unter dem Motto „Proaktiver Wirtschaftsschutz: Prävention durch Information“ statt. Zahlreiche Vertreter von Unternehmen und Wirtschaftsverbänden sowie Mitarbeiter von Ministerien und Sicherheitsbehörden nahmen an dem jährlichen Treffen teil. Die Referate von Sicherheitsexperten aus Behörden und der Wirtschaft zu diversen Aspekten des Wirtschaftsschutzes regten einen vielfältigen Informations- und Meinungsaustausch an.

Die gemeinsamen Sicherheitstagungen sind Teil umfangreicher Maßnahmen im Bereich der Information und Sensibilisierung durch das BfV und seines Kooperationspartners 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!“

Grußrede des Vizepräsidenten des Bundesamtes für Verfassungsschutz

Dr. Alexander Eisvogel

Sehr geehrte Damen und Herren,
ich begrüße Sie herzlich - auch im Namen von Herrn Präsident Fromm, der leider heute nicht anwesend sein kann - zur diesjährigen Sicherheitstagung, gemeinsam durchgeführt von der Arbeitsgemeinschaft für Sicherheit der Wirtschaft und dem Bundesamt für Verfassungsschutz. Die mittlerweile fünfte Zusammenkunft dieser Art ist ein sichtbares Zeichen für die bewährte und erfolgreiche Kooperation, die uns im Rahmen der Sicherheitspartnerschaft von Staat und Wirtschaft mit der ASW verbindet.

Vielleicht ist Ihnen das auch aufgefallen: Das Motto der Tagung ist das gleiche wie im Vorjahr: „Proaktiver Wirtschaftsschutz: Prävention durch Information“. Ich darf denjenigen, die jetzt befürchten, möglicherweise handele es sich um ein Remake des Vorjahres (mit gleichen Referenten, gleichen Themen, gleichen Inhalten) versichern: Dem ist nicht so. Die Organisatoren verbürgen sich dafür und ein Blick auf das Programm bestätigt das auch. Die Veranstalter haben den gleichen Titel gewählt, weil er ein Markenzeichen der Veranstaltungsreihe wird. Mit ihm soll der Stellenwert der Prävention im Konzept der Bekämpfung der Wirtschaftsspionage hervorgehoben werden: Prävention als eine wesentliche Voraussetzung für den Schutz vor ungewolltem Know-how-Verlust und den damit verbundenen Folgen finanzieller und materieller Art. Wir müssen uns dabei immer vor Augen halten, dass es sich um Versuche der Wissensabschöpfung mit nachrichtendienstlichen Mitteln handelt – seien sie computergestützt oder auf die klassische Art durch den Einsatz menschlicher Quellen.

Im Fokus der öffentlichen Wahrnehmung stehen derzeit vor allem die Risiken durch elektronische Angriffe. Es vergeht kaum ein Tag ohne Berichterstattung über Hackerangriffe auf Unternehmen, Organisationen und Behörden, vor allem aber vergeht kein Tag ohne einen tatsächlichen Angriff oder präziser (im Plural) ohne reale Angriffe: So wurden im Jahr 2010 allein 2.108 elektronische Attacken auf IT-Einrichtungen von Ministerien und Bundesbehörden festgestellt, das heißt – statistisch gesehen – sechs Angriffe pro Tag oder alle vier Stunden eine Attacke. Ein durchaus beunruhigender Gedanke – finden Sie nicht auch? Dabei sind Angriffe auf die Wirtschaft noch nicht einmal in dieser Zahl enthalten (da hier keine zentrale Erhebung erfolgt). Ich freue mich daher, dass wir auch zu diesem Thema, insbesondere zur Einrichtung des „Cyber-Abwehrzentrums“ heute noch mehr erfahren werden.

Ich darf besonders den Vorsitzenden unseres Partners, der ASW, Herrn Peter, begrüßen, dem ich an dieser Stelle noch einmal zu seiner Wiederwahl gratulieren möchte. Ich bin ganz sicher, dass wir die gute und vertrauensvolle Zusammenarbeit fortsetzen werden. Herr Peter wird im Anschluss zu uns sprechen.

Ich freue mich insbesondere darüber, dass Vertreter aus der Wirtschaft in großer Zahl erschienen sind. Sehen Sie mir bitte nach, dass ich nicht alle Wirtschaftsvertreter namentlich begrüßen kann. Aber es ist mir persönlich wichtig, den früheren Präsidenten des BfV, Herrn Frisch, der heute im Rahmen seiner Tätigkeit für ein Unternehmen hier unter uns weilt, besonders zu begrüßen. Herzlich willkommen, Herr Frisch!
Natürlich bleiben wir bestrebt, den Dialog mit der Wirtschaft fortzusetzen und zu vertiefen. Schließlich wissen wir um den Wert konstruktiver Kontakte. Auf der Basis von Vertrauen und Verlässlichkeit sind sie unerlässlich für die Abwehr der vielfältigen Risiken durch Spionage und Ausspähung.

Ich freue mich, dass auch Vertreter des Bundesministeriums des Innern an der heutigen Veranstaltung teilnehmen.

Besonders begrüßen möchte ich auch die Vertreter der Dienste aus Österreich, Spanien, der Türkei und der Schweiz, insbesondere Herrn Studer, der uns über die Wirtschaftsspionage in seinem Heimatland informieren und uns darlegen wird, welche Erfahrungen die Schweiz mit Präventionsmaßnahmen gemacht hat.
Die Anwesenheit ausländischer Dienste zeigt uns, wie ernst das Thema Wirtschaftsschutz auch andernorts genommen wird. Hier gilt dasselbe wie bei anderen Gefährdungen der inneren Sicherheit: Notwendig ist nicht nur eine behördenübergreifende Zusammenarbeit unter Einbeziehung zivilgesellschaftlicher Akteure, sondern darüber hinaus stets auch eine internationale Kooperation.

Auch wenn wir das gleiche Motto wie im Vorjahr haben, setzen wir doch andere Schwerpunkte. Dafür sorgen neben Herrn Studer weitere hochrangige Referenten. Ihnen gilt mein besonderer Dank.

So freue ich mich darüber, dass es uns gelungen ist, Sicherheitsfachleute aus renommierten, international agierenden Konzernen als Referenten zu gewinnen. Ich begrüße (in der Reihenfolge des Programms)
den stellvertretenden Leiter „Group Business Security“ der Deutschen Telekom, Herrn Königshofen. Er wird heute Ausführungen zu möglichen Maßnahmen im Rahmen eines sehr vielversprechenden, zielgerichteten Abwehrkonzeptes seines Konzerns machen. Ich komme später noch einmal kurz darauf zurück.

Herrn Mille, den Leiter der Unternehmenssicherheit der Siemens AG, begrüße ich und danke zugleich an dieser Stelle noch einmal ausdrücklich dafür, dass Siemens BfV-Mitarbeitern eine Hospitation in der Unternehmenssicherheit ermöglicht. Wir sehen darin eine zukunftsweisende Maßnahme und zugleich adäquate Antwort auf die gemeinsamen Herausforderungen, die sich einem führenden Technologiekonzern im Bereich der Unternehmenssicherheit und einem Nachrichtendienst - zuständig auch für die Abwehr von Wirtschaftsspionage - gleichermaßen stellen.

Schließlich begrüße ich Herrn Hartmann, den Chef der Sicherheitsabteilung von SAP. Herr Hartmann wird uns die besonderen Herausforderungen im Bereich des Security Awareness für ein weltweit agierendes Softwareunternehmen (wie SAP) darstellen.

Seien Sie alle herzlich willkommen.

Ich hoffe, dass wir viel Neues erfahren werden über die Risiken, nicht nur für Global Player, und wir Informationen erhalten darüber, wo die Gemeinsamkeiten, wo die Unterschiede der Gefahrenanalyse liegen zwischen Technologie-, Kommunikations- und Softwarebranche. Wie sehen die unterschiedlichen Programme zur Gefahrenabwehr aus? Gibt es spezielle Erwartungen an den Staat, an die Behörden für Verfassungsschutz– das interessiert uns beim BfV natürlich besonders. Die prominente Besetzung schürt Erwartungen, und ich denke, sie werden nicht enttäuscht. Vor Veranstaltungsbeginn lag mir die Zusammenfassung des Beitrages von Herrn Königshofen vor. Ihm möchte ich ganz ausdrücklich für diesen gleichermaßen pragmatischen und klugen Text zum neuen Spionageabwehr-Konzept der Deutschen Telekom danken. Er gehört zum Besten, was ich in letzter Zeit zu diesem Thema gelesen habe.

Bedanken möchte ich mich natürlich auch bei den Mitarbeitern des BfV, die heute hier referieren.

Herr Mesic wird uns einen aktuellen Überblick über Bedrohungen durch elektronische Angriffe geben, eine Form der Bedrohung, der nicht nur Behörden ausgesetzt sind, sondern auch Wirtschaftsunternehmen. Wir werden uns mit diesem Thema weit intensiver befassen müssen als wir das in der Vergangenheit getan haben. Viele glauben, es handelt sich hierbei um eine möglicherweise existenzielle Gefahr, eine Gefahr, nicht nur für einzelne Bereiche, sondern für das Funktionieren unseres Gemeinwesens insgesamt, eine Bedrohung unserer sozialen und politischen Ordnung. Das in diesem Monat gegründete „Cyber Abwehrzentrum“ ist ein erster wichtiger Schritt hin zu einer adäquaten Gefahrenabwehr.

Schließlich wird uns Herr Selzner die Gefahren aufzeigen, die von einem gewaltorientierten Linksextremismus für die Wirtschaft ausgehen. Wirtschaftsschutz ist mehr als lediglich Spionageabwehr. Es geht auch um Schutz vor Sabotage und Gewalthandlungen aus einer politischen Motivation.

Meine Damen und Herren,
die vor wenigen Wochen veröffentlichten Ergebnisse der aktuellen Wik/ASW-Sicherheitsenquete 2010/2011 haben erneut deutlich gemacht, dass illegaler Technologietransfer und Know-how-Abfluss eine Realität sind.
Gut die Hälfte der Befragten aus dem Sicherheitsmanagement von Unternehmen gab an, in den vergangenen beiden Jahren von Wirtschaftsspionage oder Konkurrenzausspähung betroffen gewesen zu sein.
Umso mehr besorgt uns, dass Sicherheitsbewusstsein und effektives Sicherheitsmanagement,

insbesondere in mittelständischen Unternehmen, weiterhin zu wenig ausgeprägt sind.
Auch scheuen betroffene Unternehmen oftmals davor zurück, mit dem Verfassungsschutz zusammenzuarbeiten und unsere Expertise in Anspruch zu nehmen um Angriffe aufzuklären oder abzuwehren.

Ich wiederhole deshalb unseren Appell: Suchen Sie den vertraulichen Kontakt mit den Mitarbeiterinnen und Mitarbeitern der Verfassungsschutzbehörden. Wir sind kein bloßer Selbstzweck, sondern für Sie da!

Die Prävention vor illegalem Know-how-Verlust steht nicht nur im Mittelpunkt der heutigen Tagung. „Prävention durch Information“ ist auch das Leitmotiv unserer Aktivitäten im Bereich Wirtschaftsschutz. Die Security-Awareness-Aktivitäten des BfV reichen von Informationsangeboten über Sensibilisierungsvorträge bis hin zu bilateralen Sicherheitsgesprächen.
Diese Aktivitäten sind eingebunden in die Kooperation mit anderen Behörden und Ministerien im Ressortkreis Wirtschaftsschutz.
Effektiver Wirtschaftsschutz aber braucht darüber hinaus die Abstimmung und Zusammenarbeit mit der Wirtschaft. Diesem Zweck dient die „Public-Private-Partnership“ mit der ASW als dem zentralen Ansprechpartner des Staates in der Wirtschaft.

Ich wünsche uns allen eine informative und interessante Veranstaltung.

Grußrede des Vorsitzenden der „Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.“

Jörg Peter

Lieber Herr Dr. Eisvogel,
meine sehr geehrten Damen und Herren,
liebe Kolleginnen und Kollegen,

auch im Namen der ASW darf ich Sie recht herzlich zur 5. Sicherheitstagung von BfV und ASW in Köln begrüßen. Besonders freue ich mich auch über die Teilnahme von zahlreichen Vertretern aus Unternehmen, Verbänden, Ministerien und Sicherheitsbehörden.

Meine Damen und Herren,
am 16. Juni 2011 hat sich der ASW-Vorstand neu formiert. Wir sind uns innerhalb der ASW einig darin, dass der Schutz der deutschen Unternehmen vor Wirtschafts- und Konkurrenzspionage nur durch eine enge und vertrauensvolle Zusammenarbeit von Staat und Wirtschaft Erfolg haben wird. Das Thema Wirtschaftsschutz wird in naher Zukunft noch mehr als bisher Herausforderung für das Wirken der ASW zur Sicherung des Wirtschaftsstandortes Deutschland und seiner global tätigen Unternehmen sein. Die bereits seit 2 Jahren fortschreitende kriegerische Auseinandersetzung im und um den virtuellen Raum der Informationstechnik hat schon lange kein rein militärisches Ziel mehr. Die ASW wird sich auch hier den Erwartungen stellen müssen, die erforderliche Kernkompetenz weiter auszubauen und das Thema Informationsschutz und -sicherheit in ihre Verantwortlichkeit aufzunehmen.

Sehr geehrter Herr Dr. Eisvogel,
bei der Vielzahl der Herausforderungen, die auf die Wirtschaft zukommen, ist es beruhigend, einen starken Partner wie das BfV an seiner Seite zu wissen. Hierfür herzlichen Dank an Herrn Fromm und Sie sowie an alle Mitarbeiter des BfV, die mit ihrem Einsatz die gemeinsame Arbeit des BfV mit der ASW unterstützen.

Mein Dank gilt auch dem Staatssekretär des Innern, Herrn Klaus- Dieter Fritsche. An dieser Stelle begrüße ich stellvertretend für das BMI Herrn Akmann. Das Thema Wirtschaftsschutz ist durch das Engagement des Herrn Staatssekretär Fritsche in der Bundesregierung und in der Öffentlichkeit zum Top-Thema gekürt worden.

Seit meinem Amtsantritt im September 2010 ist es Herr Staatssekretär Fritsche, der mich im Glauben an einen gemeinsamen Erfolg von Wirtschaft und Bundesregierung im Kampf gegen die Wirtschaftskriminalität maßgeblich stärkt. Dafür, Herr Staatssekretär, und auch Ihnen, Herr Akmann, herzlichen Dank!

Aus den Gesprächen mit Herrn Fritsche und Verantwortlichen der Sicherheitsbehörden von Bund und Land kann ich Ihnen nahe legen: Erkennen Sie die Signale der Bereitschaft zur Zusammenarbeit und lassen Sie uns die damit verbundenen Ziele nicht aus den Augen verlieren. Die derzeitige teilweise bestehende Unsicherheit der Wirtschaft und deren Spitzenverbände in Sicherheitsfragen stellt für uns alle eine nachhaltige Herausforderung dar, der wir gewachsen sein müssen. Fachkompetenz allein wird uns an dieser Stelle nicht weiter voran bringen. Ein gut organisiertes Netzwerk an Fachkompetenz in Verbindung mit einem durchdachten Marketingkonzept ist gefordert. Vorbei sind die Zeiten, in denen Sicherheitsverantwortliche auf Artikel guter Journalisten hoffen, um unsere Belange im Unternehmen endlich an den Mann zu bringen. Sicherheit braucht eine eigene Lobby.

