Bundesamt für
Verfassungsschutz

ASW
Zentralorganisation der Wirtschaft

Proaktiver Wirtschaftsschutz: Prävention durch Information

4. Sicherheitstagung des BfV und der ASW am 18. März 2010 in Köln

Tagungsband

„Proaktiver Wirtschaftsschutz: Prävention durch Information“

Tagungsband

der 4. gemeinsamen Sicherheitstagung des Bundesamtes für Verfassungsschutz (BfV)
und der
Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW)
am 18. März 2010 in Köln

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

4. Sicherheitstagung des BfV und der ASW am 18. März 2010 in Köln

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

Die 4. 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 innovativer mittelständischer Unternehmen und so genannter „Global Player“ sowie von Wirtschaftsverbänden, Ministerien und Sicherheitsbehörden nahmen daran teil. Fachleute aus den Sicherheitsbehörden und der Wirtschaft referierten zu verschiedenen Aspekten der Wirtschaftsspionage und des Wirtschaftsschutzes.

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 zur 4. Sicherheitstagung, die auch in diesem Jahr, das ist jetzt schon Tradition, gemeinsam von der Arbeitsgemeinschaft für Sicherheit der Wirtschaft und dem Bundesamt für Verfassungsschutz durchgeführt wird.

Ich freue mich, dass zahlreiche Vertreter aus Wirtschaftsverbänden und Unternehmen hier sind, sowohl von mittelständischen Unternehmen als auch von sogenannten Global Playern. Sehr herzlich begrüße ich auch die Vertreter von Ministerien und Sicherheitsbehörden. Wir sind uns bewusst, dass nur gemeinsame Anstrengungen von Staat und Unternehmen die Wirtschaft vor illegaler Ausspähung schützen können und verstehen die heutige Tagung als einen wichtigen Beitrag hierzu. Der Verfassungsschutz möchte damit den hohen Stellenwert dokumentieren, den er der Prävention bei der Bekämpfung der Wirtschaftsspionage zumisst.

Eine Säule unseres Konzeptes zum Wirtschaftsschutz ist die Sicherheitspartnerschaft, die vertrauensvolle und erfolgreiche Kooperation mit der ASW, deren Vorsitzenden Herrn Dr. Thomas Menk ich sehr herzlich begrüßen darf. Herr Dr. Menk wird nachher in das Thema einführen. Ebenso herzlich begrüße ich Herrn Michael Sorge, den Leiter des Verbands für Sicherheit der Wirtschaft Nordrhein Westfalen. Als Leiter Konzernsicherheit der Bayer AG kann er uns, wie nur wenige andere, Möglichkeiten und Interdependenzen von Sicherheitsvorkehrungen bei einem Global-Player darlegen.

Ich freue mich ganz besonders, dass zahlreiche Vertreter aus der Wirtschaft zu uns gekommen sind. Es ist uns ein besonderes Anliegen, Sicherheitsfragen mit Vertretern der Wirtschaft zu erörtern. Konstruktive Kontakte sind eine unabdingbare Voraussetzung für eine erfolgreiche Gefahrenabwehr. Sie können versichert sein: Wir vom Bundesamt für Verfassungsschutz sind an einer Fortsetzung und Vertiefung des Dialogs sehr interessiert. Konstruktive Kontakte auf der Basis von Vertrauen und Verlässlichkeit sind unerlässlich für die Abwehr der Wirtschaftsspionage und den Schutz der deutschen Unternehmen und ihres Know-hows.

Das Problem Wirtschaftsspionage hat sich im letzten Jahrzehnt entscheidend verschärft. Und das nicht nur in Deutschland, sondern in allen freiheitlichen Demokratien. Insoweit ist die Bekämpfung des illegalen Wissentransfers eine transnationale Aufgabe – wie so vieles andere auch in der Sicherheitspolitik. Der intensive – auch internationale – Austausch von Informationen und Methodik ist eine unabdingbare Voraussetzung für eine erfolgreiche Gefahrenabwehr.
Deshalb freue ich mich ganz besonders, dass mit Herrn Hubert Bartl ein Vertreter unseres österreichischen Partnerdienstes, dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, hier sprechen wird. Es ist immer von Interesse, zu sehen, wie Kollegen in anderen Ländern mit der Thematik umgehen.

Sehr herzlich begrüße ich auch die weiteren Referenten aus Wissenschaft und Behörden.

Von der Beuth-Hochschule für Technik Berlin ist Herr Professor Dr.-Ing. Alexander Huber zu uns gekommen. Wenn ich seinen Forschungsschwerpunkt nenne, klingt das beinahe so, als sei dieser eigens für unsere heutige Veranstaltung ausgewählt worden, in Wirklichkeit aber ist er Ausdruck der Kompetenz, die Herr Professor Huber für das Thema mitbringt, das uns heute beschäftigen wird: die Abwehr von Wirtschaftsspionage und Informationsschutz für Unternehmen.

Wir alle wissen, dass die Sicherheit der elektronischen Kommunikation eine immer größere Rolle spielt, dass wir unsere Anstrengungen gerade in diesem Bereich noch weiter steigern müssen. Gefährdungen und entsprechende Schutzmaßnahmen sind das Thema von Herrn Joachim Opfer, dem Fachbereichsleiter Abhörsicherheit im Bundesamt für Sicherheit in der Informationstechnik.

Die Weltwirtschaft hat sich in den letzten Jahrzehnten rapide gewandelt. Angefangen vom Fall des Eisernen Vorhangs und einer scheinbar unaufhaltsamen ökonomischen Globalisierung scheint sich dieser Prozess im Gefolge der Finanzmarktkrise weiter zu beschleunigen. Neue Wirtschaftsmächte wachsen heran, andere müssen heftig ringen, um ihren Standard halten zu können. Herr H. Schmitt vom Bundesnachrichtendienst wird uns mit Indien einen der Aufsteiger vorstellen und das Land unter Sicherheitsaspekten beleuchten. Angesichts der weltweiten wirtschaftlichen Verflechtung erwachsen deutschen Firmen nicht nur Gefahren hier in Deutschland, sondern auch anderswo. Die Konsequenz kann auch hier nur lauten: Lassen Sie uns den Informationsaustausch intensivieren, überall dort, wo rechtliche Vorgaben und insbesondere datenschutzrechtliche Normen dem nicht entgegenstehen. Und das tun sie in den seltensten Fällen, wenn es um Fragen der Methodik und Analyse geht.

Meine Damen und Herren,
das Bundesamt für Verfassungsschutz feiert in diesem Jahr seinen 60. Geburtstag. Nicht nur Menschen müssen in diesem Alter – wollen sie auf der Höhe der Zeit sein und bleiben – ihre Fähigkeiten stetig erweitern und verbessern. Dies gilt ebenso für Unternehmen wie in gleichem Maße auch für Behörden.

Für den Verfassungsschutz war die Abwehr der Spionage fremder Nachrichtendienste immer ein Schwerpunkt seiner Aufgaben. Angriffsmittel und auch Angriffsspektren unterlagen einem ständigen Wandel. Ich nenne beispielhaft das, was wir als „elektronische Attacken“ bezeichnen, und den Bedeutungszuwachs der Wirtschaftsspionage.

Bei der Abwehr dieser Gefahren kommt uns das methodische Wissen über politische und militärische Spionage zugute. Gleichwohl muss es spezifiziert und angepasst werden.
Wie wir das tun, wird Ihnen der Leiter der Abteilung Spionageabwehr erläutern, Herr Dr. Burkhard Even. Er wird das im Jahr 2008 überarbeitete Wirtschaftsschutzkonzept des Verfassungsschutzes vorstellen und die seither gemachten Erfahrungen bilanzieren.

Meine Damen und Herren,
Deutschland steht im Bereich der Wirtschaftsspionage – wie übrigens auch bei der Konkurrenzausspähung – im besonderen Fokus der Angreifer.

Neben den Global-Playern sind hiervon auch die innovativen mittelständischen Unternehmen betroffen. Während jedoch international tätige Konzerne in der Regel über eine gut funktionierende Unternehmenssicherheit verfügen, bestehen bei mittelständischen Firmen häufig noch Defizite beim Informationsschutz.
Notwendig sind hier sowohl eine Intensivierung und Bündelung der vorhandenen Ressourcen als auch eine gemeinsame Strategie von Staat und Wirtschaft, um die Unternehmen wirksam zu schützen. Das BfV ist aufgrund seiner spezifischen Kenntnisse im Bereich der Spionageabwehr in der Lage, Verdachtssituationen zutreffend einzuschätzen und geeignete Maßnahmen zu ergreifen.

Eine zentrale Säule unserer Strategie zum Schutz der Wirtschaft ist die Prävention, die „Prävention durch Information“. Sie beinhaltet umfangreiche Angebote zur Sensibilisierung in Bezug auf bestehende Sicherheitsrisiken und wird ergänzt durch eine vertrauensvolle Zusammenarbeit mit der Wirtschaft.

Im Rahmen des Ressortkreises Wirtschaftsschutz ist die Kooperation mit der ASW Ausdruck für eine funktionierende „Public-Private-Partnership“, unsere heutige gemeinsame Veranstaltung ist hierfür ein schöner Beleg.

Ich wünsche Ihnen eine informative und interessante Veranstaltung.

Wirtschaftsschutzkonzept des Bundesamtes für Verfassungsschutz - Bilanz der letzten 2 Jahre

Referent: Dr. Burkhard Even, Bundesamt für Verfassungsschutz

Meine sehr geehrten Damen und Herren,
vor zwei Jahren hat das Bundesamt für Verfassungsschutz im Rahmen der vom BMI initiierten Sicherheitspartnerschaft zwischen Staat und Wirtschaft seine bereits bestehenden Aktivitäten im Bereich des Wirtschaftsschutzes deutlich verstärkt, u.a. wurde ein eigenes Referat für diese Aufgabe eingerichtet. Die heutige Tagung gibt mir Gelegenheit, eine Bilanz dieser zwei Jahre zu ziehen.

Bilanz ziehen heißt zum einen, die Entwicklung der Bedrohungssituation in dieser Zeit zu analysieren. Zum anderen heißt es zu fragen, ob wir mit unseren Maßnahmen erfolgreich oder zumindest auf dem richtigen Weg sind.

Lassen Sie mich zunächst auf die aktuelle Bedrohung eingehen.

Die Bundesrepublik Deutschland ist nach wie vor ein interessantes und bevorzugtes Aufklärungsziel für ausländische Nachrichtendienste. Die Schwerpunkte ihrer Spionage- und Beschaffungsaktivitäten orientieren sich in aller Regel an aktuellen politischen Vorgaben und wirtschaftlichen Prioritäten in ihren Staaten. Im Fokus ausländischer Nachrichtendienste in Deutschland stehen insbesondere die Bereiche Politik, Militär, Wirtschaft, Wissenschaft und Forschung.

Für einige Nachrichtendienste nehmen Aufklärungs- und Beschaffungsziele gerade im Bereich Wirtschaftspolitik und Hochtechnologie einen zunehmend breiteren Raum ein. Auf dieses Phänomen, nämlich Wirtschaftsspionage, d.h. die von fremden Nachrichtendiensten ausgehende oder unterstützte Ausforschung von Unternehmen sowie Forschungs- und Entwicklungseinrichtungen, will ich näher eingehen.

Die Risiken, denen deutsche Unternehmen in einer globalen Welt ausgesetzt sind, sind erheblich angewachsen. Unsere Wirtschaft ist seit jeher technologie- und exportorientiert. Deutschland verdankt seinen Reichtum nicht in erster Linie Rohstoffen und Bodenschätzen. Vielmehr sind deutsche Unternehmen von ihren Ressourcen Wissen / Wissensvorsprung und Innovation abhängig. Dies sind die zentralen Objekte der Wertschöpfungskette unserer Volkswirtschaft und zugleich ihre entscheidenden Wettbewerbsfaktoren.

Diese Kernkompetenzen des Standortes Deutschland wecken naturgemäß Begehrlichkeiten sowohl bei ausländischen Konkurrenzunternehmen als auch bei fremden Staaten. Im globalen wirtschaftlichen Wettbewerb bedienen sich ausländische Regierungen und Konkurrenzunternehmen auch illegaler Mittel, d.h. auch der Spionage, um sich Wissen und Know-how anzueignen. So erwerben sie entscheidende Marktvorteile, ohne die immens hohen Kosten für Forschung und Entwicklung von Produkten und Technologien tragen zu müssen. Bei der Frage des Wettbewerbs um Know-how oder um Wissen und wissensbasierte Produkte und Verfah-

ren geht es um die Schaffung und Erhaltung von strategischen Wettbewerbsvorteilen; dabei ist der Begriff des Know-hows weit zu interpretieren und umfasst auch das Know-what, Know-who und Know-why.

Meine Damen und Herren,
die Gefährdungslage in Deutschland ist nach unseren Erkenntnissen sehr konkret. Staaten wie die Russische Föderation oder die Volksrepublik China betreiben mit ihren Nachrichtendiensten intensive Wirtschaftsspionage in unserem Land. Diplomatische und konsularische Vertretungen in Deutschland mit den darin abgetarnten sog. Legalresidenturen stellen eine bekannte Plattform für Spionageaktivitäten dar. Die dort als Diplomaten getarnt tätigen Nachrichtendienstoffiziere werden von ihren deutschen Kontaktpersonen kaum als Angehörige eines Nachrichtendienstes wahrgenommen. Sie können so ihr Interesse auch an sensiblen Informationen unauffällig mit ihrer offiziellen Funktion begründen. Sie betreiben so entweder selbst – offen oder konspirativ – Informationsbeschaffung oder leisten Unterstützung bei nachrichtendienstlichen Operationen. Im Fokus ihrer Ausspähungsbemühungen stehen Technologien, die für die Konkurrenzfähigkeit moderner Volkswirtschaften und bei der Eroberung von Märkten von Relevanz sind. Neben der Rüstungstechnologie sind Umwelttechnologien und fast alle Sparten der elektronischen und chemischen Industrie, der Maschinen- und Anlagenbau sowie die Luft- und Raumfahrttechnik von Ausspähungsaktivitäten betroffen. Sie richten sich auch auf strategische Informationen aus Politik und Wirtschaft.

An zwei Beispielen möchte ich dies verdeutlichen:

Anfang des Jahres ist uns ein Ausspähungsversuch im Büro einer Architektur- und Planungsgesellschaft bekannt geworden. Einem aufmerksamen Unternehmensmitarbeiter war aufgefallen, dass ein erst kurz zuvor eingestellter chinesischer Praktikant Projektdaten auf eine externe Festplatte kopiert hatte, obwohl er mit diesem Projekt ausdrücklich nicht befasst war. Bei der daraufhin erfolgten Überprüfung des Festplatteninhalts wurden neben allgemeinen auch sensible Daten gefunden. Zum einen befanden sich auf der externen Festplatte die kompletten Planungsunterlagen eines wirtschaftlichen Großprojekts, welche in den Händen von Konkurrenzunternehmen nichts zu suchen hätten. Zum anderen befanden sich dort sicherheitsrelevante Unterlagen bezüglich der Baumaßnahme einer deutschen Behörde. Insbesondere diese durch den Praktikanten unbefugt kopierten Daten wären für verschiedene fremde Geheimdienste von hohem Interesse.

An dieser Stelle möchte ich deutlich unterstreichen, dass aus dem Beispiel nicht gefolgert werden kann, chinesische Praktikanten seien per se oder auch nur mehrheitlich Spione. In Deutschland leben und arbeiten etwa 80.000 Chinesen, darunter etliche Wissenschaftler, Gastprofessoren, Studenten und Praktikanten. Die chinesischen Nachrichtendienste kennen das Wissenspotenzial dieser Personen sehr genau. Sie verschaffen sich einen Überblick über deren Zugänge und Kontakte und versuchen, Einzelne gezielt für eine Zusammenarbeit zu gewinnen.

Für die Nachrichtendienste bringt die Nutzung dieser so genannten Non-Professionals u.a. den Vorteil, dass bei bekannt werden eines Ausspähungsversuchs in aller Regel nicht ersicht-

lich wird, ob dieser aus Eigeninitiative oder im staatlichen, d.h. nachrichtendienstlichen Auftrag erfolgte.

Das Beispiel zeigt deutlich, dass der Unterschied zwischen Konkurrenzausspähung, Wirtschaftsspionage sowie sonstiger Spionage zuweilen fließend ist. Und das Beispiel zeigt auch, dass es immer sinnvoll ist, bei nur vorübergehend Beschäftigten genau auf die Beschränkung ihrer Zugangsmöglichkeiten zu achten.

In einem weiteren Fall kam es zu einer strafrechtlichen Ahndung eines versuchten Know-how-Diebstahls. Betroffen war ein chinesischer Geschäftsmann, der wegen Verrats von Betriebs- und Geschäftsgeheimnissen zu einer 18-monatigen Haftstrafe auf Bewährung verurteilt wurde.

Er hatte trotz ausdrücklichen Verbots während einer Werksbesichtigung heimlich mit einer am Hosengürtel befestigten Kleinkamera Aufnahmen angefertigt. Nur durch ein aufmerksames und sicherheitsbewusstes Einschreiten der Werkbegleiter wurde das Gerät entdeckt. Es enthielt in hoher Qualität Ton- und Bildaufzeichnungen zu Produkten und Produktionsabläufen. Diese hätten als Grundlage für einen Nachbau dienen können. Dem Unternehmen hätte dadurch eigenen Angaben zufolge ein Verlust in Millionenhöhe entstehen können.

Obgleich wir es hier nach der vorliegenden Sachlage mit einem Fall der Konkurrenzausspähung, d.h. der Ausforschung eines Unternehmens durch einen Wettbewerber zu tun haben, zeigt er doch sehr deutlich, dass es in der Prävention wenig Sinn macht, zwischen Wirtschaftsspionage und Konkurrenzausspähung zu unterscheiden.

Die notwendige Sensibilität hilft bei der Abwehr beider Spionageformen.

Eine stetig zunehmende Bedeutung erlangen internetbasierte Angriffe auf Computersysteme und mobile Kommunikationswege von Wirtschaftsunternehmen und Regierungsstellen; die besonderen Risiken der mobilen Kommunikation wird Herr Opfer vom BSI im Anschluss näher beleuchten.