Ein weiterer positiver Meilenstein in Bezug auf die Zusammenarbeit von Staat und Wirtschaft stellt der Ressortkreis Wirtschaftsschutz dar. Ich hatte bereits Gelegenheit, an Sitzungen dieses Gremiums als ASW-Vertreter teilzunehmen und habe einen weiteren sehr positiven Eindruck von der Zusammenarbeit zwischen Staat und Wirtschaft gewonnen. Im Rahmen des Ressortkreises Wirtschaftsschutz wurde auch ein gemeinsames Projekt zur Informationsgewinnung der Wirtschaft in Sicherheitsfragen, die Sicherheits-Plattform, ins Leben gerufen.

Ich freue mich ganz besonders, dass heute einige Kollegen von uns aus anderen Unternehmen wie Herr Königshofen, Herr Mille bzw. Herr Hartmann mit interessanten Vorträgen aus der Unternehmenssicherheit das heutige Programm mit gestalten. Herzlichen Dank vorab für Ihre Vorträge.

Meine Damen und Herren, ich denke, dass es dem BfV in Kooperation mit der ASW gelungen ist, ein interessantes Programm für uns zusammenzustellen. Insofern gilt bereits an dieser Stelle mein Dank bei der Konzeption und Realisierung der heutigen Sicherheitstagung Herrn Kurek und seinem Team auf Seiten des BfV sowie auf Seiten der ASW dem Geschäftsführer Herrn Dr. Stoppelkamp.

Uns allen wünsche ich eine informative und interessante Veranstaltung

Das neue Spionageabwehr-Konzept der Deutschen Telekom

**Referent: Thomas Königshofen, Konzern-Sicherheitsbevollmächtigter,
Deutsche Telekom AG**

Einleitung

Mit der Globalisierung der Märkte einhergehend hat sich der Rohstoff „Information" als immer wichtigeres Gut im internationalen Wettbewerb entwickelt. Da ist es nicht verwunderlich, dass sich die Meldungen über Spionage-Aktivitäten von Wirtschaftsunternehmen untereinander, aber auch von nachrichtendienstlichen Aktivitäten gegen einzelne Wirtschaftsunternehmen häufen.

Patente und Erfindungen, Kunden- und Lieferantendatenbanken, Preiskalkulationen und Marktstrategien, aber auch strategische Veränderungen eines Unternehmens wie z.B. beabsichtigte Unternehmensteil-Verkäufe und Unternehmenskäufe stellen Know How dar, das einen hohen Informationswert hat. Mit der steigenden Nachfrage nach diesen wettbewerbsrelevanten und vielleicht sogar wettbewerbsentscheidenden Informationen wächst auch das Angebot, diese Informationen mit nachrichtendienstlichen Mitteln zu beschaffen.

Hierdurch steigt die Gefahr des Verlustes der Vertraulichkeit dieser Unternehmenswerte rapide an, was wiederum zur Folge hat, dass die Unternehmen, die sich der wachsenden Gefahr ausgesetzt sehen, ihre Maßnahmen zum Schutz der Geschäftsgeheimnisse erhöhen müssen, um ihr bisheriges Sicherheitsniveau nicht zu verlieren. Dabei ist erstaunlich, dass sich nach einer jüngsten Umfrage der Fa. Ernst&Young vom April 2011[1] zwei Drittel der befragten Unternehmen einer steigenden Bedrohung durch Industriespionage ausgesetzt sahen, aber 83% dieser Unternehmen sich ausreichend geschützt wähnten, wobei bei 66% der Unternehmen der IT-Abteilung die Verantwortung für die Abwehr von Industriespionage zukam. Spätestens mit dem Bekanntwerden der Schadsoftware „Stuxnet" und ihrer Wirkungsweise ist aber deutlich geworden, das die klassischen IT-Schutzmaßnahmen gegen vergleichbare Virenattacken nicht mehr ausreichend sind und folglich die IT-Abteilung eines Unternehmens der Problematik nicht (mehr) alleine Herr werden kann.

1. Formen der Wirtschafts- und Konkurrenzspionage

Die nachrichtendienstlichen Methoden der Aufklärung bzw. Informationsgewinnung stehen einem Angreifer auf die Vertraulichkeit von Geschäftsgeheimnissen wie ein Werkzeugkoffer zur Verfügung. Dabei kann man zwischen den Formen der IT-Spionage (Signal-Intelligence, SIGINT), die sich auf Werkzeuge der Informations- und Telekommunikationstechnologie stützt und der Abschöpfung von Wissensträgern (Human-Intelligence, HUMINT) durch den Agenten unter Zuhilfenahme von psychologisch ausgefeilten Methoden der Vertrauensbildung und der Gesprächsführung unterscheiden.

[1] Ernst&Young, Studie „Datenklau", April 2011

Zu den wichtigsten Formen der sogenannten Signal-Intelligence gehören z.B.
- das Eindringen in die IT-Systeme des Opfers; - der Lauschangriff mit Hilfe von versteckten Mikrofonen, Kameras, etc.;
- der Lauschangriff mit Hilfe von Mikrofonen, Kameras etc.;
- die forensische Untersuchung zuvor gestohlener Datenträger (Laptops, Smartphones, USB-Sticks etc) mit dem Ziel des Auffindens geschützter Daten;
- die klassische Telekommunikationsüberwachung (z.B. mittels sogenannter Sniffer im Firmennetzwerk; aber auch
- die softwaregestützte Analyse sozialer Netzwerke im Internet (z.B. „facebook“) im Hinblick auf vertrauliche Informationen.

Auch im Bereich der Human-Intelligence wächst die Bedeutung sozialer Netzwerke im Internet (sog.Web 2.0 - Applikationen) ständig an. So kann sich ein Angreifer mit falscher Identität als „friend“ oder „follower“ leicht das Vertrauen des Opfers erschleichen und mit Hilfe des Internet die ersten intensiveren Kontakte vorbereiten.

Daneben ist aber auch das sogenannte „Social Engineering“ in seinen klassischen Ausprägungen, insbesondere im Bereich der telefonischen Kontakte, weiter zu beobachten. So geben sich die Angreifer häufig als Mitarbeiter von Software- oder Hardwareunternehmen oder auch als Internet-Provider aus, die mit Hilfe ausgeklügelter Gesprächsmethoden versuchen, den Gesprächspartnern die Unternehmensgeheimnisse (z.B. Passwörter) zu entlocken, oftmals mit Erfolg.

2. Herausforderungen im Hinblick auf die Spionage-Abwehr

Die Abwehr solcher Angriffe auf die Geschäftsgeheimnisse eines Unternehmens stellen dieses vor einige Herausforderungen:

Zunächst einmal ist es erforderlich, den Informations- und Datenschutz als ein Management-System zu etablieren. Hier helfen national und international anerkannte Standards wie BSI-Grundschutz und das Informationssicherheits-Managementsystem (ISMS) nach der ISO-Familie 27.000 ff. und eine prozessorientierte Risiko-Analyse der Datenverarbeitung sowie die Bestimmung der technischen und menschlichen „Geheimnis-Träger“.

Will man aber alle schützenswerten Informationen vor Angriffen mit nachrichtendienstlichen Mitteln wirksam schützen, so stößt ein internationales Großunternehmen schnell an die Grenzen der Praktikabilität.
Deshalb macht ein abgestuftes Konzept, basierend auf dem Wert eines Geschäftsgeheimnisses (im Sinne der Bewertung der Schadenshöhe bei Verlust der Vertraulichkeit) Sinn, das insbesondere die sogenannten „Kronjuwelen“, also die wenigen Prozent an TOP-Geschäftsgeheimnissen mit einem extrem hohen Wert für das jeweilige Unternehmen, in den Fokus stellt.

3. Entwicklung des neuen Konzepts

Mit diesen Grundannahmen startete das Sicherheitsmanagement des Konzerns Deutsche Telekom im Jahre 2009 ein Projekt, welches zum Ziel hatte, neue, international im Konzern verbindliche Sicherheitsanforderungen (sogenannte Security Requirements) zum Schutz von TOP-Geschäftsgeheimnissen zu entwickeln. Bei der Zusammenstellung des Projekt-Teams wurde besonders darauf geachtet, sowohl das fachliche Know-How der internen Sicherheitsexperten als auch die Erfahrung und Beratungskompetenz externer Sicherheitsberater und der deutschen Sicherheitsbehörden an Bord zu holen. So kamen die internen Sicherheitsexperten im Projekt aus den Tochtergesellschaften des Konzerns in Europa, Asien und den USA, als externes Beratungsunternehmen wirkte die Pinkerton Group (USA), eine Tochtergesellschaft der SECURITAS-Gruppe, mit.

Die deutschen Sicherheitsbehörden waren mit dem Bundeskriminalamt (BKA), dem Bundesamt für Verfassungsschutz (BfV) und dem Verfassungsschutz NRW vertreten. Dabei kam der Arbeitsgruppe insbesondere das umfangreiche Fachwissen der Verfassungsschutzbehörden bei der Evaluierung der Entwürfe der neuen Sicherheitsanforderungen sehr zu Gute. Im Dezember 2009 wurde das neue Konzept vom Konzernvorstand verabschiedet. Die Zustimmung des Konzernbetriebsrats folgte kurze Zeit später. Seit dem Jahre 2010 wird es nun Schritt für Schritt national und international implementiert. Als erste Pilotprojekte dienten dabei die Frequenz-Auktionen für den Mobilfunk in Deutschland und Österreich. Beim diesjährigen „Top Management Team Meeting“ wurde das neue Konzept als Beispiel für gelungene Innovation vor rund eintausend internationalen Top Managern des Konzerns Deutsche Telekom präsentiert.

4. Grundpfeiler des neuen Konzepts

Als Grundpfeiler des Spionage-Abwehr-Konzepts dienen die bisherigen umfassenden Maßnahmen des Konzerns zum Informations- und Datenschutz, die als Basis dienen, auf der dann maßgeschneiderte Zusatz-Schutzmaßnahmen aufsetzen.

Zu den Basis-Schutzmaßnahmen des Konzerns zählen dabei der vorhandene zertifizierte IT-Grundschutz nach ISO 27001, die Implementierung des Business Continuity Management Systems nach BS 25999 sowie das Datenschutz- und Sicherheitsmanagement mit dem Kernprozess des sogenannten „Privacy and Security Assessment (PSA). Daneben wären auch die Schulungs- und Awarenesskonzepte des Konzerns zu den Themen Datenschutz und Sicherheit zu nennen, bei denen z.B. jeder Mitarbeiter standardmäßig ein Web Based Training zum Datenschutz und zur Informationssicherheit zu absolvieren hat.

Zu diesen Basis-Schutzmaßnahmen wird nun ein Zusatz-Schutz durch verbindliche neue Sicherheitsanforderungen verankert:

- die Identifzierung und der Schutz von sogenannten Top-Geschäftsgeheimnissen (Top- Business Secrets, TBS) in einem rollen- und prozessbasierten Modell;
- die Erhöhung der allgemeinen und speziellen Awareness durch zielgruppenorientierte

Schulungen und Informationen einschließlich spezieller Web Based Trainings zum Thema „Social Engineering“; sowie
- die Messung des Informationsschutz-Levels der Dienstleister und Lieferanten des Konzerns durch Einführung eines Scoring-Systems, das bei Einkaufsentscheidungen von sicherheitskritischen Komponenten zu berücksichtigen ist.

Für die Identifizierung der Top-Geschäftsgeheimnisse wurde ein Risk-Assessment verankert, das – basierend auf den Auswirkungen des Vertraulichkeitsverlustes – die Top-Geschäftsgeheimnisse als Teil der im Konzern höchsten Infoschutz-Kategorie „streng vertraulich“ („strictly confidential“) einstuft, welches aber der besonderen Gefährdung durch Angriffe mit nachrichtendienstlichen Rechnung trägt.

Für die Identifikation und die Festlegung der Schutzmaßnahmen wurde außerdem eine rollenbasiertes Modell entwickelt, wobei davon ausgegangen wurde, das das Top Management in der Regel auch über die Top-Geschäftsgeheimnisse Bescheid weiß bzw. von ihnen Kenntnis erhält. Diese Gruppe, die sogenannten TBS-Owner, wird deshalb besonders im Hinblick auf die neuen Sicherheitsanforderungen geschult.

Aus der Gruppe der TBS-Owner bestimmt sich dann der jeweilige TBS-Identifier, der zunächst einmal die Verantwortung für den Schutz eines konkreten Geschäftsgeheimnisses hat (z.B. der Leiter „Mergers & Acquisitions“ bei einem geplanten An- oder Verkauf eines Unternehmensteils). Sobald dieser von einem TBS erfährt oder ein solches erwartet (z. B. das Zielobjekt und das Maximal-Angebot für einen Unternehmens-Ankauf), kann er dann mit dem sogenannten Spionageabwehr-Beauftragten (Counter Espionage Officer, CE-Officer) Kontakt aufnehmen. Gemeinsam werden dann eine spezielle, projektorientierte Risiko-Analyse durchgeführt und konkrete Schutzmaßnahmen vereinbart, für deren Umsetzung der Spionageabwehr-Beauftragte verantwortlich ist.

Dieser Spionageabwehr-Beauftragte ist durch die Geschäftsführung eines jeden selbständigen Konzern-Unternehmens mit Zustimmung des Sicherheits-Chefs (Chief Security Officers, CSO) des Unternehmens zu bestellen.

Die Spionageabwehr-Beauftragten werden von Experten des Konzerns geschult und auf ihre Aufgabe vorbereitet. Verantwortlich hierfür ist die Abteilung Geheim- und Sabotageschutz, die vom Konzern-Sicherheitsbevollmächtigten geleitet wird. Diese Abteilung, die auch als „Center of Excellence“ für den Spionageabwehr-Prozess im Konzern verantwortlich ist, verantwortet auch die sogenannte Toolbox, also den „Werkzeugkasten“ mit den Werkzeugen, die für die Umsetzung der besonderen technischen und nichttechnischen Schutzmaßnahmen erforderlich sind, wie z.B. Krypto-Handys und Präsentations-Unterlagen für Sicherheits-Schulungen. Daneben sorgt das „Center of Excellence“ für die Awareness des Konzernvorstands, für den Informations- und Erfahrungsaustausch unter den Experten, für den Aufbau und die Pflege einer „Incident“-Datenbank, wo z.B. vermutete oder tatsächliche Fälle von Spionage und Fälle von Social Engineering konzernweit erfasst und ausgewertet werden, sowie für die kontinuierliche Verbesserung der Spionageabwehr-Prozesse.

5. Konzernweite Implementierung

Ganz nach dem Prinzip, das Leben für die Agenten der Wirtschaftsspionage schwieriger zu machen, wird das neue Konzept im Konzern nach und nach ausgerollt. So haben gerade im Monat Juni 2011 die ersten Schulungen für die Counter-Espionage Officer der asiatischen Tochtergesellschaften des Konzerns in Kuala Lumpur (Malaysien) stattgefunden. Zeitgleich bereiten wir uns auf den Schutz der Top-Geschäftsgeheimnisse bei den milliardenschweren Frequenzauktionen in Griechenland in diesem Sommer vor.

6. Erste Erfahrungen

Wie jeder neue Prozess hakt auch die Einführung des neuen Konzepts zur Abwehr von Wirtschafts-und Konkurrenzspionage an vielen Ecken und Enden. Die Probleme reichen von der Bereitstellung von Ende-zu-Ende-Verschlüsselungssystemen für die verschiedenen digitalen und analogen Telefonverbindungen in der Welt bis hin zu Reisebeschränkungen der benannten Counter Espionage Officer durch das lokale Management (aus Kostengründen). Gleichwohl kann schon jetzt gesagt werden, dass die Unterstützung durch die Spionageabwehrbeauftragten sehr gerne angenommen wird, da sie dem verantwortlichen Management hilft und es nicht übermäßig belastet, zumal die Hilfsmittel zum Schutz (wie z.B. auch das SiMKo 2, das derzeit wohl sicherste Smartphone) weitgehend zentral vorgehalten und für die Projekte vom Telekom Sicherheitsmanagement zur Verfügung gestellt werden. Auch das Konzept des Scorings unserer wichtigen Lieferanten und Geschäftspartner unter dem Gesichtspunkt des jeweiligen Sicherheitslevels kommt gut an, zumal Anstrengungen der Partner im Hinblick auf den Level der eigenen Informationssicherheit nun im Einkaufsprozess positiv berücksichtigt werden.