Aus Sicht des Verfassungsschutzes möchte ich an dieser Stelle auf einige Besonderheiten bei elektronischen Angriffen eingehen, die sich in den letzten Jahren zu einer ständig steigenden Gefahr entwickelt haben.

Ohne weitreichende IT- und Internetnutzung ist effektives Wirtschaften heute nicht mehr denkbar. Wir alle haben Nutzen davon. Die Kehrseite ist jedoch eine weitgehende Abhängigkeit von dieser Technik. Und zu den Risiken zählt nicht zuletzt auch die Gefahr elektronischer Angriffe.

Eine häufig genutzte Angriffsmethode besteht in der Versendung von E-Mails mit verseuchten Anhängen. An erkennbar gezielt ausgesuchte Empfänger werden E-Mails versendet, die im Betreff für den Empfänger interessante Themen ansprechen. Im Inhaltsteil der E-Mail werden die jeweiligen Themen nur kurz angerissen und dann auf ein angehängtes Dokument verwiesen. Die signaturarme Schadsoftware, die mit kommerziellen Virenscannern typischerwei-

se nicht zu erkennen ist, wird dann beim Öffnen des Dokumentes unbemerkt installiert und gestartet. Nach der Installation versucht das aktivierte Schadprogramm Kontakt mit einem ihm vorgegebenen Computer im Internet aufzunehmen, der nicht der Ausgangspunkt des Angriffs ist. Über diesen Kontakt werden weitere Befehle übertragen, die den eigentlichen „Auftrag“ enthalten, Daten unbemerkt zu übermitteln oder auch direkte Schäden zu verursachen.

Insgesamt gilt für die elektronischen Angriffe, dass ihnen oftmals ein umfangreiches - auch mit nachrichtendienstlichen Methoden durchgeführtes - "Social Engineering" des Empfängers vorausgeht. Dazu sammeln die Angreifer im Vorfeld der Attacken Informationen über die potenziellen Zielpersonen, z.B. Visitenkarten, Profile und Tätigkeitsfelder, berufliche und persönliche Kontakte, Interessen und Hobbys und genutzte Informationsquellen wie Zeitungen oder andere Veröffentlichungen. So kann der Angreifer sicherstellen, dass die E-Mail durch ihre inhaltliche Gestaltung für die Empfänger interessant bzw. wichtig erscheint; das macht die Methode so heimtückisch und gefährlich.

Die bisherigen Recherchen nicht nur in Deutschland, sondern auch in anderen westlichen Staaten in diesem Bereich weisen auf einen oft staatlichen Ursprung solcher Angriffe hin. Dafür sprechen die zu beobachtenden Ziele der elektronischen Angriffe, deren Intensität, Struktur und Breite, sowohl bei den Wirtschaftsunternehmen, dem Bankensektor als auch in den spezifisch angegriffenen Behördenbereichen.

Zudem setzen die Qualität der genutzten Technik und die gut koordinierten Angriffe ein erhebliches finanzielles Potenzial und entsprechende personelle Ressourcen voraus. Ein Beleg für die Bedeutung elektronischer Angriffe stellt auch das Ergebnis einer 2009 erschienenen kanadischen Studie des „Munk Centre for International Studies“ über das so genannte „Ghostnet“ dar. Im Rahmen umfangreicher Untersuchungen wurde festgestellt, dass weltweit Rechner in über 100 Staaten mit Trojanern verseucht wurden. Diese Angriffe gingen von acht Servern in der Volksrepublik China aus und richteten sich gezielt u.a. gegen Rechner von Botschaften und anderen Regierungsstellen. Mittels solcher Trojaner kann z.B. der E-Mail Verkehr überwacht und ein Rechner zu eigenen weitergehenden Ausforschungszwecken fremdgesteuert werden.

Angesichts des Umstands, dass die Bedrohung durch elektronische Attacken ständig zunimmt und jeder Rechner im Internet gefährdet ist, kommt der IT-Sicherheit im Rahmen der Abwehr von Wirtschaftsspionage eine besondere Bedeutung zu. Dabei ist zu beachten, dass ergriffene Maßnahmen zur IT-Sicherheit nicht für die Ewigkeit gedacht sind, vielmehr bedürfen sie einer permanenten Überprüfung und Optimierung.

In diesem Zusammenhang möchte ich betonen, dass jede potenziell gefährdete Stelle, sei es Behörde oder Unternehmen, letztlich selbst die Verantwortung für alle ergriffenen oder nicht ergriffenen Maßnahmen zur Abwehr von elektronischen Attacken trägt. Es gib keine zentrale Stelle, weder im staatlichen noch im privaten Bereich, die dies übernehmen kann.

Deshalb mein Appell: lassen Sie Ihre Mitarbeiter nicht alleine; sorgen Sie für Ihre IT-Sicherheit!

Meine Damen und Herren,
in den Medien wird immer wieder über die mutmaßliche Höhe des volkswirtschaftlichen Schadens durch Wirtschaftsspionage bzw. Konkurrenzausspähung spekuliert. Auch die Verfassungsschutzbehörden werden immer wieder mit dieser Frage konfrontiert. Festzustellen ist, dass hierzu verlässliche und belastbare Aussagen fehlen und wahrscheinlich auch nicht präzise möglich sind. Untersuchungen hierzu sind abhängig von Selbstangaben Betroffener, die dann auf die gesamte Wirtschaft hochgerechnet werden müssen. Die Probleme beginnen schon bei der rechtlichen Einordnung der Sachverhalte. Auch die Schadenshöhe im Einzelfall kann regelmäßig nur sehr grob geschätzt werden. Entscheidend aber dürfte sein, dass die erkannten Fälle nur die Spitze des Eisberges darstellen. Es gibt eine erhebliche Dunkelziffer, teilweise aufgrund der Tatsache, dass Spionage - insbesondere die via Computer - oftmals gar nicht oder erst sehr spät, d.h. zu spät bemerkt wird. Hinzu kommt allerdings auch der Umstand, dass die betroffenen Unternehmen meist aus Furcht vor einem Imageschaden die Einschaltung der Sicherheitsbehörden scheuen.

Für die Frage der Notwendigkeit von Prävention kommt es auf den genauen Umfang des gesamtwirtschaftlichen Schadens allerdings letztlich nicht an. Entscheidend ist vielmehr dass das Risiko von Spionage sehr hoch ist und die Schadenshöhe jedenfalls im Einzelfall sehr erheblich sein kann.

Unsere Volkswirtschaft befindet sich derzeit in der wohl schwierigsten Bewährungsprobe seit Jahrzehnten. Als Folge der weltweiten Finanz- und Wirtschaftskrise wird bei vielen Unternehmen bedauerlicherweise allzu häufig auch auf dem Gebiet der Sicherheit und Prävention der Rotstift angesetzt. Es bedarf jedoch einer vorausschauenden und an nachhaltigen Kriterien ausgerichteten Sicherheitsstrategie in den Unternehmen, um Risiken und Gefahren - wie sie Wirtschaftsspionage und Konkurrenzausspähung darstellen - aktiv zu begegnen und sie bereits im Vorfeld zu vermeiden. Voraussetzung ist die Einsicht in die Notwendigkeit von Schutzmaßnahmen und Akzeptanz von Prävention. Daher sollte eine professionelle Aufklärung und Sensibilisierung der Mitarbeiter für mehr Sicherheit an erster Stelle stehen.

Nur der informierte und aufmerksame Mitarbeiter kann Risiken rechtzeitig erkennen und so Schaden im Unternehmen vermeiden. Und das ist gerade in wirtschaftlich schwieriger Zeit besonders wichtig.

Es stellt sich die Frage: Was tut der Staat zur Abwehr von Wirtschaftsspionage, insbesondere wie unterstützt er die deutsche Wirtschaft in diesem Bereich?

Die Bundesregierung räumt dem Schutz der Wirtschaft einen hohen Stellenwert ein. Zur Klarstellung sei allerdings deutlich gesagt: Die Verantwortung für Sicherheit und Schutz von Firmengeheimnissen trägt primär das Unternehmen selbst. Der Staat hat nicht die Aufgabe, hier umfassenden Schutz zu leisten. Er kann jedoch als „Hilfe zur Selbsthilfe“ die Unternehmen auf diesem Gebiet aktiv unterstützen und dadurch einen wichtigen Beitrag zum Wirtschaftsschutz leisten. Die heutige Sicherheitstagung ist ein Beispiel dafür.

Das Kernstück der staatlichen Initiative im Rahmen des Wirtschaftsschutzes bildet der interministerielle „Ressortkreis Wirtschaftsschutz“, der 2008 eingerichtet wurde. Ihm gehören

neben den Sicherheitsbehörden des Bundes Vertreter weiterer für Wirtschafts- und Sicherheitsfragen zuständige Ministerien sowie die ASW an. Der Ressortkreis tagt zweimal im Jahr, die nächste Sitzung wird Ende April im BMI stattfinden.