7. Fazit

Nach den bisherigen Erfahrungen lässt sich folgendes Zwischenfazit ziehen:

1. Wirtschafts- und Wettbewerbsspionage ist ein Risiko, das bei vielen Unternehmen mit schützenswertem Know-How oder schützenswerten Informationen (z.B. Strategien, Wirtschafts- und Vertriebspläne, FuE-Ergebnisse, Marketingpläne, Kunden- und Personaldaten) zunehmend ernster genommen wird.

2. Effektive Präventionskonzepte zum Schutz vor Wirtschafts- und Wettbewerbsspionage mit dem Ziel, unter Beachtung einer sinnvollen Kosten-Nutzen-Relation die Risiken deutlich und nachhaltig zu minimieren, bedürfen einer ganzheitlichen Betrachtungsweise, die nur im Sinne eines strategischen Ansatzes zum Management der schützenswerten Informationen und der Informations- und ITK-Sicherheit „state of the art“ gelingen kann.

3. Top-Geschäftsgeheimnisse sind nur ein sehr kleiner Anteil des schützenswerten Unternehmens-Know-Hows, haben aber einen hohen Wert für Nachrichtendienste und Wettbewerber. Entsprechend aufwändig sind die nachrichtendienstlichen Methoden, um an diese Geheimnisse heranzukommen. Dem müssen die Schutzmaßnahmen für die Zeit der Notwendigkeit strikter Geheimhaltung entsprechen. Klassische IT-Security und Infoschutz-Ansätze reichen nicht.

4. Ein modulares Schutzkonzept basierend auf der Identifikation jedes einzelnen Top-Geschäftsgeheimnisses ist skalierbar, bezahlbar und umsetzbar. Und es senkt effektiv die Gefahr eines Vertraulichkeitsverlustes.

Lagebild Wirtschaftsspionage/Wirtschaftsschutz in der Schweiz

Referent: Roman Studer, „Nachrichtendienst des Bundes“ Schweiz

Die Tatsache, dass innere und äußere Sicherheit seit Jahren untrennbar verbunden sind, hat das Schweizer Parlament bewogen, die gemeinsame Unterstellung von Inland- und Auslandnachrichtendienst unter ein Departement, dem Departement für Verteidigung, Bevölkerungsschutz und Sport, kurz VBS, festzulegen. Der Bundesrat, d.h. die Schweizer Regierung, ging dann den konsequenten nächsten Schritt und führte die beiden zivilen Nachrichtendienste auf 1.Januar 2010 zum neuen Nachrichtendienst des Bundes NDB zusammen. Dieser besorgt neu die zivilen nachrichtendienstlichen Tätigkeiten aus einer Hand – in Deutschland vergleichbar wäre das etwa die Zusammenlegung von BfV und BND.

Der NDB ist somit eine Organisation, die Informationen mit nachrichtendienstlichen Mitteln beschafft, analysiert, auswertet und verbreitet, mit dem Ziel, eine führungsrelevante Nachrichtenlage für Entscheidungsträger aller Stufen zu erstellen. Sie trägt mit operativen und präventiven Leistungen direkt zum Schutz der Schweiz bei.

Konkret heißt das, der NDB

- beschafft sicherheitspolitisch bedeutsame Informationen über das Ausland und wertet diese aus (früher: Auslandsnachrichtendienst SND)
- nimmt nachrichtendienstliche Aufgaben im Bereich der inneren Sicherheit wahr (früher: Inlandnachrichtendienst DAP)
- und stellt die umfassende Berteilung der Bedrohungslage sicher.

Diese umfassende Bedrohungslage beinhaltet in der neuen Organisationsstruktur sowohl die Bedrohungen von außen als auch diejenigen im innern der Schweiz. Der NDB legt in diesem Sinne auch der Öffentlichkeit jährlich eine Gesamtbeurteilung unter dem Titel „Sicherheit Schweiz“ vor. Diese beschränkt sich nicht auf den engeren Bereich der Sicherheitspolitik, sondern umfasst auch andere Bedrohungen, die der Schweiz Schaden zufügen können. Negative Entwicklungen in der Wirtschaft gehören damit ebenso zum Katalog der Bedrohungen wie schädliche Folgen der Interessenpolitik anderer Staaten.

Um die heutigen Fähigkeiten des NDB – insbesondere im Bereich Beschaffung – zu erhalten und auszubauen ist eine neue gesetzliche Regelung in Planung, die unter anderem dem NDB in besonderen Lagen zusätzliche gesetzliche Mittel zur Informationsbeschaffung ermöglichen soll. Das geplante neue ND-Gesetz wird dann die gesetzliche und umfassende Grundlage für den zivilen Nachrichtendienst der Schweiz bilden und wird die aktuell gültigen Grundlagen namentlich das Bundesgesetz über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes (ZNDG) und das Bundesgesetz zur Wahrung der inneren Sicherheit (BWIS) ablösen. Das zentrale Anliegen der Vorlage besteht darin, mit nachrichtendienstlichen Mitteln einen größtmöglichen Beitrag für die Sicherheit der Schweiz und ihrer Bürger zu gewährleisten.

Das Aufgabengebiet des NDB umfasst sechs nachrichtendienstliche Kernbereiche; dies sind:

- Terrorismusabwehr
- Proliferation
- Politische und wirtschaftliche Themen (mit den geographischen Schwerpunkten USA, GUS, Afrika, Asien, naher und mittlerer Osten)

- Abwehr von Gewaltextremismus
- Spionageabwehr
- Militärische und rüstungstechnische Themen

Diese Themen beschlagen teilweise die innere und äußere Sicherheit, teilweise nur einen Bereich, je nach tatsächlicher Bedrohungslage.

Als Querschnittsaufgabe behandelt der NDB ferner Angriffe auf die strategische Informationsinfrastruktur der Schweiz.

Diese Fokussierung ist notwendig, um die begrenzten personellen Kapazitäten des NDB gezielt einsetzen zu können und um in den politisch definierten Kernbereichen genügende nachrichtendienstliche Kenntnisse zu erwerben und zu erhalten. Eine prioritäre Stoßrichtung des Nachrichtendienstes des Bundes ist die Kundenausrichtung. Die Kundenbetreuung wird durch das Instrument der Steuerungsverantwortlichen intensiviert. Insgesamt sechs Steuerungsverantwortliche (entsprechend den sechs vorerwähnten nachrichtendienstlichen Kernbereichen gewährleisten die thematische Ausrichtung und die Leistungserbringung des NDB sowie die Liaison zwischen definierten Kundengruppen und dem NDB. Es geht dabei auch darum, die Bedürfnisse der Leistungsbezüger besser kennen zu lernen.

Damit komme ich im Nachfolgenden zu einigen konkreteren Ausführungen zu den Themenbereichen Wirtschaftsspionage/Wirtschaftsausforschung, dem Präventionsprogramm Prophylax des NDB und den Beiträge des NDB zum Schutz der Informationsinfrastruktur.

Ausländische Nachrichtendienste sind auch in der Schweiz aktiv.

Die illegalen Aktivitäten ausländischer Nachrichtendienste und anderer, auch privater Informationsbeschaffer in unserem Land verletzen die Sicherheitsinteressen der Schweiz, die Interessen von Drittstaaten sowie von internationalen Organisationen und gefährden die Sicherheit von in der Schweiz niedergelassenen Regimegegnern/Oppositionellen samt Angehörigen in den Herkunftsländern.

Die Attraktivität der Schweiz sowie die konkreteren Ziele für Beschaffungsaktivitäten fremder Nachrichtendienste begründen sich hauptsächlich wie folgt:
- Der hohe technologische Standard der Schweizer Industrie, der Forschungsstandort, die Hochschulen, die internationalen Forschungsgemeinschaften, die zentrale Lage in Europa, die UNO und andere internationale Gremien mit Schwerpunkt Genf, der Finanzplatz, der Energie und Rohstoffhandel, die gute Infrastruktur und die Kommunikationsmittel machen die Schweiz attraktiv als Ziel der Informationsbeschaffung seitens fremder Nachrichtendienste.
- Ausländische Regimegegner und Oppositionelle, die sich in der Schweiz niedergelassen haben, stellen ein weiteres Ziel ausländischer Nachrichtendienste dar.
- Staaten, welche für die Herstellung von Massenvernichtungswaffen die entsprechende Technik und das Know-how beschaffen wollen, versuchen in der Schweiz auch mit nachrichtendienstlichen Methoden ihre Ziele zu erreichen.

Schwerpunktmäßig sind ND-Aktivitäten der Nachrichten- und Sicherheitsdienste Russlands, Chinas, des Iran, Nordkoreas sowie in geringerem Ausmaße Länder des Nahen und Mittleren Ostens sowie Nordafrikas in unserem Land festzustellen. Es kann auch vorkommen, dass Interessen von Nachbarstaaten nicht immer vollständig mit denjenigen der Schweiz

übereinstimmen, was zur Folge haben kann, dass auch von dieser Seite illegale Aktivitäten auf schweizerischem Territorium vorgenommen werden. Dabei können nebst eigentlichen Geheimdiensten auch andere ausländische private oder staatliche Akteure eingesetzt werden. In jüngster Zeit war die Schweiz mehrmals mit unerlaubten Aktivitäten ausländischer Finanz-, Steuer- und Zollbehörden konfrontiert.

Die Bedrohung des schweizerischen Werk- und Finanzplatzes durch verbotenen wirtschaftlichen Nachrichtendienst und generell durch Wirtschaftsausforschung ist erheblich. Wiederholt konnte die Anwesenheit von Angehörigen ausländischer Nachrichtendienste in der Schweiz festgestellt werden. Diese suchten sowohl mit legalen wie auch illegalen Methoden nach Informationen, die für ihre Wirtschaftsinteressen beziehungsweise für ihren Forschungsstandort von Bedeutung sein könnten. Sollte sich die Finanz- und Wirtschaftskrise weiter verschärfen, wie sich im Moment leider abzeichnet, kann diese Bedrohung noch zunehmen.

Die negativen Folgen von Wirtschaftsspionage und Wirtschaftsausforschung sind beträchtlich:

- Sie bedeuten einen Abfluss von Know-how und damit eine Schädigung der Position der Schweiz im verschärften globalen Wettbewerb
- Sie wirken sich auf Unternehmungen aus mit Verlust von Aufträgen, einer schlechteren Position auf dem Markt und können damit zum Abbau von Arbeitsplätzen führen
- Sie haben generell negative Auswirkungen auf die Volkswirtschaft: Forschungs- u. Ausbildungskosten verlieren an Wert, Steuereinnahmen verringern sich.

Konkrete Zahlen zum Gefährdungspotential und zu den Kosten, die dem Staat, den Wirtschaftsbereichen, Firmen und Verbänden durch Wirtschaftsspionage, Wirtschaftsausforschung und Know-how-Abfluss erwachsen, sind nicht bekannt. Für die Schweiz liegt bis heute keine entsprechende wissenschaftliche Studie vor. Bekannt sind Ihnen vielleicht entsprechende Studien von Baden-Württemberg und Österreich.

Zur strafrechtlichen Bekämpfung von Wirtschaftsspionage und Konkurrenzausforschung stellt das Schweizer Recht eine Reihe von Normen zur Verfügung.

Ihre Anwendung richtet sich danach, ob die Wirtschaftsspionage von einer fremden amtlichen Stelle, oder einer ausländischen Organisation oder privaten Unternehmung oder deren Agenten ausgeht oder aber ob die Ausspähung eines Schweizer Unternehmens durch ein ebenfalls schweizerisches Konkurrenzunternehmen stattfindet.

Für die erste erwähnte Kategorie steht mit Art. 273 des Schweizerischen Strafgesetzbuches (Wirtschaftlicher Nachrichtendienst) ein taugliches Mittel zur Verfügung. Die Strafverfolgung dieses Offizialdelikts liegt in Bundeskompetenz; präventive Informationsbeschaffung erfolgt durch den Nachrichtendienst des Bundes. Fälle innerschweizerischer Konkurrenzausforschung werden unter Anwendung diverser Normen des Wettbewerbsrechts, des Bankengesetzes und des Strafgesetzbuches, namentlich auch Art. 162 StGB (Verletzung des Fabrikations- oder Geschäftsgeheimnisses) verfolgt. Es handelt sich dabei um ein Antragsdelikt in kantonaler Strafkompetenz. Das Problem liegt aber oft im Erkennen der Tathandlungen. Gut ausgeführte Spionage bleibt unsichtbar.

Der NDB besitzt derzeit kein ausreichendes politisches Mandat, um den Schutz des Finanz-, Wirtschafts- und Technologieplatzes Schweiz wahrzunehmen. Vor diesem Hintergrund ist einen Richtungsentscheid unserer Regierung in Vorbereitung bezüglich des zukünftigen Stellenwertes einer nachhaltigen nachrichtendienstlichen Bearbeitung von Themen mit Relevanz für den Schutz des Finanz-, Wirtschafts- und Technologieplatzes Schweiz. Die politische Diskussion zur skizzierten Problematik bzw. zur entsprechenden Mandatserweiterung des NDB ist angelaufen.

Präventions- und Sensibilisierungsprogramm Prophylax

International zeichnet sich die Schweiz durch einen wettbewerbsfähigen Werkplatz mit exzellenten Produkten auch im Hochtechnologiesektor aus. Diese Stärke ist auch für Staaten attraktiv, die den Besitz von Massenvernichtungswaffen anstreben. Deshalb suchen Akteure im Bereich Proliferation Kontakte in die Schweiz oder versuchen, selbst hier präsent zu sein. Oft berühren sich dabei die Themenfelder „Proliferation“ und „verbotener Nachrichtendienst“, da die Proliferationstätigkeit staatliches Handeln darstellen kann und vor allem bei sensitiven Beschaffungen durch nachrichtendienstliche Maßnahmen begleitet wird. Eine bewusste Kenntnis dieses Umstandes ist für die Wirtschaft wichtig, da eine Firma, die sensitive Kontakte zu Beschaffungsstrukturen in Risikoländern unterhält, sehr schnell auch zum Ziel von Nachrichtendiensten werden kann. Gleichermaßen ist Vorsicht auf dem Forschungs- und Ausbildungsplatz Schweiz geboten, da Proliferation den Wissenstransfer einschließt.

Den Interessen eines Kleinstaates wie der Schweiz läuft dies zuwider und sie bekämpft die Bemühungen ausländischer Staaten, in den Besitz von Massenvernichtungswaffen zu gelangen. Zur Wahrnehmung ihrer Verantwortung bei der Bekämpfung der Weiterverbreitung von Massenvernichtungswaffen sind die Behörden auf schlagkräftige Instrumente angewiesen. Dazu zählen beispielsweise moderne Methoden der Informationsbeschaffung und ein unkomplizierter Austausch von Daten zwischen den Dienststellen von Bund, Kantonen und ausländischen Dienststellen, aber auch und vor allem das erfolgreich durch den NDB geführte Präventions- und Sensibilisierungsprogramm Prophylax mit seinem dichten Kontaktnetz zur Industrie. Prophylax zeigt seit Jahren seine positive Wirkung.