In diesem Gremium werden wirtschaftsschutzrelevante Informationen und Erkenntnisse ausgetauscht, bewertet, koordiniert und - das ist ein besonderes Anliegen - in geeigneter Weise der Wirtschaft zur Verfügung gestellt. Besondere Aufmerksamkeit wird der Effizienz der Kommunikationswege und dem Informationsaustausch zwischen den Sicherheitsbehörden und der Wirtschaft auf dem Gebiet gewidmet. Hierbei möchte ich unterstreichen, dass wir gerade den Dialog suchen; Wirtschaftsschutz darf keine Einbahnstraße sein!

Mit dem „Ressortkreises Wirtschaftsschutz“ 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 der Schutzmaßnahmen erfolgen kann.

Als ein Ergebnis des Ressortkreises möchte ich hier den von den Sicherheitsbehörden gemeinsam erstellten monatlich erscheinenden „Sonderbericht Wirtschaftsschutz“ hervorheben, der der ASW, ihren Mitgliedsverbänden und Mitgliedern zugeht, und der grundsätzliche und aktuelle Beiträge zu Gefährdungspotenzialen und Schadensereignissen in der Wirtschaft enthält.

In diesem Zusammenhang wurde auch die bestehende „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“ überarbeitet. Sie ist die Grundlage der Kooperation zwischen der ASW, dem BfV und anderen staatlichen Institutionen. Für dieses Jahr ist eine weitere Evaluierung der Rahmenregelung vorgesehen. Wir wollen hier unsere Erfahrungen für eine weitere Optimierung mit einbringen.

Meine Damen und Herren,
an dieser Stelle möchte ich besonders hervorheben, dass der Wirtschaftsschutz seit geraumer Zeit einen prioritären Platz im Aufgabenspektrum des Bundesamtes für Verfassungsschutz besitzt. Diese Schwerpunktsetzung wird vom Bundesinnenministerium voll mitgetragen und stetig angestoßen. So wurden vor zwei Jahren die Ressourcen im Wirtschaftsschutz durch ein eigenständiges Referat verstärkt, um die Informationstätigkeit als zentralen Service für die Wirtschaft weiter zu optimieren und die Zusammenarbeit mit den Landesbehörden für Verfassungsschutz in diesem Bereich zu beleben und besser zu koordinieren.

Unter dem Motto „Prävention durch Information“ werden Kontakt- und Informationsangebote für Wirtschaft, Wissenschaft und Forschung erstellt. Kernstück ist eine breit gestreute Vortragstätigkeit begleitet durch moderne Medien, seien es Broschüren, Internetauftritte und regelmäßige Newsletter.

Zu den Aktivitäten und damit zum Service unseres Wirtschaftsschutzreferates zählen insbesondere:

Sensibilisierungsvorträge in Unternehmen, sowohl bei den Global Playern als auch bei den kleinen und mittelständischen Unternehmen. In diesem Zusammenhang sind auch zu nennen die Wirtschaftsverbände und Organisationen sowie Hochschulen und sonstige Forschungseinrichtungen. Im vergangenen Jahr waren dies im besonderen Unternehmen und Verbände aus dem Telekommunikationsbereich, der IT-Branche, Luft- und Raumfahrt, Banken sowie dem Maschinen- und Anlagenbau. Hinzu kamen Sensibilisierungsgespräche bei verschiedenen Forschungseinrichtungen und Akademien.

Ergänzt werden diese Vorträge durch bilaterale Informationsgespräche zu konkreten Sicherheitsthemen und Sachverhalten.

Hervorheben möchte ich auch unseren regelmäßig erscheinenden Newsletter, mit dem wir auf eine besondere Resonanz gestoßen sind. Er verkörpert unseren Leitgedanken, nämlich: „Transparenz schafft Vertrauen und Vertrauen schafft Dialog“. Und eben dieser vertrauensvolle Dialog ist es, den wir uns mit der Wirtschaft wünschen.

Mit Beiträgen, die über die ASW an die Unternehmen gerichtet sind, berichten wir regelmäßig über Bedrohungspotenziale und Schadensereignisse aus verschiedenen Beobachtungsbereichen des Verfassungsschutzes, so z.B. auch aus dem militanten Linksextremismus.

Mit der Präsentation eines eigenen Angebots auf der Homepage des BfV verfügen wir über eine zusätzliche weitreichende Informationsplattform in Sachen Wirtschaftsspionage und Wirtschaftsschutz.

Abgerundet werden diese Aktivitäten durch eine intensive Öffentlichkeitsarbeit. Verstärkte Medienpräsenz des Themas Wirtschaftsspionage führt zwangsläufig zu einer Auseinandersetzung mit diesem Phänomen in der Gesellschaft und schärft ihr Sicherheitsbewusstsein.

Unser Wirtschaftsschutzreferat ist der zentrale Ansprechpartner in allen Belangen des Wirtschaftsschutzes und der Prävention sowohl für die ASW als auch für die Wirtschaft und die Unternehmen.
Sie werden dort immer ein offenes Ohr auch für vertrauliche Gespräche finden, das kann ich Ihnen versichern.

Als weitere Aktivitätsfelder mit der ASW möchte ich die gemeinsame Teilnahme an der alle zwei Jahre in Essen stattfindenden Messe „security“ nennen, so auch im Oktober diesen Jahres. Dabei erfahren wir seit Jahren auch eine wesentliche Unterstützung durch die Landesbehörden für Verfassungsschutz. Auch hier gilt unser Motto „Wirtschaftsschutz ist Teamwork“.

Wir praktizieren eine enge und konstruktive Zusammenarbeit insbesondere mit dem Bundeskriminalamt, dem Bundesnachrichtendienst und dem Bundesamt für die Sicherheit der Informationstechnik, zum Teil auch durch gemeinsame Sensibilisierungsmaßnahmen.

Der Schutz einer global agierenden Wirtschaft erfordert auch eine intensive Zusammenarbeit der Sicherheitsbehörden auf internationaler Ebene.

Deshalb stehen wir auf diesem Gebiet im regelmäßigen Informations- und Erfahrungsaustausch mit Partnerdiensten im Ausland. Das Bedrohungsszenario auf dem Gebiet der Wirtschaftsspionage ist in einer Reihe von Staaten, insbesondere in Europa, durchaus vergleichbar. Ergebnis und Zeichen dieser vertrauensvollen Partnerschaft ist die Anwesenheit unserer Kollegen aus der Schweiz und den Niederlanden sowie der sich anschließende Vortrag von Herrn Bartl vom österreichischen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung.

Die Hospitationen von Mitarbeitern des Wirtschaftsschutzreferates in der Sicherheitsabteilung von Großunternehmen haben sich besonders bewährt und dazu geführt, dass wir dadurch die Interessen und Sorgen der Wirtschaft besser verstehen können. Sie sind ein besonderer Beweis für eine praktizierte „Public-private-partnership“.

Meine Damen und Herren,
die Kombination aus persönlichen und medialen Kontaktmöglichkeiten stößt in der Wirtschaft auf erfreulich hohe Resonanz und führt zu einer Vielzahl von Kontakten und Gesprächen. In der Regel werden unsere Referenten zu Multiplikatorenveranstaltungen eingeladen. Aus diesen Kontakten haben sich zum Teil beständige Beziehungen verfestigt. In vielen Fällen kommt es zu Folgekontakten, Einzelinformationsgesprächen und erneuten Einladungen zu Vorträgen. An dieser Stelle möchte ich nochmals hervorheben, dass insbesondere unsere Sensibilisierungsvorträge sich einer überaus regen Nachfrage und Akzeptanz erfreuen. Dies spricht nicht nur für die Professionalität unserer Awareness-Maßnahmen sondern verdeutlicht zugleich auch den hohen Bedarf dieser Kontakte und Gespräche. Rechtzeitige Prävention ist bekanntlich die sicherste Art, Schaden im Unternehmen zu vermeiden.

Regelmäßige konstruktive Kontakte schaffen nicht nur Vertrauen, sie sind zugleich eine unabdingbare Voraussetzung für eine erfolgreiche Gefahrenabwehr und bereiten die Basis für einen echten Informations- und Erfahrungsaustausch.

Unser Angebot zur Sensibilisierung für Wirtschaftsspionage und Informationsschutz richtet sich primär an kleine und mittelständische Unternehmen, die das Rückgrad der deutschen Wirtschaft bilden.

Unsere Erfahrungen zeigen, dass dort zum Teil Spitzentechnologie und hohe Innovation vorzufinden sind, jedoch mangelt es oft am Bewusstsein für die unterschiedlichen Gefährdungsaspekte sowie an den notwendigen Vorsichtsmaßnahmen. Sicherheit ist leider nicht immer Chefsache, sondern häufig ein vernachlässigtes Thema und beschränkt sich in vielen Unternehmen auf IT-Sicherheit. Das Bewusstsein für Informationssicherheit mit den Aspekten Verhaltenssicherheit, Gebäudesicherung oder Sicherheit auf Reisen, u.a. im Ausland, ist in vielen Fällen gering.

Anders ist die Situation bei den als Global Player bezeichneten Unternehmen. In der Regel sind dort gut aufgestellte Sicherheitsabteilungen vorhanden. Diese sind allerdings häufig mit dem Problem konfrontiert, dass es den von ihnen getroffenen Sicherheitsvorkehrungen innerhalb der Konzerne oftmals an Einsicht in die Notwendigkeit und damit an Akzeptanz fehlt. Sie werden so lange als lästiges und unnötiges Beiwerk betrachtet, bis das Unternehmen

nachweislich Opfer eines Spionagefalles geworden ist. Hinzu kommt, dass bei mangelndem Sicherheitsbewusstsein Schadensfälle kaum detektiert werden.

Dabei kann ein präventives Sicherheitsmanagement, zu dem wir durch unsere Maßnahmen beitragen können, die Gesamtsituation des Unternehmens in verschiedener Hinsicht durchaus positiv beeinflussen, z.B. durch die nachhaltige Sicherung der Wettbewerbsfähigkeit, durch Optimierung des betriebswirtschaftlichen Erfolgs und nicht zuletzt durch Verbesserung des Image.

Bevor ich zum Schluss komme, möchte ich noch einmal hervorheben:

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

Hier ist aus unserer Sicht noch erheblicher Nachholbedarf.

Die Grundlage unserer Arbeit ist Vertrauen und Diskretion. Wir sind der Überzeugung, dass eine konstruktive und vertrauensvolle Zusammenarbeit zwischen der Wirtschaft und den Verfassungsschutzbehörden einen wirkungsvollen Beitrag zum Schutz der Unternehmen vor Wirtschaftsspionage leistet.

Wirtschaftsschutz ist und bleibt Teamwork!

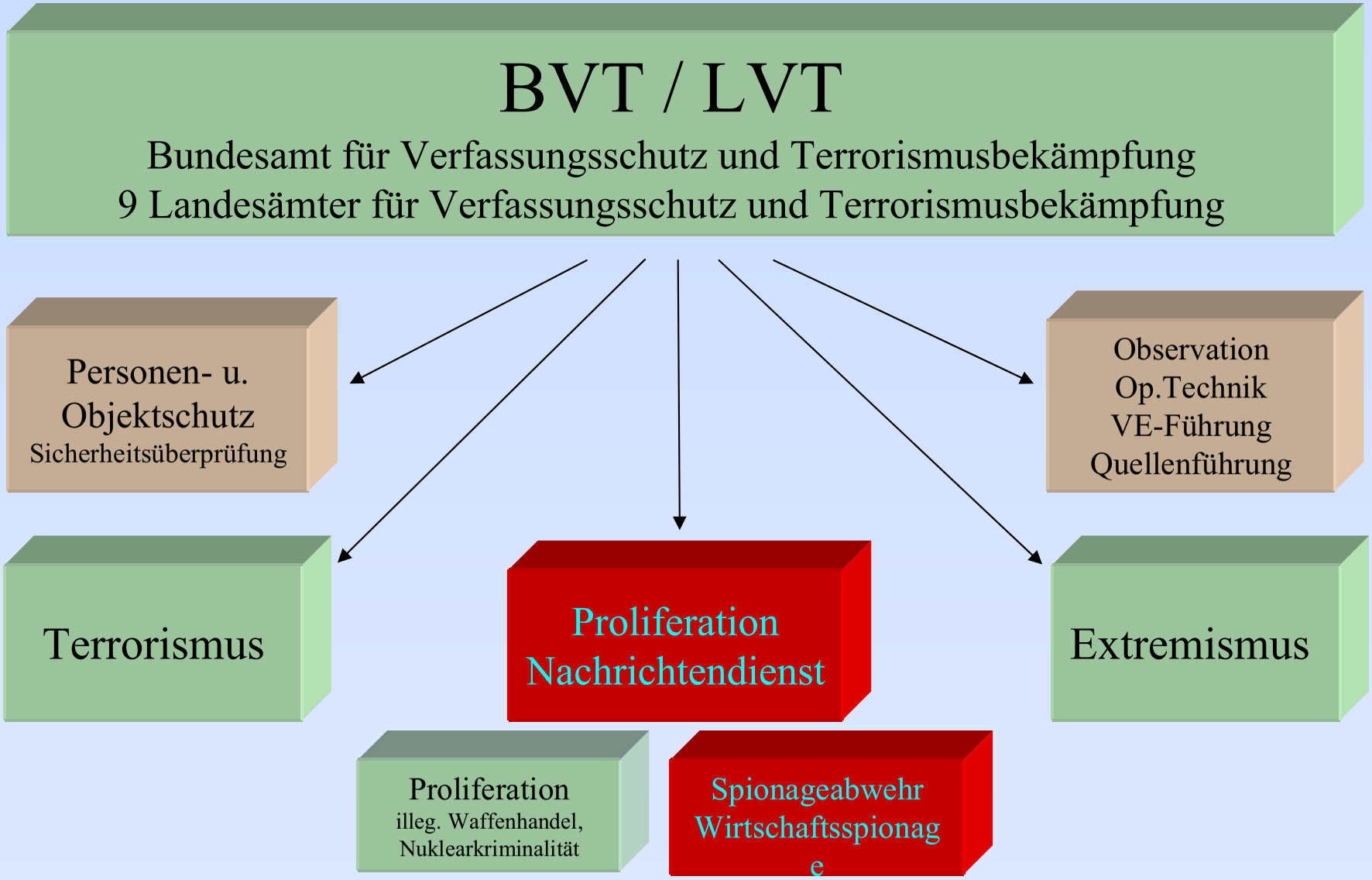
Meine Damen und Herren, ich denke, es ist deutlich geworden, dass sich auf dem Gebiet des Wirtschaftsschutzes bei den Verfassungsschutzbehörden von Bund und Ländern in den letzten Jahren einiges getan hat.

Die Resonanz und die erfreulich rege Nachfrage nach unserem Service zeigt m.E., dass wir auf dem richtigen Weg sind.

Ich möchte Sie daher ausdrücklich ermuntern, auch weiterhin unser breites Angebot zu nutzen und bei sich bietender Gelegenheit dafür zu werben.

Danke für Ihre Aufmerksamkeit!


BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG
BVT
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES


BVT / LVT
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
9 Landesämter für Verfassungsschutz und Terrorismusbekämpfung
Personen- u. Objektschutz
Sicherheitsüberprüfung
Observation
Op.Technik
VE-Führung
Quellenführung
Terrorismus
Proliferation Nachrichtendienst
Extremismus
Proliferation
illeg. Waffenhandel, Nuklearkriminalität
Spionageabwehr
Wirtschaftsspionage