Mit dem Präventions- und Sensibilisierungsprogramm Prophylax soll eine gezielte Sensibilisierung der Firmen erreicht werden. Dies geschieht durch regelmäßige Information und mit Pflege der Kontakte zu den Verantwortlichen in den verschiedenen Betrieben.

Hauptsächliche Ziele sind:

- Systematische und permanente Sensibilisierung
- Bekämpfung der Spionage und der illegalen Informationsbeschaffung
- Erkennung und Bekämpfung der Proliferation (Stärkung der Exportkontrolle)
- Beratung von Firmen, Forschungsinstituten und Hochschulen die über Expertise, Technologie oder Güter verfügen, die offizielle oder private Nachrichtendienste interessieren
- Informationsgewinnung des NDB und damit auch ein Instrument für die schweizweite Gefahrenanalyse

Die Hauptverantwortung über das Programm Prophylax liegt beim NDB. Er führt Buch über die offenen und getätigten Ansprachen, evaluiert neu einzubeziehende Firmen und Institutionen und wertet die Berichte der erledigten Ansprachen aus. Vermehrt werden Ansprachen von Spezialisten der Melde- und Analysestelle Informationssicherung (MELANI) begleitet. Dadurch können speziell Firmen in der Informatik- und Kommunikationsbranche und solche, die besonderen Bedarf an Informationssicherheit haben, optimal beraten werden.

Derzeit sind vom Programm PROPHYLAX rund 2'100 Firmen und 100 Forschungsinstitute und Hochschulen mit Domizil in der Schweiz und dem Fürstentum Liechtenstein erfasst. Die Liste basiert auf einer Evaluierung des NDB sowie auf Vorschlägen der kantonalen und städtischen Staatsschutzorgane. Bei der Entstehung des Präventionsprogramms im Jahre 2004 wurde der Fokus deutlich auf den Werkplatz Schweiz gelegt. Bis heute wurden rund 900 Firmen kontaktiert. Der Forschungs- und Bildungsplatz wird seit 2010 unter dem Begriff Technopole verstärkt berücksichtigt und kundengerecht betreut.

Am Ende der Ansprache werden die Firmen oder Institutionen jeweils nach ihrer Meinung in Bezug auf die Nützlichkeit des Programms gefragt. Eine Auswertung der diesbezüglichen Antworten zeigt, dass rund drei Viertel aller befragten Gesprächspartner die Sensibilisierung als nützlich eingestuft haben.

Die Erfahrungen in Zusammenhang mit Ansprachen bei Institutionen des Forschungs- und Bildungsplatzes Schweiz sind zum jetzigen Zeitpunkt noch bescheiden. Dies liegt daran, dass der Fokus in einer ersten Phase – wie vorerwähnt - auf den Werkplatz gerichtet wurde und erst wenige Institutionen der Bereiche Forschung und Bildung angesprochen worden sind. Erste Erfahrungen zeigen, dass Bildungs- und Forschungseinrichtungen, die nicht Bestandteil einer kommerziellen Struktur, also eines Unternehmens sind, tendenziell weniger Grundverständnis für Abwehranliegen haben, weil sie oft eine ausgeprägte Tendenz zur Offenheit pflegen.

Der NDB wird das Programm Prophylax weiterführen und vermehrt auch den Kontakt zum Forschungsplatz Schweiz intensivieren. Das Präventions- und Sensibilisierungsprogramm gilt dabei nicht nur der Proliferation, sondern auch der damit eng verknüpften Wirtschaftsspionage. In dieser Hinsicht wird politisch geprüft, wie bereits zu Beginn der Ausführungen skizziert, ob das Sensibilisierungsprogramm in einer geeigneten Form ebenfalls auf den Banken- und Finanzplatz Schweiz ausgeweitet werden soll.

SIEMENS

Corporate Security eines Global Players

Marco Mille,
Leiter Unternehmenssicherheit Siemens AG

5. Sicherheitstagung des BfV und der ASW
Köln | 30. Juni 2011

© Siemens AG 2011. All rights reserved.

Die Siemens AG
Megatrends, Vision und Kennzahlen

SIEMENS

Unsere Welt verändert sich

Urbanisierung

Demograf. Wandel

Klimawandel

Globalisierung

Kennzahlen (GJ 2010)

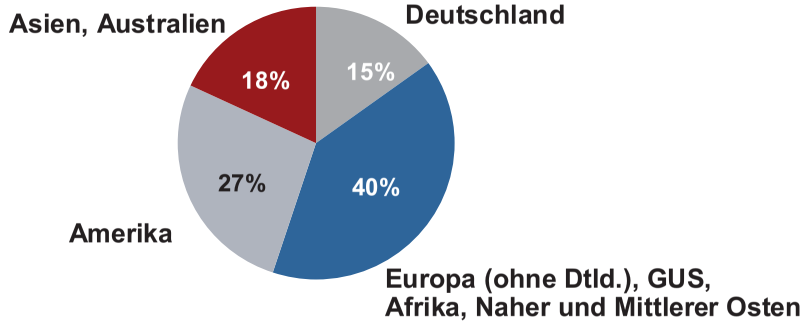
Umsatz:	76 Mrd. Euro
Ergebnis:	4,1 Mrd. Euro
Mitarbeiter:	405.000
Präsenz:	~ 190 Staaten
Standorte:	1.640 Standorten
Reisen/Tag	~ 35.000
Reiseregelungen:	~ 70 bis 80 Staaten

Siemens - der Pionier

gestern – heute – morgen

- Energieeffizienz
- Industrielle Produktivität
- Bezahlbare und personalisierte Gesundheitssysteme
- Intelligente Infrastukturlösungen

Umsatz nach Regionen



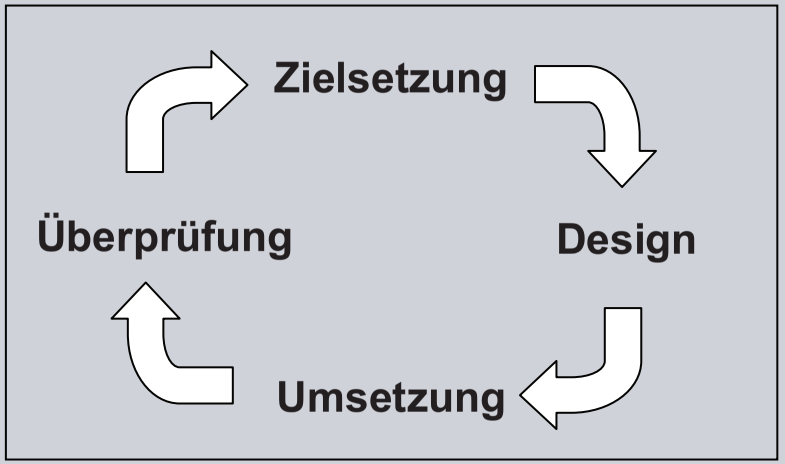
Die Siemens AG
Unternehmenssicherheit im Überblick

SIEMENS

- „Sicherheit“ als unternehmerische Verpflichtung der Siemens AG
- Unternehmenssicherheit: Der nachhaltige Schutz seiner Mitarbeiter, seiner Sach- und Vermögenswerte sowie des Know-how und anderer materieller wie immaterieller Unternehmenswerte
- Corporate Security Office (CSO): Unterstützung und Beratung des Vorstands und der Geschäftseinheiten in allen Fragen der Unternehmenssicherheit

Security-Themenfelder (CSO-Governance):

1. Reisesicherheit
2. Objektschutz
3. Projektsicherheit
4. Personen- und Veranstaltungsschutz
5. Informations-, Geheim- und Sabotageschutz
6. Krisenmanagement



Unternehmenssicherheit eines Global Players
Vom Cost Center zum Business Enabler …

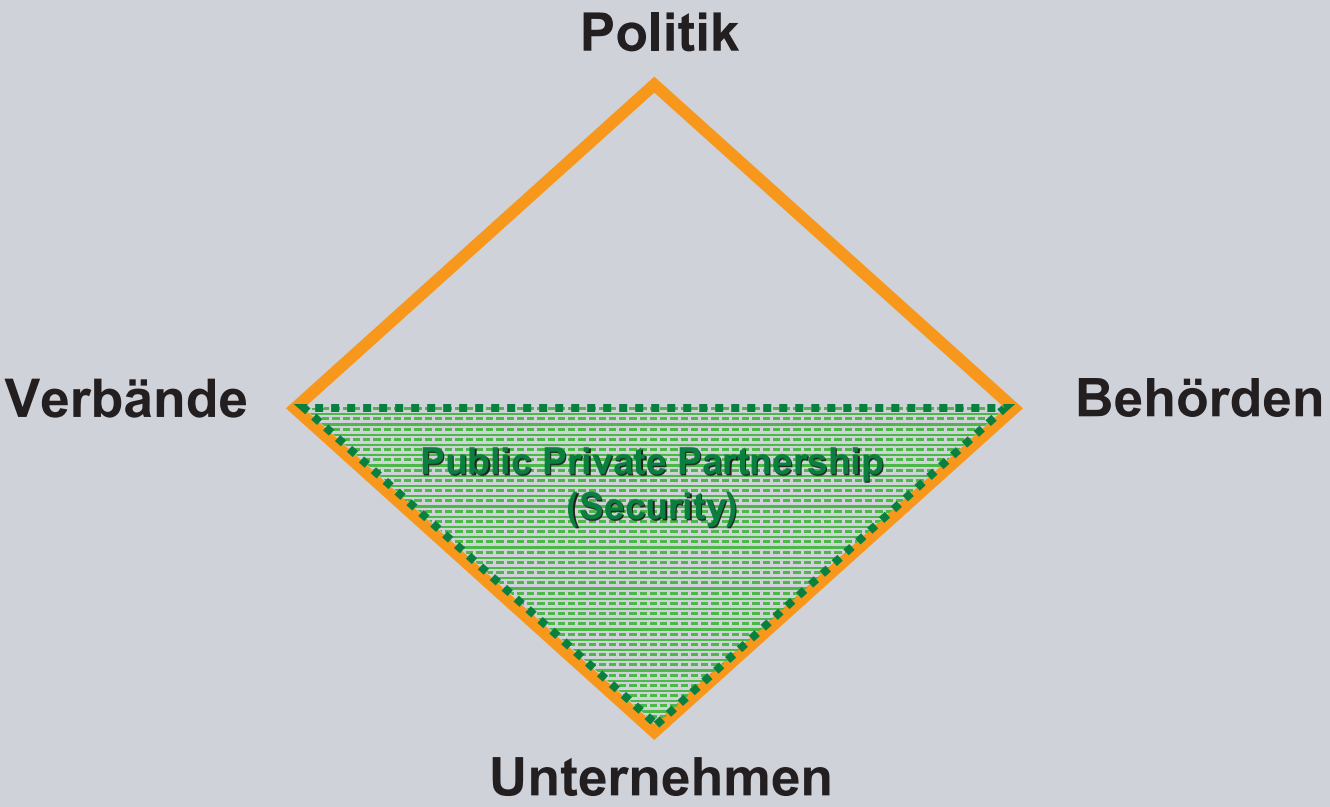
SIEMENS

- Ausrichtung aller Aktivitäten am Geschäft (Business Alignment)
- „Sprache der CEOs“ sprechen, ihre Bedürfnisse verstehen
- individuelle Lösungen anbieten
- Sicherheit als Mehrwert für den CEO
  - besser, schneller und effizienter als der Wettbewerber
  - verbessertes Risikomanagement
  - Aufbau eines robusten Krisenmanagements im Einklang mit den Geschäftsinteressen
  - Unterstützung bei der Öffnung neuer Märkte („hostile Environments“)

… ein Paradigmenwechsel

Security Partnership
Wo stehen wir in Deutschland?

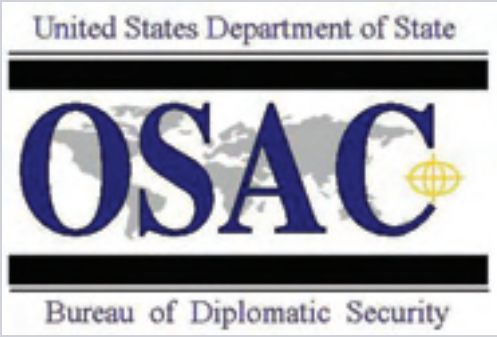
SIEMENS



- Wie leistungsfähig sind wir im Vergleich zu anderen Modellen im Ausland?
- Erfüllt die bestehende Public Private Partnership (PPP) meine Bedürfnisse und Erwartungen?

Security Partnership
Ein Blick über die Grenze

SIEMENS



Security Partnership in Deutschland
I have a dream …

SIEMENS

Verbände

- Schaffen eines Netzwerkes von Unternehmenssicherheiten
- Aktive Einbindung von relevanten Sicherheitsbehörden und Verwaltungen
- Stellvertreterfunktion/Interessen-vertretung gegenüber Politik und Behörden
- auf interne Zielgruppen orientiert
- transparente Diskussions- und Entscheidungsprozesse
- Blick über die Grenze - Europa?

Behörden / Verwaltungen

- klares politisches Bekenntnis zur Kooperation mit Privatsektor
- effiziente Zusammenarbeit und Unterstützung in Krisenfällen
- zeitnaher systematischer Informationsaustausch in Bezug auf weltweite Entwicklungen
- Ansprechpartner im Ausland
- effiziente Koordination aller relevanten Behörden und Ministerien untereinander
- Ausrichtung an der internationalen Konkurrenz

Security Partnership in Deutschland
Die Herausforderung

SIEMENS

Nachrichtendienstlich initiierte Elektronische Angriffe auf die deutsche Wirtschaft

Referent: Jadran Mesic, Bundesamt für Verfassungsschutz

Die Bundesrepublik Deutschland steht im Fokus fremder Nachrichtendienste. Dabei richtet sich das Informationsbedürfnis fremder Nachrichtendienste nicht nur gegen staatliche Stellen, sondern im Rahmen der von ihnen betriebenen Wirtschaftsspionage auch gegen deutsche Unternehmen. Dies ist insbesondere der Tatsache geschuldet, dass die Bundesrepublik Deutschland eine der führenden Industrienationen ist und hier eine Vielzahl von Unternehmen ansässig sind, die in ihrer Geschäftssparte eine führende Rolle auf dem Weltmarkt einnehmen.

Neben den klassischen nachrichtendienstlichen Methoden zur Informationserlangung sind in der Vergangenheit vermehrt Elektronische Angriffe als „neue“ Methode fremder Nachrichtendienste erkennbar. So wurden beispielsweise alleine im Jahr 2010 ca. 2100 Angriffe auf deutsche Behördenrechner erkannt, die einen nachrichtendienstlichen Hintergrund vermuten lassen. Aufgrund dieser massiven Angriffe muss davon ausgegangen werden, dass deutsche Unternehmen ebenfalls im erheblichen Maße auch elektronisch angegriffen werden.

Elektronische Angriffe bieten für einen fremden Nachrichtendienst vielfältige Vorteile. Sie sind vergleichsweise kostengünstig durchzuführen, da neben einem Schadprogramm lediglich ein handelsüblicher Rechner mit Internetzugang erforderlich ist. Auch sind die Angriffe sehr effektiv, einfach und weltweit platzierbar sowie in Real-Zeit durchführbar. Ist der Rechner einmal in der Hand der Angreifer, kann dieser Zugriff für diverse Zwecke benutzt werden. So mag zwar in der Regel das Informationsinteresse im Vordergrund stehen, der Übergang zur Sabotage (beispielsweise Löschung der Daten) besteht lediglich in wenigen Mausklicks.