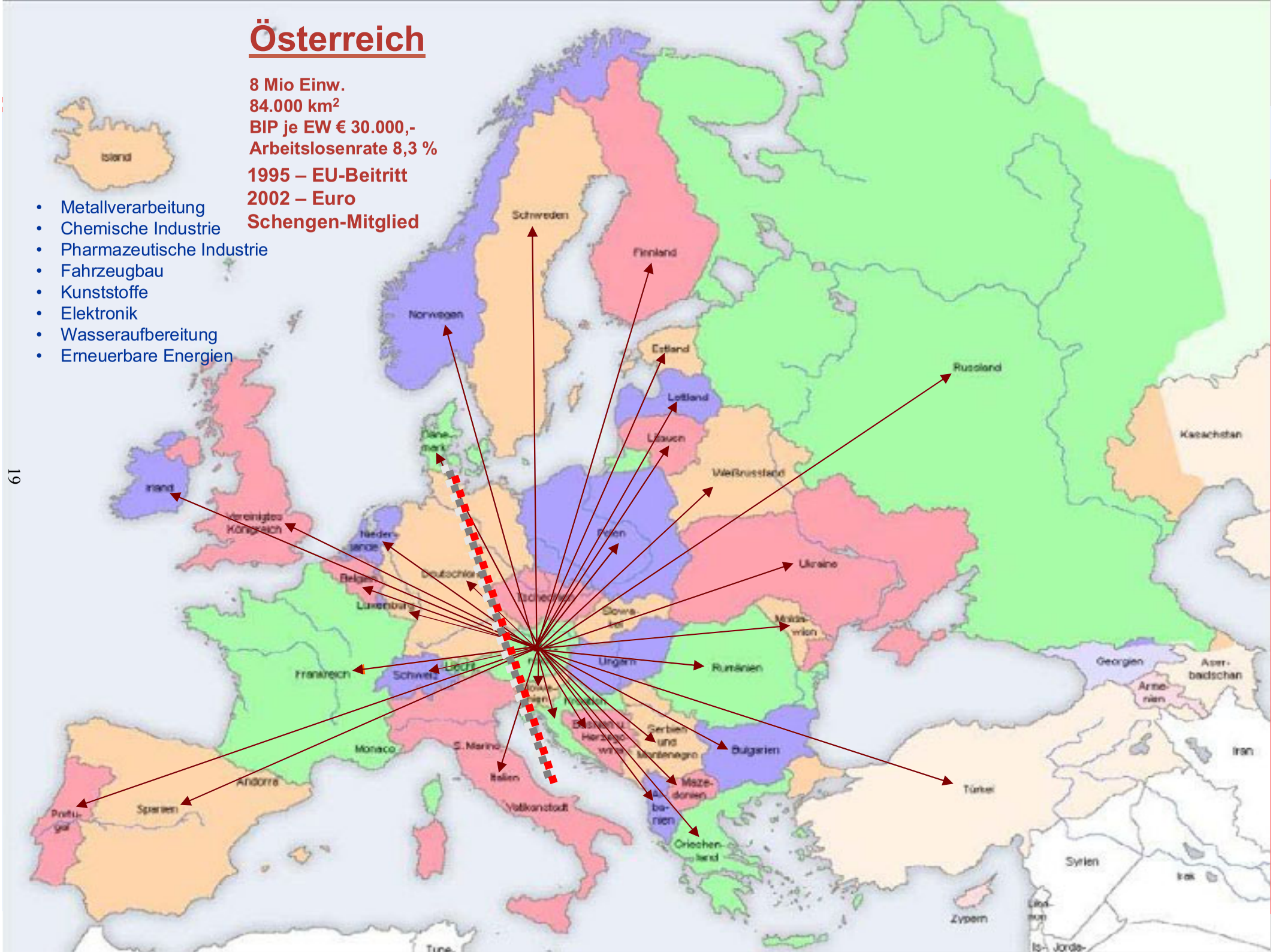
18

Österreich

8 Mio Einw.
84.000 km²
BIP je EW € 30.000,-
Arbeitslosenrate 8,3 %

1995 – EU-Beitritt
2002 – Euro
Schengen-Mitglied

- Metallverarbeitung
- Chemische Industrie
- Pharmazeutische Industrie
- Fahrzeugbau
- Kunststoffe
- Elektronik
- Wasseraufbereitung
- Erneuerbare Energien



Wirtschaftsspionage

Konkurrenzausspähung

RUSSLAND

PUTIN 2007 - „Der Nachrichtendienst muss seine Anstrengungen verstärken, um die russische Wirtschaft und die Interessen russischer Unternehmen im Ausland aktiver zu unterstützen.“.

SWR-Chef Sergej Lebedew - Informationen aus der Aufklärung sind unbezahlbar. So hätten wissenschaftlich-technische Informationen und zugehöriges Know-how einen Effekt, den man in Zahlen mit vielen Nullen messen müsse.

In Österreich festgestellte Aufklärungsziele

- **Metallverarbeitung**
- **Maschinenbau**
- **Autoindustrie**
- **Elektronik**
- **Erneuerbare Energien**
- **Umwelttechnologie**
- **Biotechnik**
- **Chemie**

- Softwareentwicklungen
- Wasseraufbereitung
- Medizinische Hochtechnologie
- Pharmazeutische Industrie
- Atomforschung
- Nachrichtentechnik
- Flugsicherungstechnik
- Energietechnik
- Kommunikationstechnik
- Funksysteme für Betriebsanlagen
- Schlüsselfunksysteme für Exekutive
- Containerkameras
- Röhren und Objektive für Nachtsichtgeräte
- Spezialmunition
- Militärische Schutzbekleidung
- Technische Datenbanken
- Spezialtextilien aus Kohlegewebe

Motivation

- berufliche Perspektiven
- materielle Vorteile
- Selbstwertgefühl
- Liebesbeziehung

- **berufliche Unzufriedenheit**

- finanzielle Probleme
- politische / religiöse Überzeugung oder ethnische Gründe
- Abenteuerlust
- andere charakterliche oder psychologische Aspekte

23

.BVT

CHINA

- **Autoindustrie**
- **Umwelttechnologien**
- **Erneuerbare Energien**

25

2005

9.职业及工作单位 Beruf und Arbeitgeber

2008

四、你的联系方式/ Teil 4. Ihre Kontaktdaten

4.1 你的工作单位或学校名称 / Name des Arbeitgebers oder der Schule:	4.2 日间电话 /Telefonnummer(tagsüber):
4.3 你的工作单位或学校地址 / Adresse des Arbeitgebers oder der Schule:	4.4 夜间电话 / Telefonnummer (in der Privatzeit):
4.5 你的家庭住址 / Privatadresse:	4.6 你的电子信箱 / E-mail Adresse:

1.14 当前职业（可多选）/Derzeitige berufliche Tätigkeit(en):

☐商人 / Geschäftsmann	☐ 教师、学生 / Leher oder Student	☐政府官员 / Beamter
☐乘务人员 / Crew Mitglied (Flugzeug, Zug oder Schiff)		☐新闻从业人员 / Journalist oder Redakteur
☐议员 / Parlamentarier, Kongressabgeordneter oder Senator		☐宗教人士 / Geistlichkeit

☐其他（请说明）/Sonstiges (Bitte nähere Angaben):

2005

13.邀请单位名称或邀请人姓名、地址、电话 Name, Anschrift und Telefonnummer der Auskunftsstelle oder Auskunftspersonen in China

2008

2.5 请按时间顺序列明你访问中国的地点（省及市/县）/Bitte Ihre Besuchsorte in China der Reihenfolge nach angeben:	

4.7 在华邀请、联系的单位名称或探亲对象的姓名 /Name der Person in China, die Sie besuchen möchten:	4.8 联系电话 /Telefonnummer dieser Person:
4.9 在华邀请、联系的单位名称或探亲对象的地址 /Adresse der einladenden Person:	4.10 电子信箱 / E-mail Adresse dieser Person:

27

Danke

für Ihre Aufmerksamkeit !

28


BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG
BVT
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

29

IT-basierte Informationsgewinnung durch Angriffe auf die Mobilkommunikation

Gefährdungen und Schutzmaßnahmen

Joachim Opfer

Fachbereich 22: Abhörsicherheit

Bundesamt für Sicherheit in der Informationstechnik

18. März 2010

Gliederung

- Ausgangslage
- Appetizer: Berlin Mitte
- Appetizer: Brüssel
- Problemaufriss
- Bedrohungslage: WLAN
- Bedrohungslage: Bluetooth
- Bedrohungslage: GSM
- Bedrohungslage: Mobile Endgeräte
- Fazit
- Exemplarische Lösungen

Einleitung

- Ausgangslage
  - Verlagerung der Aufklärungsmethoden: Elektronische Ausspähung / Aufklärung ist risikoärmer als “social engineering”.
  - „Belauschen“ ist deutlich risikoärmer als aktive Angriffe.
  - Elektronische Aufklärungsfähigkeiten sind weit verbreitet und werden durch weltweite Kommunikationsnetze erleichtert.
  - IT-Sicherheitssysteme sind im Fokus der Nachrichtendienste.

Problemaufriss (1)

- Fact 1: Aktuelle I&K-Systeme sind zu komplex, um unter Sicherheitsgesichtspunkten vollständig beherrschbar zu sein.
  (Beispiel: Sicherheitslücken in Betriebssystemen)

- Fact 2: Time to Market:
  ->Funktionalität vor Sicherheit

- Fact 3: Eine nachträgliche Sicherheitsüberprüfung ist aufgrund der Komplexität nicht durchführbar.

- Konsequenz 1: Wenig widerstandsfähige Systeme verfügbar.

Problemaufriss (2)

- Begründete Befürchtung: Unter dem Gesichtspunkt der Industriespionage ist mit einer vorsätzlichen Schwächung strategisch wichtiger I&K-Systeme zu rechnen.
  Auch betroffen: IT-Sicherheitssysteme

- Fact 4: Eine solche Beeinflussung ist faktisch nicht detektierbar.

- Konsequenz 2: Vertrauenswürdige, d.h. nationale Lösungen sind unter der Bedrohung „Industriespionage“ unabdingbar.

Verlässliche IT-Sicherheitssysteme

- **Strategie des BSI:**

Für zentrale IT-Sicherheitssysteme:

- Zusammenarbeit mit nationalen, vertrauenswürdigen Firmen
- Designvorgaben für „Sicherheit in unsicheren Umgebungen“
  - Vertrauenswürdige Sicherheitsanker (Chipkarten)
  - Kapselung
  - Virtualisierung
- Evaluierung / Zulassung

Zusammenfassung
Technische Angriffe auf IKT

- Bedrohung:
  - (nicht nur) nachrichtendienstliche Angriffe auf Informations- und Kommunikationstechnologie
- Angriffspunkte:
  - 1. öffentliche Kommunikationsstrecken „abhören“
    - kein Entdeckungsrisiko, deshalb bevorzugte Technologie
  - 2. Platzierung von „vorbereitetem“ Equipment
    - geringes Entdeckungsrisiko, schwieriger zu platzieren
  - 3. Nachträgliches Einschleusen von „Aufklärungshilfen“
    - geringes Entdeckungsrisiko, (heute noch) leicht zu platzieren
  - 4. Ausnutzen von Schwachstellen
- Angriffsziele:
  - gesprochenes Wort (klassisch)
  - digitale Information (zunehmend)