Besonders hervorzuheben ist in diesem Zusammenhang auch, dass Elektronische Angriffe relativ risikolos sind. So ist beispielsweise für die nachrichtendienstliche Tätigkeit kein Grenzübertritt und Aufenthalt in einem fremden Staat erforderlich. Ein weiterer erheblicher Vorteil ist die Anonymität, die das Internet bietet. Die ausführende Person oder Stelle gerichtsfest zu ermitteln ist nahezu unmöglich.

Die Angriffsmethoden sind mannigfaltig. Eine weitverbreitete Methode ist die Versendung von E-Mails, die im Anhang versteckt ein Schadprogramm enthalten. Ist der Anhang einmal geöffnet, installiert sich das Schadprogramm und ermöglicht so dem Angreifer den Zugriff auf den Rechner. Dieser kann unbemerkt Daten kopieren und auf einen über die ganze Welt verstreuten Server laden. Denkbar sind jedoch auch Angriffe, die über Webseiten erfolgen, auf denen ein Schadprogramm installiert ist, welches sich durch das alleinige Aufrufen dieser Webseite auf dem Opferrechner installiert.

Regelmäßig werden auch Angriffe festgestellt, bei denen das Schadprogramm durch Datenträger übertragen wird. Als Beispiel sei hier der bekannte Stuxnet-Vorfall genannt, bei dem die Infektion durch einen USB-Stick erfolgte.

Nachrichtendienstlich initiierte Elektronische Angriffe stellen eine besondere Bedrohung für Wirtschaftunternehmen dar. Dies ist der Tatsache geschuldet, dass diese Angriffe überaus zielgerichtet und signaturarm erfolgen. Das bedeutet, dass es sich nicht um Massenangriffe handelt und somit eine Detektion durch kommerzielle Antivirenprogramme stark eingeschränkt ist.

Bezogen auf die Rechner von Bundesbehörden bestehen im BfV weitreichende Erkenntnisse zu Elektronischen Angriffen. Sofern deutsche Unternehmen durch Elektronische Angriffe betroffen sind, stehen wir diesen Unternehmen mit unserer Expertise gerne zur Verfügung. Dabei geht es nicht darum, organisatorisch-technische IT-Lösungen zu präsentieren, sondern vielmehr darum, das Wissen über nachrichtendienstlich initiierte Angriffe gegen deutsche Wirtschaftsunternehmen zu bündeln, auszuwerten und in geeigneter Form an diese zurückzugeben. Zum Beispiel könnten die Wirtschaftunternehmen auf diese Weise mehr über den Umfang der Bedrohung (bezogen auf ihre Geschäftssparte) und die für Angriffe genutzten Infrastrukturen erkennen.

Das Feedback, welches an die Wirtschaftsunternehmen zurückfließt, ist jedoch davon abhängig, in welchem Maße IT-Vorfälle bzw. Elektronische Angriffe dem BfV gemeldet und so einer Analyse und Bündelung zugänglich gemacht werden.

Dabei sind absolute Vertraulichkeit und Anonymität in jedem Falle selbstverständlich.

Kontaktdaten: Bundesamt für Verfassungsschutz, Merianstraße 100, 50765 Köln, Mail: sensea@bfv.bund.de.

Sicherheit beginnt in Ihrem Kopf

Security Awareness Maßnahmen am Beispiel der SAP

Michael Hartmann, Chief Security Officer SAP AG
Juni 2011

Agenda

- Wie ist Sicherheit bei SAP organisiert?
- Der Mensch als wichtigstes Glied in der Sicherheitskette
- Sensibilisieren – aber wie?

© 2011 SAP AG. All rights reserved.

Wie ist Sicherheit bei SAP organisiert?

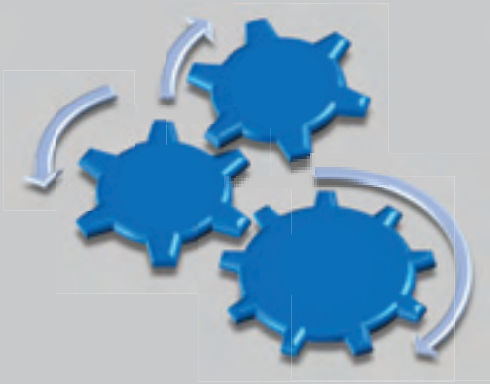
Sicherheit ist Teil der globalen GRC Organization

Compliance Management

Compliance with internal and external regulations, and adherence to the business code of conduct

Global Internal Audit Services

Enforce compliance with all policies and guidelines including compliance with statutory and legal requirements



Insurance Strategy

Establishment of a risk adjusted, effective global insurance program

Internal Controls

Securing an effective, annual internal control system for the SAP group

Security

Safeguarding of SAP's most important assets through a global security management program

Risk Management

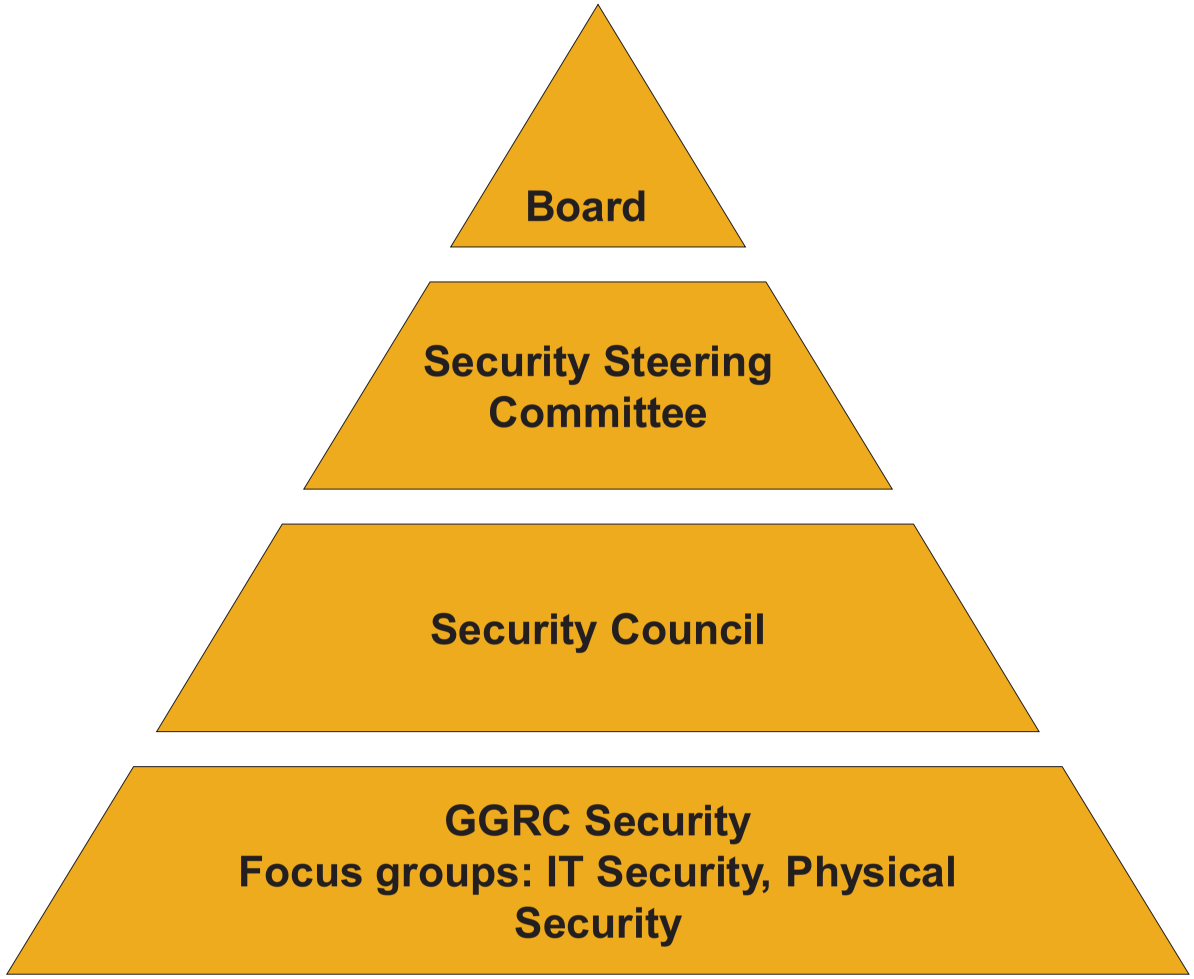
Establishment of a state of the art, company-wide Risk Management based on a global policy and model

© 2011 SAP AG. All rights reserved.

Organisationsübergreifende Zusammenarbeit

© 2011 SAP AG. All rights reserved.

Governance Panels

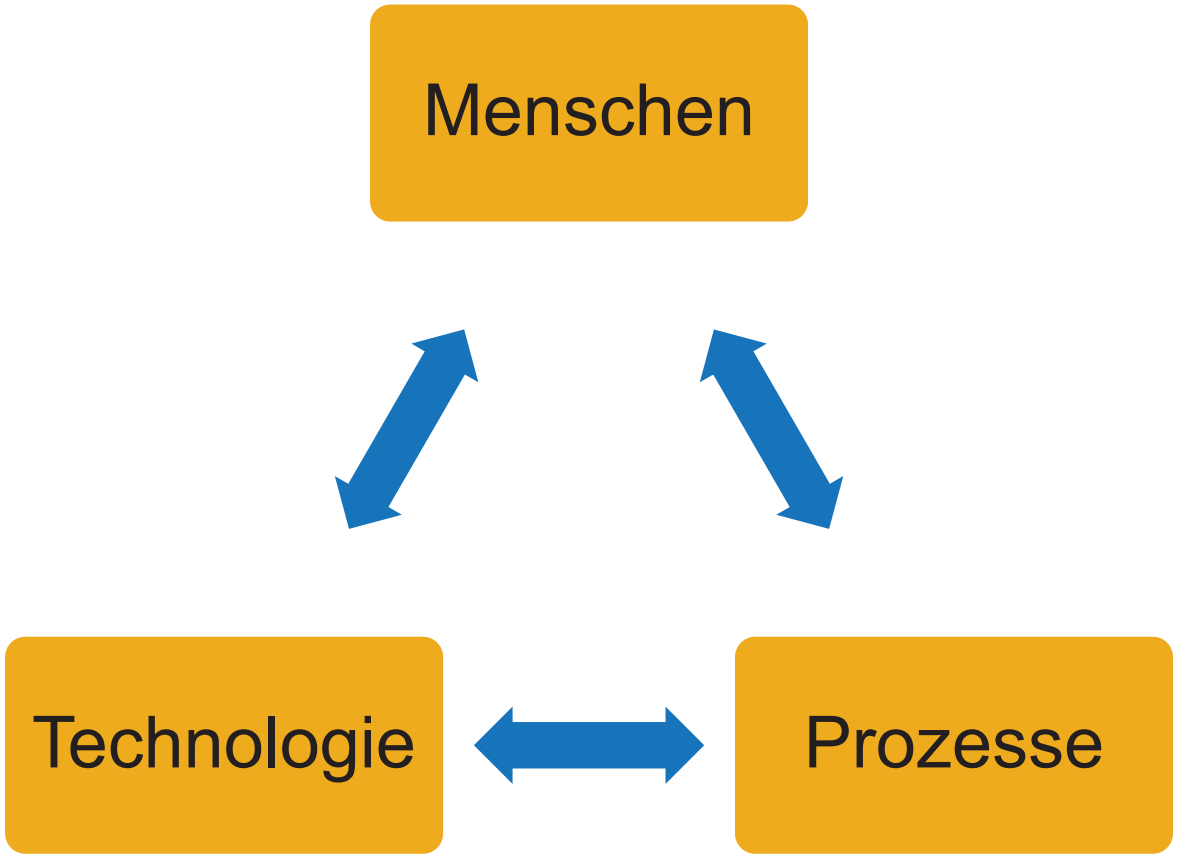


© 2011 SAP AG. All rights reserved.

Security Policy Framework

© 2011 SAP AG. All rights reserved.

Security beinhaltet...



© 2011 SAP AG. All rights reserved.

Der Mensch als wichtigstes Glied in der Sicherheitskette

Zynismuswarnung

"Zwei Dinge sind unendlich, das Universum
und die menschliche Dummheit, aber bei
dem Universum bin ich mir noch nicht ganz sicher"

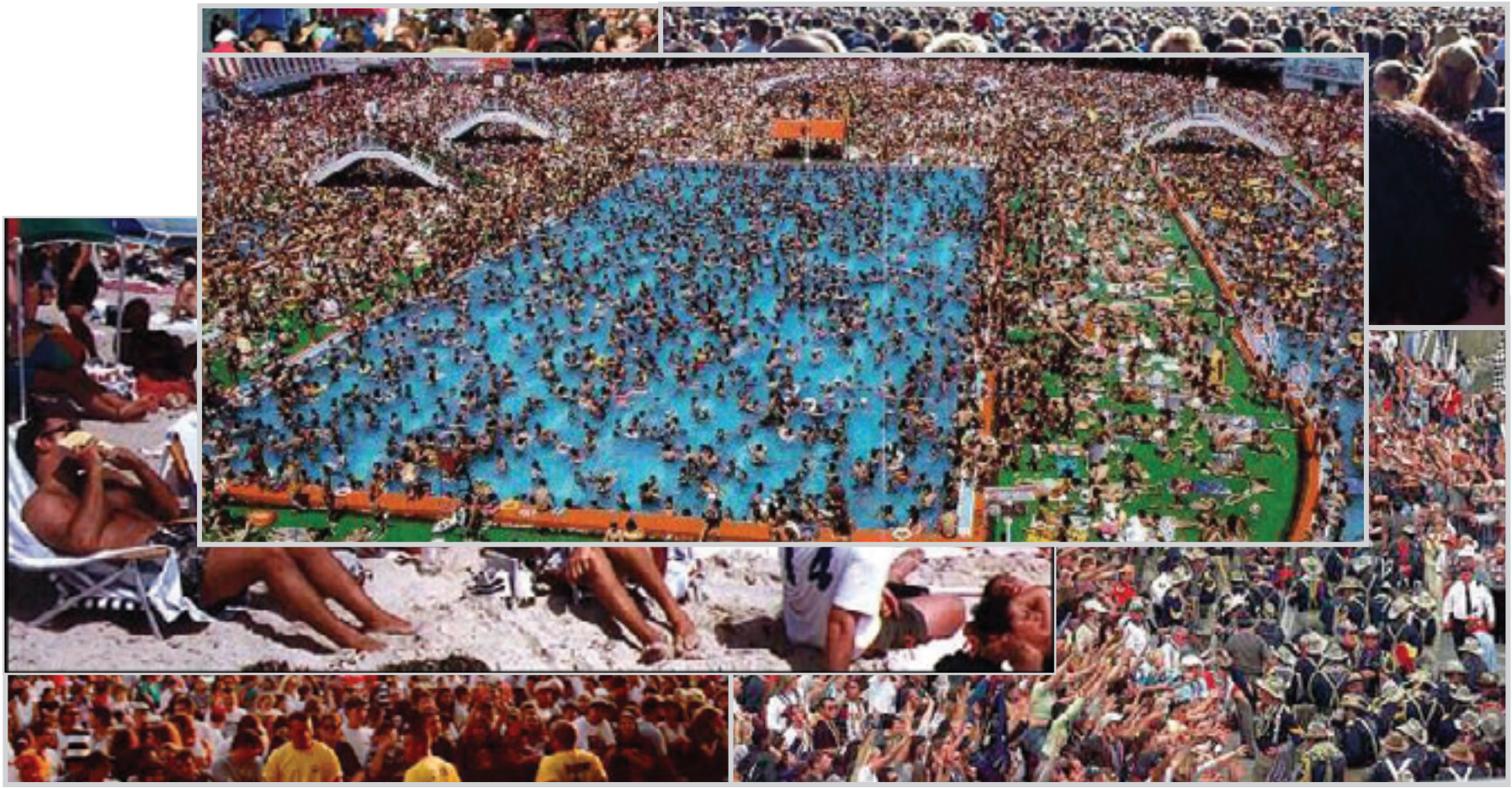
Albert Einstein

"There is no patch for human stupidity"

Spruch auf einer Website für Datenbank-Administratoren

© 2011 SAP AG. All rights reserved.

Die mißachtete Gefahr



© 2011 SAP AG. All rights reserved.

Der Mensch – wichtigstes Glied in der Security-Kette

Der Mensch ist und bleibt das stärkste und gleichzeitig schwächste Glied in der Security-Kette.

- Irrtum und Nachlässigkeit der Mitarbeiter ist Gefahr Nummer 1
- 65% der Angriffe kommen von innen
- Sicherheitsregeln müssen von Menschen umgesetzt werden
- Alle Technik nutzt nichts, wenn Menschen sie nicht einsetzen

© 2011 SAP AG. All rights reserved.

Der Mensch – wichtigstes Glied in der Security-Kette

Faktor Mensch

	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	progn. Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,52	2	1,17	1	49%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,06	1	1,51	4	35%
Software-Mängel-/Defekte	3	0,60	5	0,58	2	46%
Hardware-Mängel-/Defekte	4	0,55	6	0,34	3	45%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5	0,50	3	0,63	7	12%
unbeabsichtigte Fehler von Externen	6	0,39	7	0,32	5	30%
Hacking (Vandalismus, Probing, Missbrauch,...)	7	0,37	4	0,59	8	12%
Mängel der Dokumentation	8	0,27	9	0,27	6	20%
Manipulation zum Zweck der Bereicherung	9	0,26	8	0,29	10	11%
höhere Gewalt (Feuer, Wasser,...)	10	0,21	11	0,03	9	12%
Sabotage (inkl. DoS)	11	0,17	10	0,22	11	10%
Sonstiges	12	0,02	12	0,00	12	3%

Basis: 155 Antworten (Bedeutung), Ø 130 (Prognose), Ø 127 (Schäden)

Quelle: KES Sicherheitsstudie2006

© 2011 SAP AG. All rights reserved.

Hindernisse bei der Verbesserung von Informationssicherheit

Faktor Mensch

Bei der Verbesserung der ISi behindern am meisten:	
Es fehlt an Geld	55%
Es fehlt an Bewusstsein bei den Mitarbeitern	52%
Es fehlt an Bewusstsein und Unterstützung im Top-Managment	45%
Es fehlt an Bewusstsein beim mittleren Management	37%
Es fehlen verfügbare und kompetente Mitarbeiter	32%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31%
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	29%
Die Kontrolle auf Einhaltung ist unzureichend	27%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	25%
Die vorhandenen Konzepte werden nicht umgesetzt	22%
Es fehlen realisierbare (Teil-)Konzepte	19%
Es fehlen geeignete Methoden und Werkzeuge	16%
Es fehlen geeignete Produkte	13%
Es fehlt an praxisorientierten Sicherheitsberatern	8%
Sonstiges	5%
keine Hindernisse	3%

Quelle: KES Sicherheitsstudie2006

© 2011 SAP AG. All rights reserved.

Sensibilisierung der Mitarbeiter als Schlüsselaufgabe

Die Sensibilisierung der Mitarbeiter für das Thema Sicherheit ist eine der wichtigsten Aufgaben, um die Sicherheit im Unternehmen zu erhöhen!

© 2011 SAP AG. All rights reserved.

Eine schwere Aufgabe, die Mitarbeiter in Bezug auf Sicherheit auf eine Linie zu bringen …

Gesagt ist nicht gehört.

Gehört ist nicht verstanden.

Verstanden ist nicht einverstanden.

Einverstanden ist nicht behalten.

Behalten ist nicht angewandt.

Angewandt ist nicht beibehalten.

Zitat: Konrad Lorenz

© 2011 SAP AG. All rights reserved.

Ziele der Sensibilisierung

Motivieren

- Mitarbeitern eine positive Einstellung zum Thema Sicherheit vermitteln

Informieren

- Mitarbeitern generelle Informationen über Gefahren, Informationssicherheit und Richtlinien geben
- Die Ziele und Maßnahmen der Sicherheitspolitik im Unternehmen vermitteln
- Die Ansprechpartner zum Thema Sicherheit bekannt machen

Sensibilisieren

- Verständnis für Sicherheitsmaßnahmen erzeugen
- Anregen, aktiv an der Umsetzung der Maßnahmen mitzuwirken

© 2011 SAP AG. All rights reserved.

Herausforderungen bei der Sensibilisierung…

Informationsflut

Bildung im 20. Jarhundert erfordert vor allem und zunächst die instinktsichere Abwehr überzähliger Informationen.

Hans Kasper

Management

Erfahrung ist eine nützliche Sache.
Leider macht man sie immer erst kurz nachdem man sie brauchte...

Engagement der Mitarbeiter und des Managements

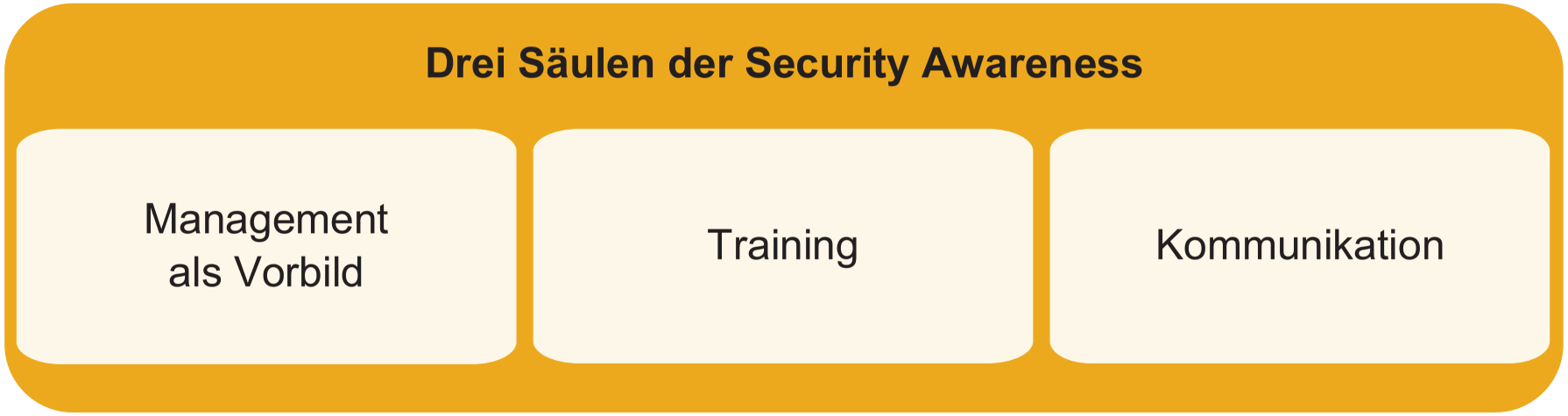
Niemand, der sich nicht selbst überzeugt, wird von Dir überzeugt werden.

Platon 427-347 v.Chr

© 2011 SAP AG. All rights reserved.

Sensibilisieren – aber wie?

Komponenten Security Awareness



© 2011 SAP AG. All rights reserved.

Beispiele zu Training und Kommunikation

Training

- (Virtual) Classroom Trainings
- Online Trainings
- Lernmaterialien
- Broschüren

Kommunikation

- Kampagnen
- Formelle E-Mails
- Newsletter, Artikel
- Videos

© 2011 SAP AG. All rights reserved.

Beispiele Trainingsmaterialien

Mitarbeiterbroschüre Security Policy

Wird mit dem Arbeitsvertrag ausgehändigt

Eigener Bereich im SAP Corporate Portal

© 2011 SAP AG. All rights reserved.

Beispiele (Virtual) Classroom Trainings

Onboarding

- Security ist integraler Bestandteil der Einführugsveranstaltung für neue Mitarbeiter

Executive Management

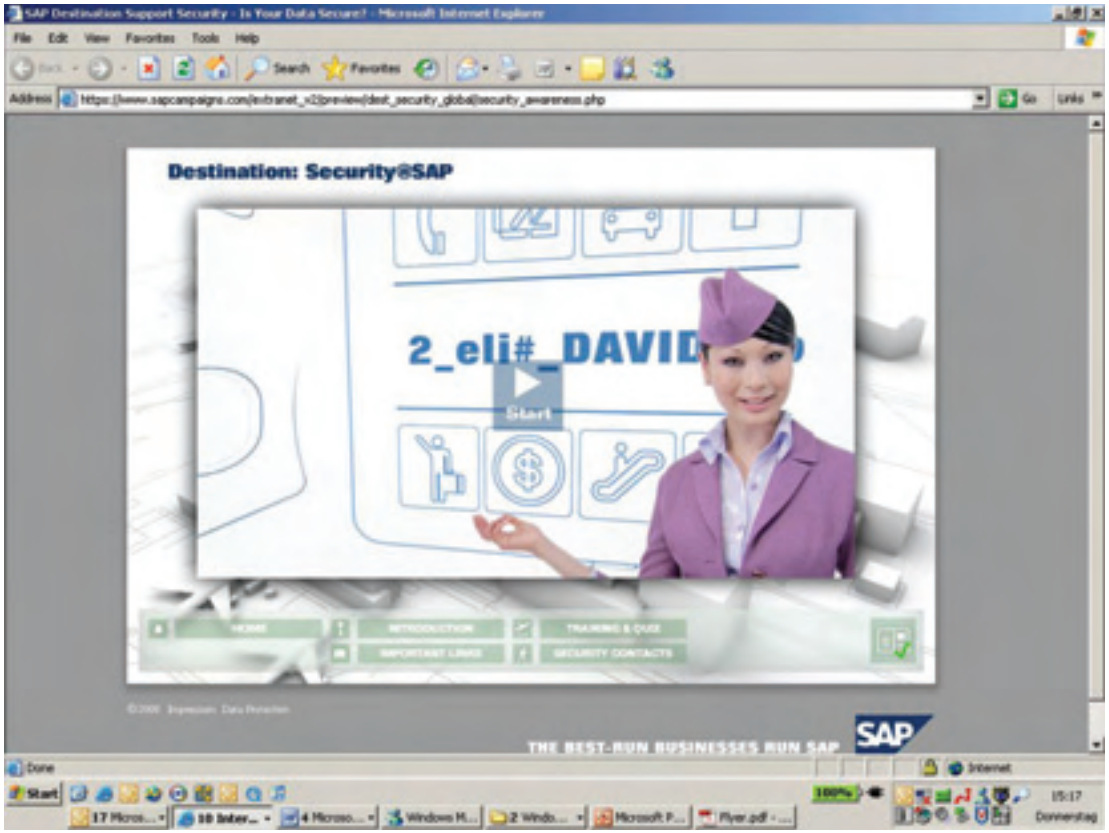
- Verpflichtendes Training für das Top Management mit internen & externen Referenten

Infosessions zu speziellen Themen

- Social Engineering
- Sicheres Entwickeln

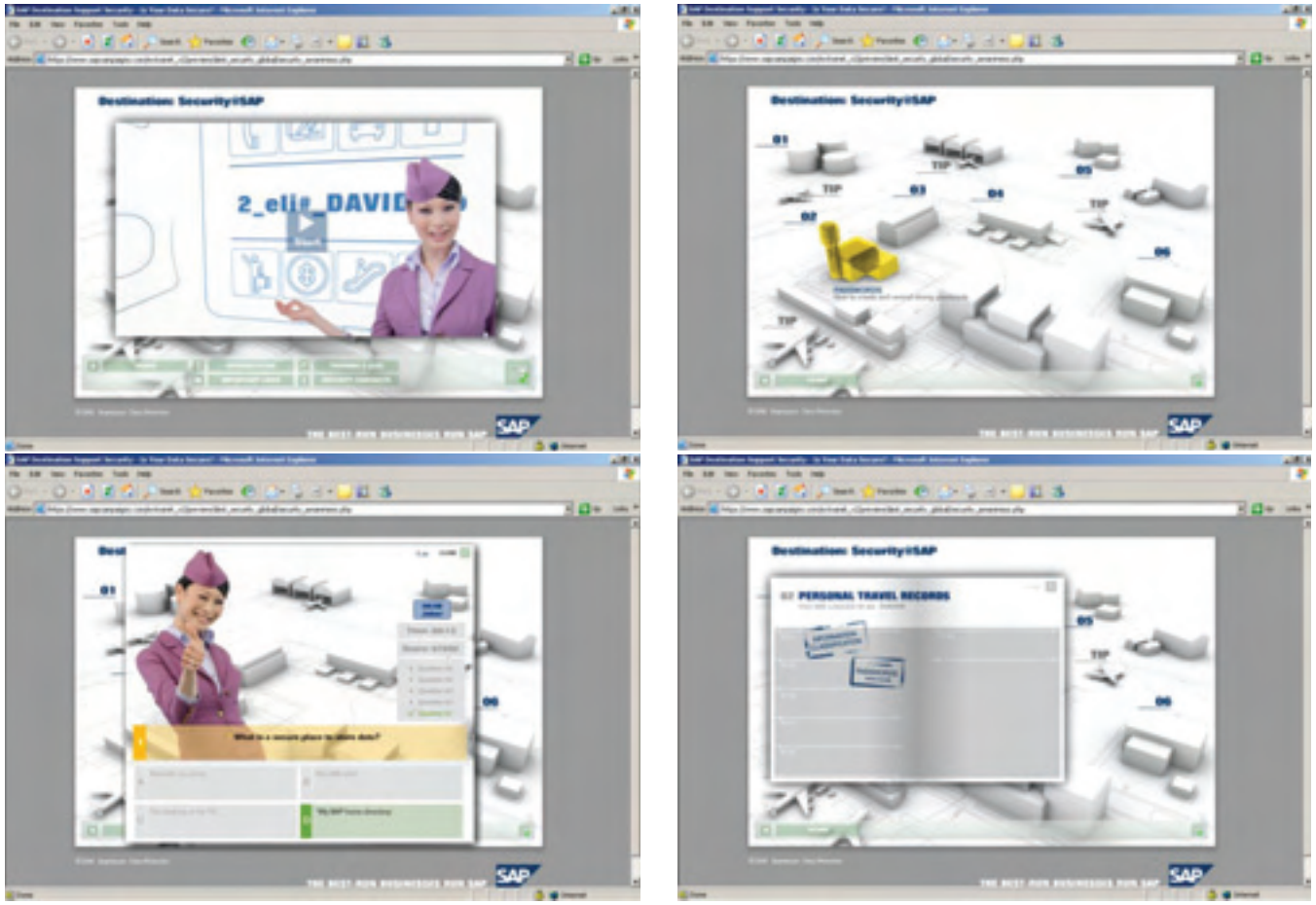
© 2011 SAP AG. All rights reserved.

SAP Awareness Kampagne „Destination Security“



© 2011 SAP AG. All rights reserved.

Kampagne – Webseite „Destination Security“



© 2011 SAP AG. All rights reserved.

Beispiele Security Kommunikation SAP

- Mail des Vorstandes
- Eigene Website im SAP Intranet
- Film SAP TV
- Artikel in SAPNews (Online)
- Interview mit CSO im SAPNet
- Infosession
- Newsletter an alle Mitarbeiter
- Posteraktion
- Spiegel-Display
- Spiegelaufkleber
- Reminder-Mails
- Broschüre für neue Mitarbeiter
- Follow-up-Aktionen – einzelne Standards als Schwerpunkt

© 2011 SAP AG. All rights reserved.