Bedrohungslage WLAN

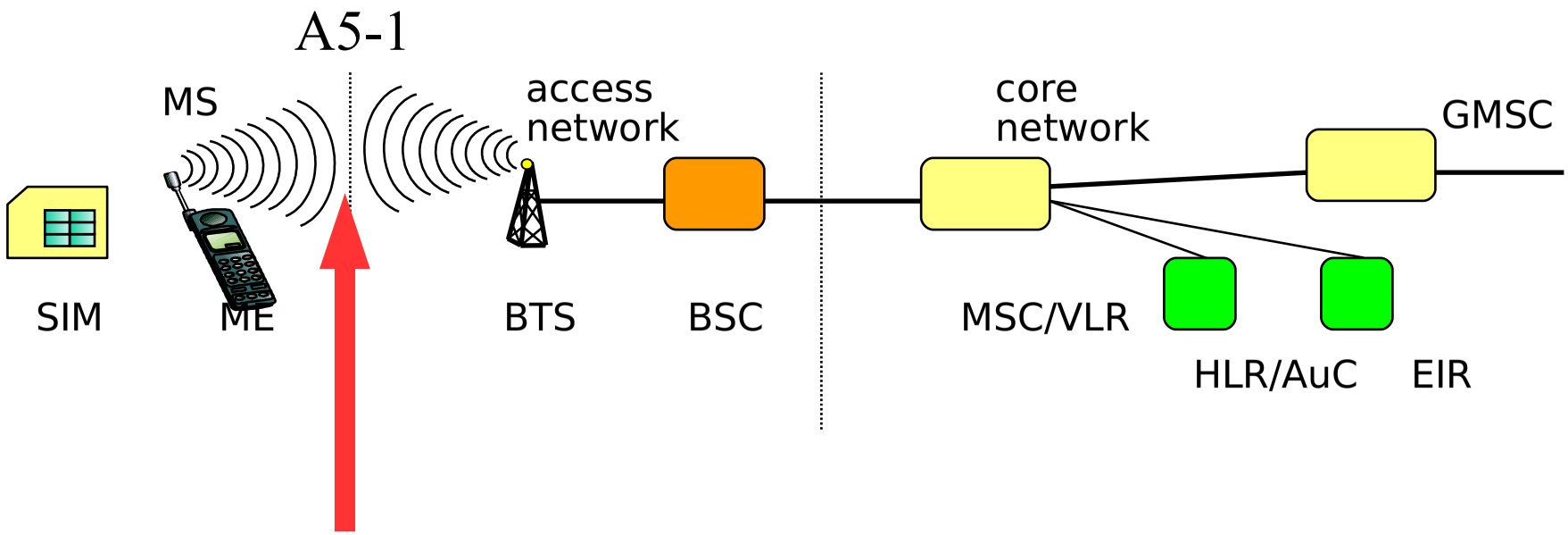
- Funkwellen potenziell von jedermann abhörbar (shared medium)
- Im Small-Office/Home-Office-Bereich mit Pre-Shared-Key (PSK)
  - Verschlüsselungsart und Passphrase sind entscheidend für die Güte der Verbindung
  - WEP (unsicher)
  - WPA/WPA2 (sicherer)
    - Zahlreiche Angriffstools im Internet
    - Triviale Passwörter (PSK) können mit einer Wörterbuchattacke herausgefunden werden

- Für höheren Schutzbedarf
  - Beispielsweise RADIUS-Server mit EAP-TLS

Bedrohungslage Bluetooth

- Funkwellen potenziell von jedermann abhörbar
- Bekannte Angriffe betreffen „alte“ Hardware mit Implementierungsfehlern (grob vor 2006)
- Dennoch gilt:
  - Bluetooth nach Gebrauch wieder ausschalten
  - Sichtbarkeit nur bei Bedarf einschalten
  - neue Firmwareversion installieren
  - keine Nachrichten unbekannter Herkunft öffnen
  - Einführung mit dem Bluetooth-Standard 2.1
    - „Secure Simple Pairing“
    - Geräte voraussichtlich in 2009 verfügbar
    - erhöhter Schutz gegen passives Abhören und Attacken

Bedrohungslage GSM

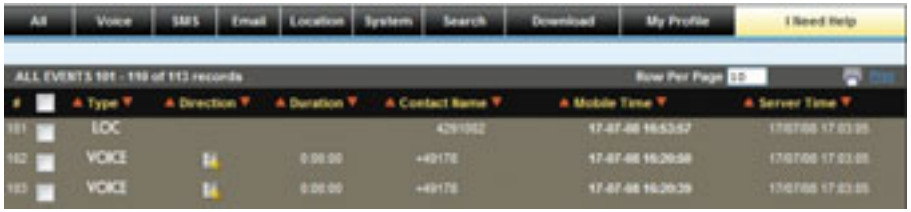


Schwächen in der Verschlüsselung sind lange bekannt, aber:
Enormer Rechenaufwand.
Seit CCC 2009: Erforderliche Rechenleistung ist leicht verfügbar, mit „Hacker-Tools“ im Internet ist zu rechnen.

Bedrohungslage - Trojaner

Spionagesoftware Flexispy

- Hauptfunktionen
  - Versteckte Anrufe zur Zielperson
  - Speicherung von SMS und Emails
  - Protokollierung von Verbindungsdaten und Zellinformationen
  - Call Interception
- Web-Interface



Schadsoftware wie Flexispy können durch versierte Programmierer leicht nachgebaut werden!

Bedrohungslage - Netzbetreiber

Problem Provider:

- Juli 2009:
  Der arabische Mobilfunk-Provider Etisalat hat 140.000 BlackBerry-Handys über einen Softwareupdate mit einer Spionagesoftware infiziert.

23.07.2009, 13:15 | ★★★★★ | 5 Kommentare

Abhörskandal: Der Spion im Blackberry

Der arabische Mobilfunk-Provider Etisalat hat offenbar die Blackberry-Handys von über 140 000 Kunden verwanzt. Hersteller RIM wehrt sich nun gegen die Schnüffel-Software.

Von FOCUS-Online-Autor Torsten Kleinz

Eigentlich ist es ein alltäglicher Vorgang: Die Blackberry-Kunden des arabischen Mobilfunk-Providers Etisalat erhielten Anfang Juli eine SMS-Nachricht zu einem neuen Software-Update. Wenn sie dem angegebenen Link folgten, sollten Verbindungsfehler beseitigt und die Erreichbarkeit der **Smartphones** erhöht werden.

Welche Nachrichten US-Präsident Barack Obama auf seinem Blackberry empfängt, wüssten viele Geheimdienste gerne AFP

Die Nachricht war legitim und gleichzeitig auch nicht. Zwar stammte sie tatsächlich von dem Mobilfunk-Provider, das unverdächtig „Registration" genannte Programm war aber in Wahrheit eine Spionage-Software aus US-Produktion.

Fehler führt zu Entdeckung

Aufgeflogen ist der breit angelegte Spionageangriff nur, weil sich die Software als fehlerhaft erwies. So schalteten einige Blackberrys nicht mehr in den Ruhezustand, der Akku des Smartphones war schon nach einer halben Stunde leer gesaugt. Für den Programmierer Nigel Gourlay, der derzeit in Katar wohnt, war das rätselhafte Verhalten seines Blackberrys Grund genug, sich das vermeintliche Service-Update genauer anzusehen.

Bedrohungslage
Mobile Endgeräte

- Angriffe auf die Kommunikation:
  - Bluetooth
  - WLAN
  - GSM
- Angriffe auf das Endgerät:
  - Auslesen des Speicherinhalts
  - Gelöschte Daten sind nicht gelöscht!
  - Installation von Spionageprogrammen
- Handyviren
- Angriffe über die Netzinfrastruktur

Bedrohungslage
Mobile Endgeräte

- Schadfunktionen
  - Mithören der Telefonaten, Mails, SMS
  - Auslesen von Anruflisten, SMS, Mails, Adresslisten ...
  - Protokollierung von Verbindungsdaten („Persönliche Vorratsdatenspeicherung“)
  - Mithören von Raumgesprächen
  - Lokalisierung (auch GPS!)
  - Zugang zur IT-Infrastruktur

Zusammenfassung:

- Angriffspotential auf Mobilkommunikation:
  - Angriffe auf die Mobilkommunikationsinfrastruktur mit preiswerten Mitteln von NDs, OK, und Terrororganisationen machbar.
  - Aktive Spionageangriffe über die Infrastrukturen aus der Ferne und kaum detektierbar möglich.
  - Fehlende Sicherheitseigenschaften mobiler Endgeräte eröffnen zusätzliche Angriffspfade.