Spiegeldisplay

Der Mitarbeiter sieht sich selbst als wichtigstes Glied in der Security Kette

© 2011 SAP AG. All rights reserved.

Spiegelaktion

Spiegeldisplay leicht gemacht!

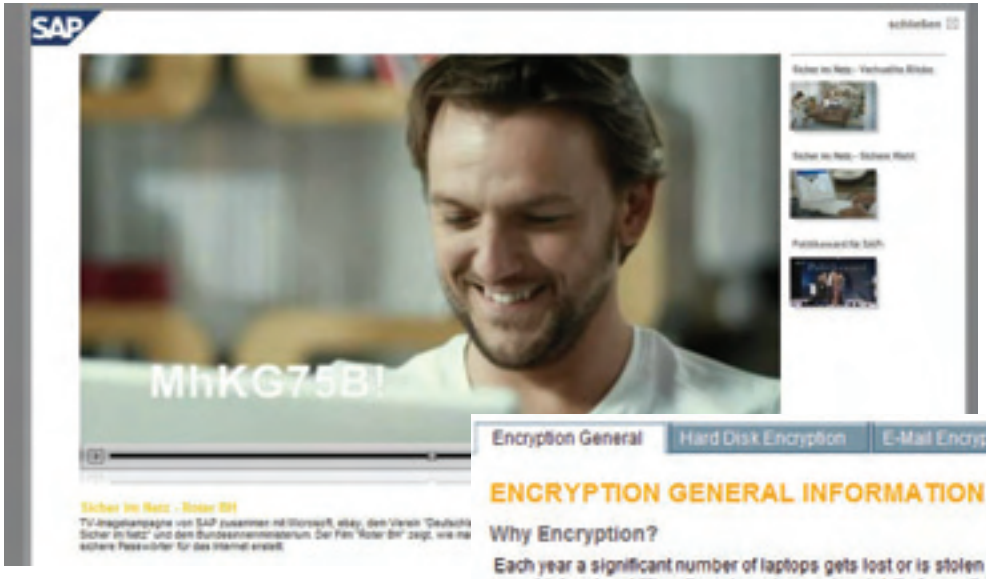
Weltweit auf alle Waschraumspiegel

100% Aufmerksamkeit!

© 2011 SAP AG. All rights reserved.

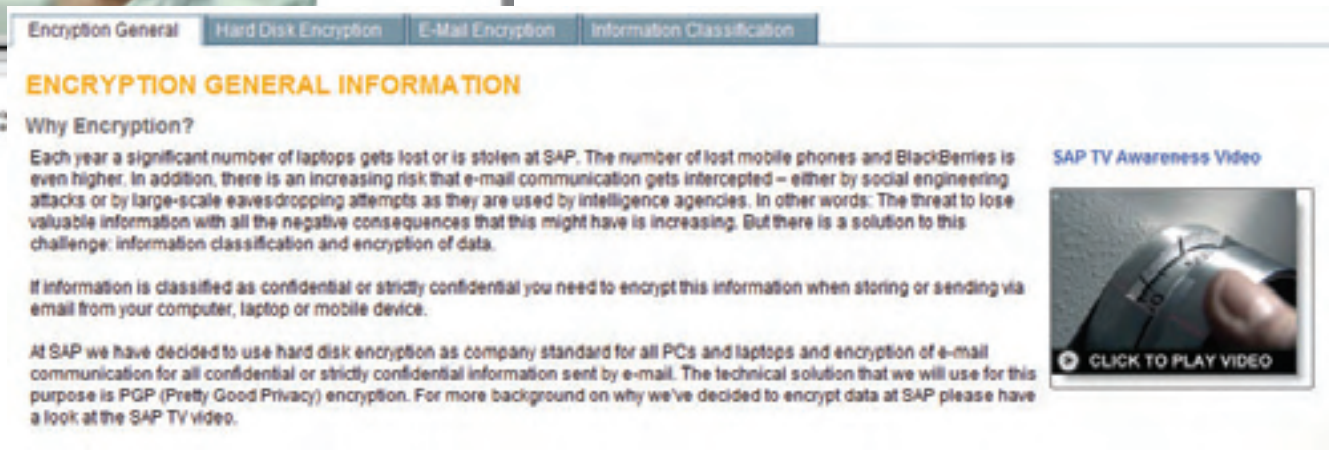
Beispiele: Security Awareness Videos

Passwortvideo (meistgesehenes SAP TV video)



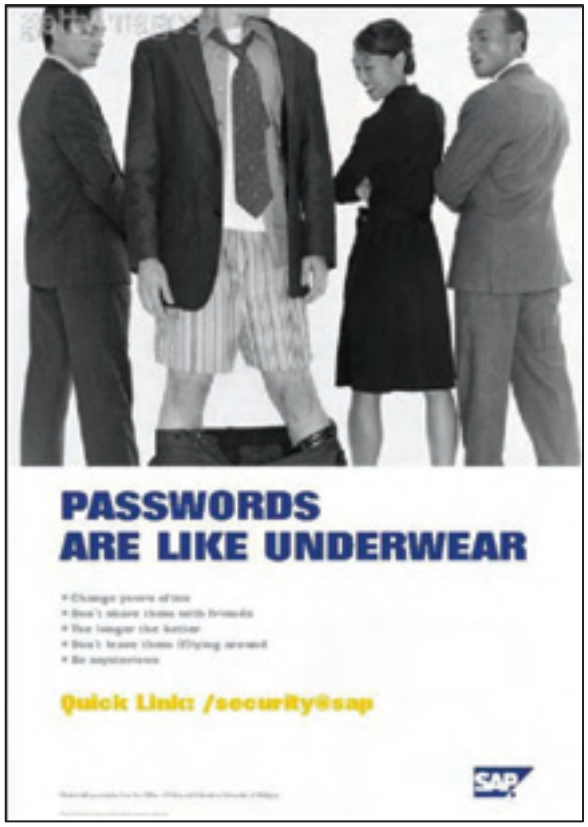
Encryption video

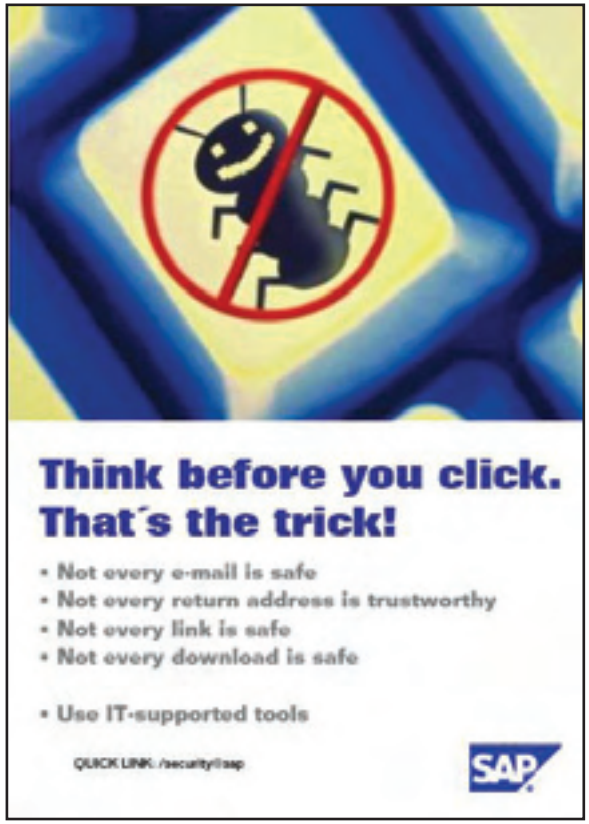
(wird in Kürze im Rahmen des PGP roll out veröffentlicht)



© 2011 SAP AG. All rights reserved.

Beispiele Posterkampagnen





© 2011 SAP AG. All rights reserved.

Einbeziehung unabhängiger externer Quellen und Referenten

Wie können wir die Bedrohung der Informationssicherheit glaubwürdig darstellen?

Medien

- Pressemeldungen
- Internet

Austausch und gemeinsame Aktivitäten mit öffentlichen Stellen

- BfV, LfV
- BSI
- BKA
- ASW Baden Würtemberg
- Lokale Polizeibehörden

© 2011 SAP AG. All rights reserved.

Fazit

Security Awareness Erfolgsfaktoren

- Kurzweilig, Spaß machen, interessant sein
- Einfache, kurze und prägnante Botschaften
- Konkrete Beispiele mit Praxisbezug
  - Kontext
  - Wiedererkennung
- Kontinuität
- Glaubwürdigkeit

© 2011 SAP AG. All rights reserved.

Vielen Dank!

Kontakt Information:

Michael Hartmann
Chief Security Officer
SAP AG
michael.hartmann@sap.com

5. ASW/BfV-Informationsveranstaltung
30. Juni 2011 in Köln

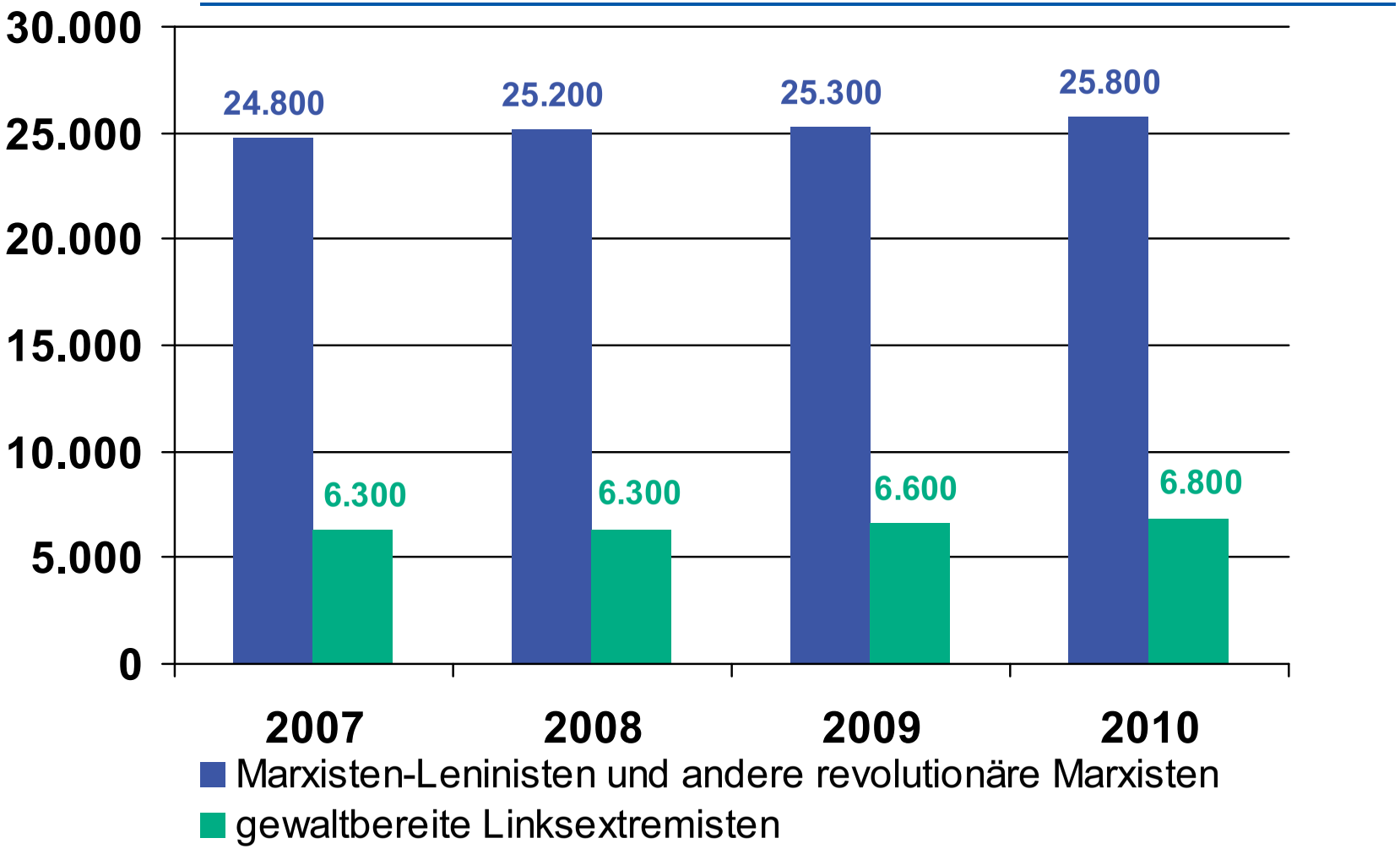
„Gewaltorientierter Linksextremismus in Deutschland
- eine Gefahr für die Wirtschaft?“

Lagedarstellung

- Seit den Protesten gegen den NATO-Gipfel 2009 in Straßburg gesteigerte Militanzbereitschaft feststellbar
  - erhöhte Aggressivität bei Protesten/Demonstrationen
  - anhaltend hohes Aggressionsniveau gegenüber Rechtsextemisten
  - hohe Gewaltbereitschaft gegen „Vertreter des Repressions-apparates“
  - erhebliche Steigerung der Straf- und Gewalttaten in 2009
  - leichter Anstieg des gewalttätigen Personenpotenzials
- Schwerpunktthemen linksextremistischer Agitation und Aktion
  - Antifaschismus
  - Antimilitarismus
  - Antirepression
  - Freiräume/Gentrifizierung

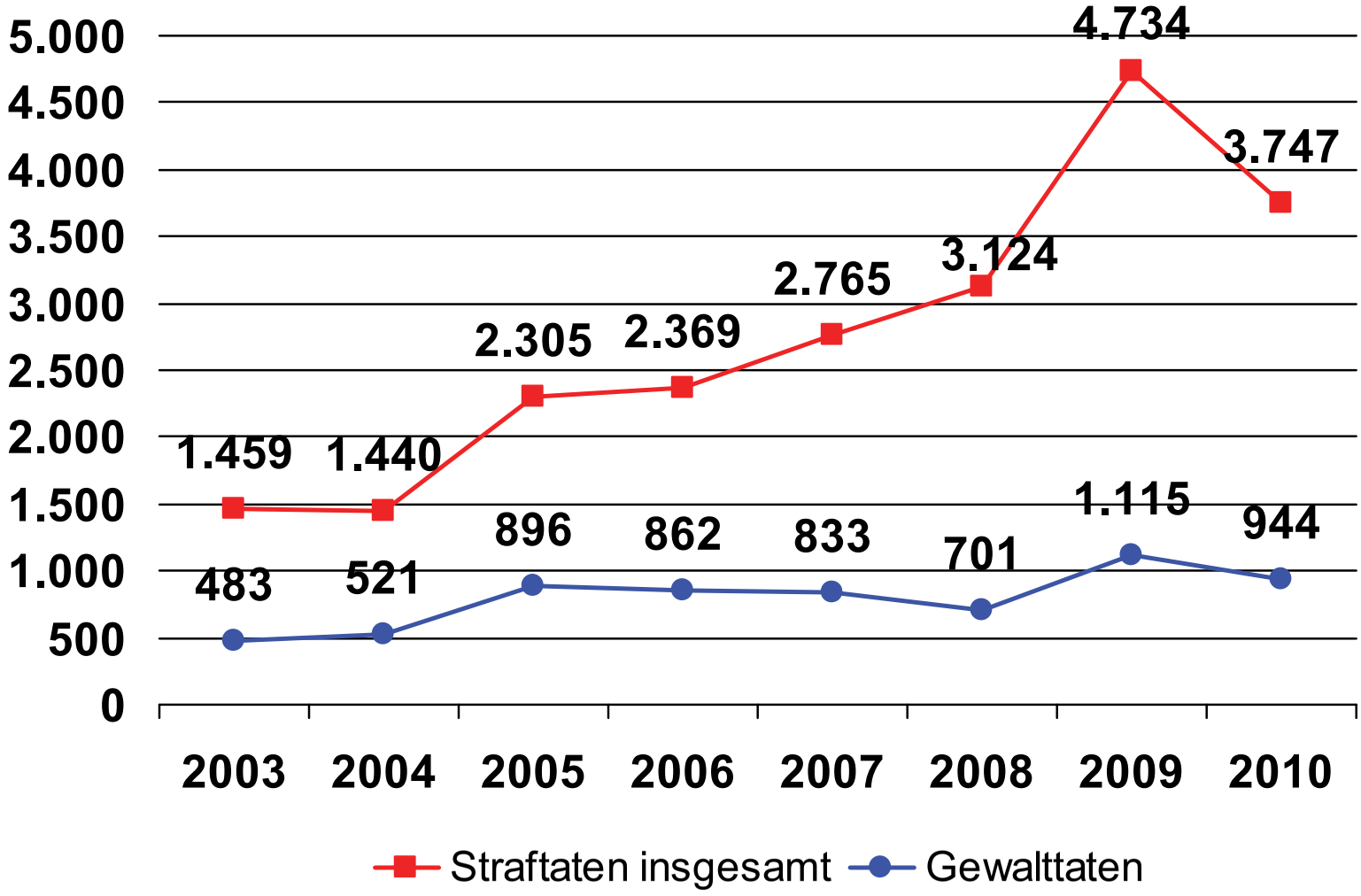
Bundesamt für Verfassungsschutz

Linksextremismuspotenzial



Bundesamt für Verfassungsschutz

Linksextremistische Straf- und Gewalttaten seit 2003



Bundesamt für Verfassungsschutz

Wirtschaftsunternehmen im Visier

- Wirtschaftsunternehmen (WU) sind Teil des kapitalistischen Systems
- Mitverantwortung für angebliche soziale und politische Missstände
- Vorwurf: zur Gewinnmaximierung und zur Sicherung ihres politischen und wirtschaftlichen Einflusses beuten WU Mensch und Natur aus

Bundesamt für Verfassungsschutz

Gefährdete Wirtschaftsbereiche

- Unterstützer des **„Faschismus“**
- „Profiteure“ der **Asylpolitik**
- „Profiteure“ des **Sozialabbaus**
- „Profiteure“ der **Globalisierung**
- Im **„Atomgeschäft“** tätige Unternehmen
- An Projekten zur **„Umstrukturierung“** beteiligte Unternehmen
- Im Bereich der **Bio- und Gentechnologie** tätige Unternehmen und Einrichtungen
- **Rüstungsbetriebe** und deren Zulieferer

Militante Kampagne gegen Deutsche Post DHL

- Initiiert von militanten Linksextremisten auf den „Antimilitaristischen Aktionstagen“ Ende Oktober 2008 in Berlin
- DHL als Logistikdienstleister für Bundeswehr und US-Militär
- bislang 23 Brandanschläge auf Fahrzeuge, Hunderte weitere Sachbesch.

Militante Kampagne gegen Deutsche Post DHL

- Kampagnenvorschlag: „DHL - Olivgrün unter postgelbem Tarnanstrich“

Neben politischer Arbeit für Kriegsdienstverweigerung mit Wehrpflichtigen und Soldaten, oder konkreten Initiativen gegen Militärgerät und Rüstungsbetriebe wurde auch die Idee stark gemacht, am Beispiel des zivil-militärischen Unternehmens DHL die Kritik an der NATO und an der neuen NATO-Doktrin (mit ihrem Kernstück "comprehensive approach" = "umfassender Ansatz") praktisch werden zu lassen. Die Deutsche Post-Tochter DHL entpuppt sich nämlich als "Deutsche Heeres Logistik" und bietet sich deswegen für eine aktionsbezogene Mobilisierung im Vorfeld der NATO-Feierlichkeiten an.

Diese Idee reiht sich ein neben Vorschläge, Aktionstage gegen Rüstungsbetriebe und die Commerzbank durchzuführen (weil diese Bank im Bereich der Wirtschaft mit an vorderster Front im Bereich der Akzeptanzbeschaffung für die Bundeswehr steht). Ebenso wie die Commerzbank gibt es DHL, Postämter und Postbriefkästen in fast jeder Stadt. Diese Orte bieten sich somit für lokale Aktivitäten zur NO-NATO-Mobilisierung und darüber hinaus an. So ergeben sich vielfältige Möglichkeiten, die militärische Unterstützungsarbeit von vornehmlich zivilen Dienstleistern mit hohem Verbreitungsgrad und der hohen Abhängigkeit von ihrer Reputation beim Endkunden öffentlichkeitswirksam anzugehen.

Die fortschreitende Militarisierung im Zivilen anzugreifen scheint ein lohnenswerter „comprehensive approach" für eine antimilitaristische Gegenstrategie.

Bundesamt für Verfassungsschutz

Militante Kampagne gegen Deutsche Post DHL

Bundesamt für Verfassungsschutz

Militante Kampagne gegen Deutsche Post DHL


Drensteinfurt, 18. April 2010


Drensteinfurt, 18. April 2010


Berlin, 27. Oktober 2009

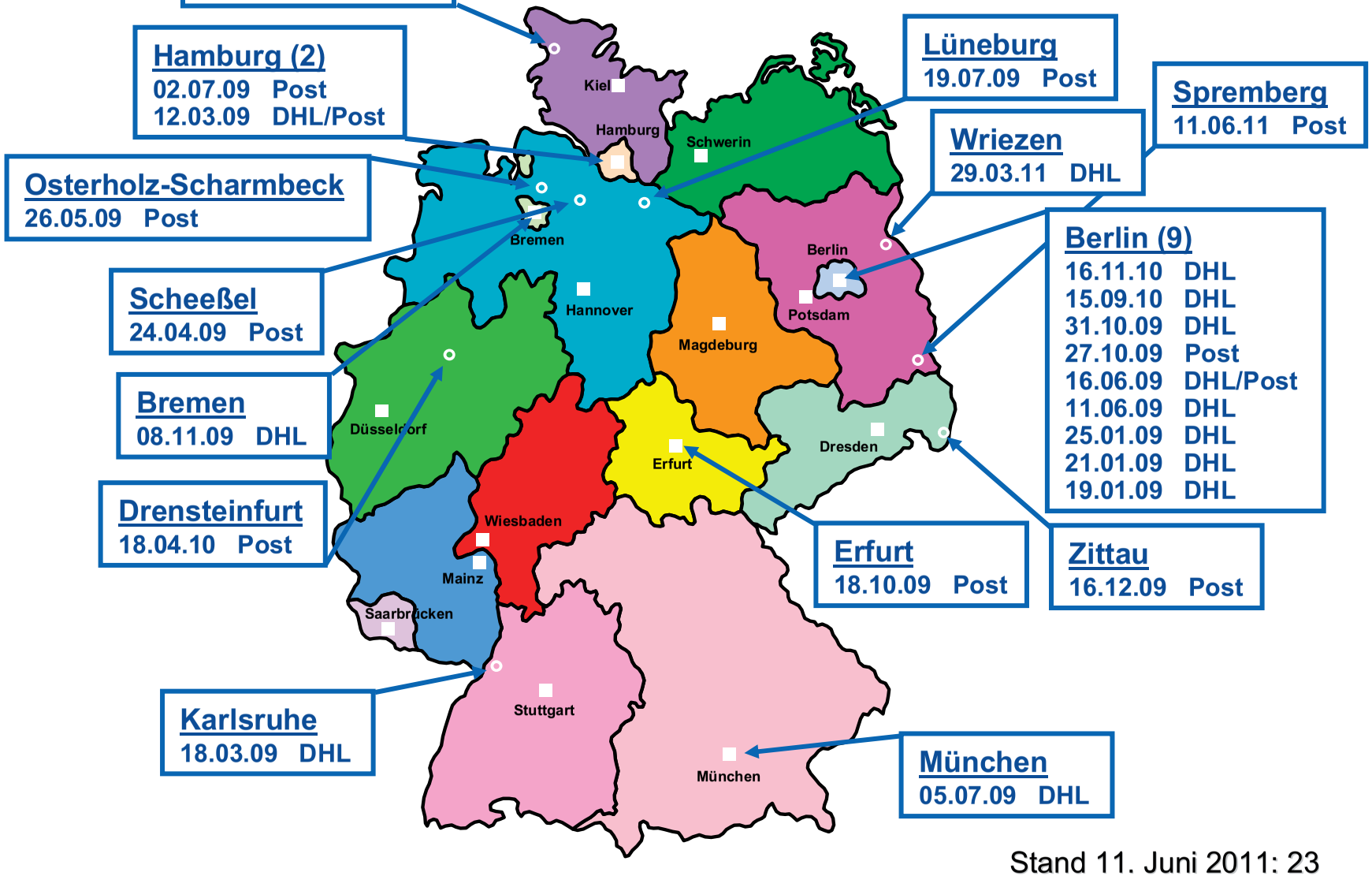
Berlin, 15. September 2010

Militante Kampagne gegen Deutsche Post DHL

Militante Kampagne gegen Deutsche Post DHL

Bundesamt für Verfassungsschutz

Brandanschläge auf DHL-/Post-Kfz seit 2009



Bredstedt
11.01.09 Post

Hamburg (2)
02.07.09 Post
12.03.09 DHL/Post

Osterholz-Scharmbeck
26.05.09 Post

Scheeßel
24.04.09 Post

Bremen
08.11.09 DHL

Drensteinfurt
18.04.10 Post

Karlsruhe
18.03.09 DHL

Lüneburg
19.07.09 Post

Wriezen
29.03.11 DHL

Spremberg
11.06.11 Post

Berlin (9)
16.11.10 DHL
15.09.10 DHL
31.10.09 DHL
27.10.09 Post
16.06.09 DHL/Post
11.06.09 DHL
25.01.09 DHL
21.01.09 DHL
19.01.09 DHL

Erfurt
18.10.09 Post

Zittau
16.12.09 Post

München
05.07.09 DHL

Stand 11. Juni 2011: 23

Bundesamt für Verfassungsschutz

Militante Kernkraftgegner

- Aktionsfeld gewinnt seit den szeneintern als erfolgreich bewerteten Protesten gegen den Castortransport 2010 an Bedeutung
- Seit Fukushima/Japan: Linksextremisten nutzen hohe Präsenz und Aktualität des Themas
  ➔ Anstieg von Straftaten gegen Bahn und Energieversorger
- Ende April: Aufruf zu „offensiven Aktionen“ gegen die vier großen Energieerzeuger RWE, E.ON, EnBW und Vattenfall sowie die „mit ihnen verflochtene Atomindustrie“:

  „In jeder Region befinden sich Kundenbüros der Großkonzerne, stehen die Banken, die sie mit den nötigen Krediten versorgen, fahren Züge der deutschen Bahn als Großkunde und Müll-Logistiker der AKW-Betreiber. Alltäglich und überall sind Aktionen möglich, die Atomenergieversorger und Atomindustrie gerade jetzt empfindlich treffen – seid kreativ!“
  (Aufruf „Atomindustrie stilllegen! Energieriesen zu Fall bringen!“ von „anti-atomare Stolpersteine“)

Militante Kernkraftgegner

Militante Aktionen gegen Deutsche Bahn und Energieversorger

- **Hamburg, 14. Juni:** Brandstiftung an mehreren Firmen-Kfz der E.ON Hanse
- **Berlin, 6. Juni:** Brandanschlag auf ein Firmenfahrzeug von Vattenfall
- **Hamburg, 25. Mai:** Sachbeschädigung an einem Bürogebäude der E.ON Hanse
- **Berlin, 23. Mai:** Brandanschlag auf eine provisorische Kabelbrücke am Bahnhof Ostkreuz
- **Berlin, 18./19. Mai:** Brandanschläge auf Firmenfahrzeuge von Deutscher Bahn, Vattenfall und Siemens
- **Berlin, 14. Mai:** Brandanschlag auf ein Kraftwerksgebäude sowie Sachbeschädigungen an einem Bürogebäude von Vattenfall
- **Hamburg, 17. März, 25. und 29. April:** Brandanschläge auf Firmenfahrzeuge von Vattenfall
- **Wuppertal, 6. April:** Sachbeschädigungen an Firmen-Kfz von RWE

Militante Kernkraftgegner

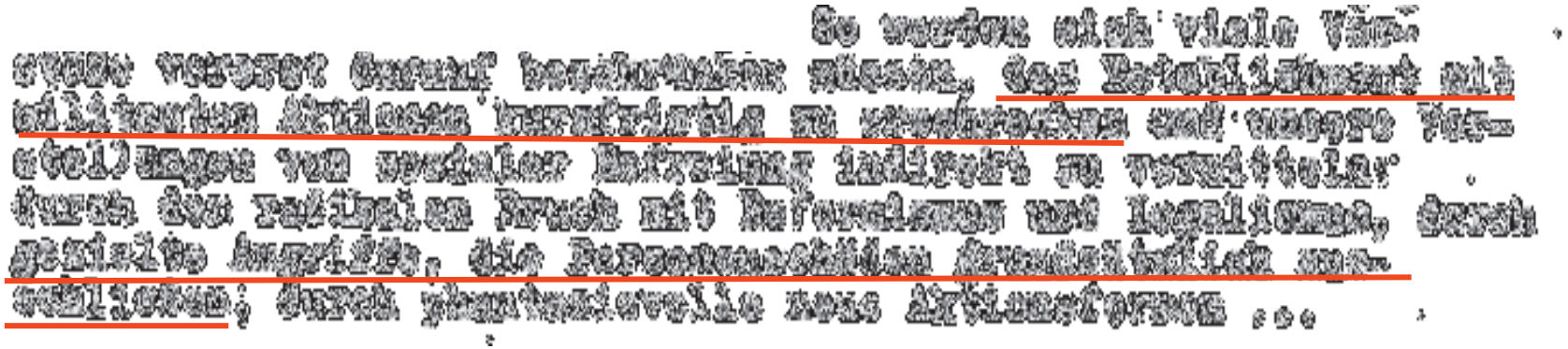
Bewertung und Ausblick (1)

- Wirtschaftsunternehmen weiterhin im Zielspektrum gewaltbereiter Linksextremisten
- Zieleingrenzung kaum möglich; akt. Bsp. Citroen Berlin

> Am 13. Juni haben wir also in Berlin-Lichtenberg einen Citroën Händler mit Brandsätzen angegriffen. Dabei wurden zehn Autos zerstört. Wir haben uns für Citroen entschieden, weil dieser französische Konzern Fahrzeuge an die griechische Polizei liefert. Griechische Bullen machen mit Streifenwagen von Citroën Jagd auf Migranten und nutzen die Technik dieser Firma zur Unterdrückung sozialer Spannungen. Mit unserem Angriff auf einen Berliner Citroën Händler zeigen wir den Profiteuren des inneren Krieges, dass es keine klare Front gibt. Was in Athen Bullen zu ihren Einsätzen transportiert kann in Berlin schon mal brennen.

Bewertung und Ausblick (2)

- Klandestin operierende Kleingruppen mit sachschaden-orientierter Zielrichtung



- Keine Anzeichen für den Übergang zu personenbezogenen Anschlägen oder Herausbildung terroristischer Strukturen

Ende des Vortrages

Vielen Dank für Ihre Aufmerksamkeit!

Wirtschaftsschutz
ist
Teamwork

BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Referat Wirtschaftsschutz
Merianstr. 100
50765 Köln
Telefon: 0221/792-0
Fax: 0221/792-2915
E-Mail: wirtschaftsschutz@bfv.bund.de