Fazit

- Professionelle Industriespionage als Bedrohung ist real.
- Zur Abwehr ist der Einsatz vertrauenswürdiger IT-Sicherheitsprodukte aus nationaler Fertigung notwendig.
- Die Antworten des BSI auf die Bedrohungen sind
  - Grundschutz
  - Beratung
  - IT-Sicherheitslösungen in den Bereichen
    - Internet
    - Telefonie
    - Mobile Kommunikation
    - Gateways
- Die Lösungen sind auch für die Wirtschaft verfügbar

Mobile Endgeräte: sicherheitsbewußter Umgang

- Mobile Endgeräte sind kein Spielzeug!
  - Nur dienstlich notwendige Anwendungen installieren
  - Kritische Prüfung des Notwendigen
- SIM-PIN aktivieren
- Mobile Endgeräte nicht unbeaufsichtigt lassen
  - Installation von Spionageprogrammen ist in Sekunden möglich
- Geregelter Weitergabe- und Entsorgungsprozess
  - Vollständiges Rücksetzen des Gerätes mit zuverlässigem Löschen
- Virenschutz

Mobile Endgeräte
Zielperspektive für Mobilität mit Sicherheit

- Verschlüsselung der Kommunikation
  - Sprache
  - SMS
  - Daten
- Sicheres Schlüsselmanagement
- Verschlüsselung der gespeicherten Daten
- Kapselung von Sicherheitsfunktionen in einem geprüften „Sicherheitsanker“
- Sichere Speicherung von Langzeitgeheimnissen
- Sichere Authentisierung mit „Digitaler Identität“

Lösungen: Mobile Sprachkommunikation

TOPSec GSM

ROHDE&SCHWARZ

http://www.rohde-schwarz.de/

Lösungen: TOPSec-Mobile

- Zulassung für VS- Nur für den Dienstgebrauch
  - nach Anpassung der Kryptographie (ggf auch VS-Vertraulich)
- Fortentwicklung der Lösung für den VS-V/Geheim-Bereich
  - Zielrichtung: Interoperabilitätsstandard SCIP
  - Arbeitsname: Elcrodat Mobile
  - Zeithorizont: Q3 2010

Lösungen: Mobile Sprach- (künftig auch Daten-) kommunikation

http://www.secusmart.de/

secusmart

So einfach kann sicheres Telefonieren sein.

Secusmart kombiniert weltweit als einziges Unternehmen hochsichere Kommunikation und kryptografisch gesicherte Authentifizierung mit modernsten Mobiltelefonen.

Secusmart verschlüsselt Handy- Telefonate hochsicher mit BSI-Kryptotechnik 25.02.08

Telefonieren mit dem Handy ist heute nicht mehr sicher. Der in fast allen GSM-Mobilfunknetzen... → weiterlesen

Lösungen: Secuvoice

- Lösung basiert auf der BOS-Kryptokomponente
  - Integriert auf µSD-Karte
- Sprachverschlüsselung in der Nokia E-Serie
  - von Secusmart in Zusammenarbeit mit Nokia integriert
  - VS-NfD-Zulassung: seit Q4 2008
- Geplante Erweiterungen:
  - Erweiterung auf SMS
  - Erweiterung auf E-Mail

Lösungen: Email-Synchronisation/PIM SimKo2

- Betriebssystem: Windows Mobile 6.1
- Applikationen: Pocket Outlook, Active Sync
- Hardware: htc Touch hd
- Schlüsselspeicher/
- Random Generator: µSD-Card
- Verbindungen : GSM/GPRS/UMTS

- Speicherverschlüsselung
- Sichere Authentisierung mit PIN
- Digitale Identität (Zertifikatsbasiert)
- Zugelassenes VPN-Tunneling

- Spezifische Einsatzempfehlung für VS-NfD

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Joachim Opfer
Godesberger Allee 185-189
D-53175 Bonn

Tel: +49-1888-9582-5500
Fax: +49-1888-109582-5500

Joachim.Opfer@bsi.bund.de
www.bsi.bund.de

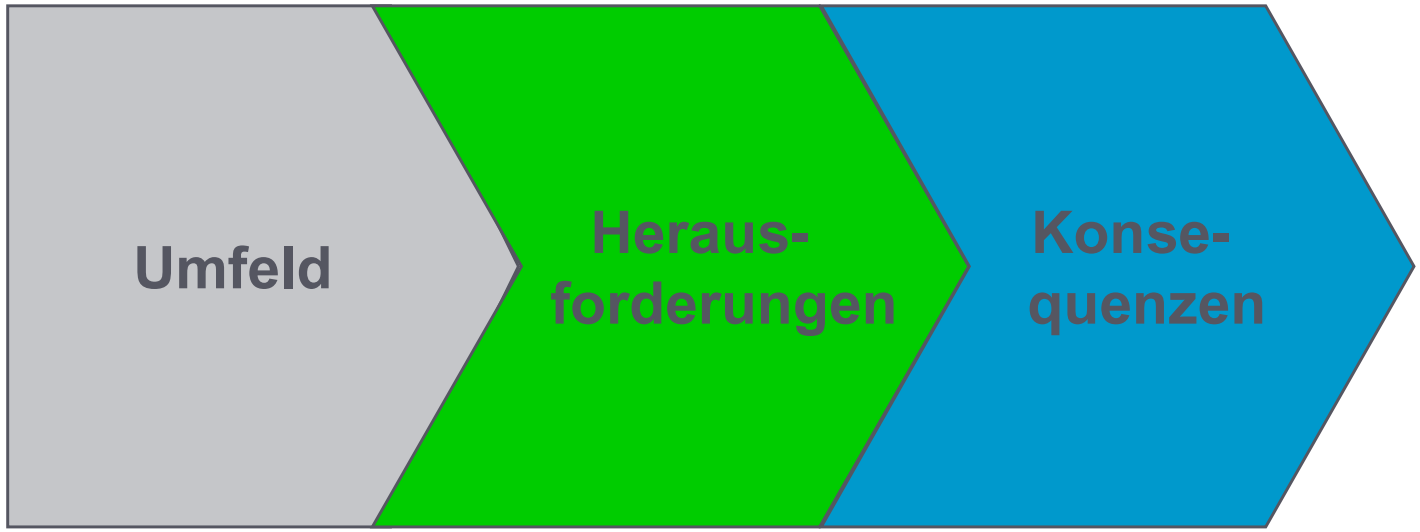
Corporate Security eines Global Players

Umfeld – Herausforderungen – Konsequenzen

Michael Sorge, Leiter Corporate Security Bayer AG

Köln, 18. März 2010

Corporate Security eines Global Players



Aufgabenstellung Corporate Security

- Aufgabe der Abteilung BAG RC Corporate Security ist es, sicherheitsrelevante Situationen zu erkennen und ihnen, möglichst bereits im Vorfeld, erfolgreich entgegenzuwirken. Dazu ist eine systematische Auswertung aller relevanten Informationen ebenso notwendig wie die enge Zusammenarbeit mit allen Institutionen auf dem Gebiet der Gefahrenabwehr. Corporate Security ist deshalb in internationale Netze eingebunden, die einen optimalen Informationsfluss sicherstellen. Im Gegenzug muss im Ereignisfall richtig und der Situation angemessen reagiert werden, um die Sicherheit unserer Mitarbeiter und Einrichtungen bestmöglich zu gewährleisten.
- Der Aufgabenbereich beinhaltet:
  - Konzernweites globales Risk- und Krisenmanagement für den Konzern.
  - Know-how- und Informationsschutz („Human Firewall“)
  - Internationale Produkt- und Markenpiraterie
  - Betreuung von Konzernveranstaltungen in punkto Sicherheit (Executive and Event Protection)
  - weltweite fachliche Verantwortung für die Funktion Security im Bayer-Konzern.

Einflussfaktoren Corporate Security

Äußere Einflussfaktoren / Ursachen für Global Risks

- Gesetzliches Umfeld – national und international

- Behördenstruktur
  - Zunehmende Vernetzung von organisierter Kriminalität, ansteigendes Potential von Wirtschaftskriminalität und Wirtschaftsspionage

- Medien/Internet

- Politisches Umfeld (sicherheitspolitisch, innenpolitisch, sozio-kulturell)
  - unterschiedlich ausgeprägte und entwickelte Rechts- und Gesellschaftssysteme
  - Unterschiedlich ausgeprägte Formen des politischen Extremismus und der politischen und sozialen Agitation gegen Wirtschaft und Teile der Gesellschaft

- Sicherheitsumfeld
  - unterschiedliche regionen-spezifische Kriminalitätskulturen und -formen

Produktpalette

Standorte

Absatzmärkte

Grundlage ist die unternehmensspezifische Organisation!

Unternehmensstruktur und -Organisation

Unternehmensziele

Einflussfaktoren Corporate Security

- **Häufig unterschätzte „innere“ Einflussfaktoren**
  - Wertewandel bei den Mitarbeitern
  - Abnahme des Zugehörigkeitsgefühles zum Unternehmen und der Loyalität
  - Einfluss von negativer / kritischer Medienberichterstattung über das Unternehmen auf Mitarbeiter
  - Know-how Abfluss durch Umstrukturierung und Outsourcing (hohe Mitarbeiter-Fluktuation)
  - Personalabwerbung (Headhunting)
  - Infiltration und Ausspähung durch eigene Mitarbeiter (Datendiebstahl, Betrug, Korruption – Ergebnisse einer aktuellen Studie von KPMG: zwei drittel der Unternehmen rechnen mit einer Zunahme der Kriminalität im eigenen Betrieb in den nächsten Jahren)

Risiko-Umfeld

09

Mega-Trends im globalen Sicherheitsumfeld

- Demographischer Wandel
  - Überalterung und Rückgang der erwerbstätigen Bevölkerung in Industriestaaten
  - Bis 2050 wird die europäische Bevölkerung von 495 auf 455 Mio. sinken, in Deutschland von derzeit 82 Mio. auf 65-70 Mio. bis 2060 (-15%)
  - Über 30% der Bevölkerung wird älter als 65 Jahre sein
- Migration
  - 2 Mio. Zuwanderer aus Afrika „warten“ derzeit an den Europäischen Grenzen
  - Um die Kosten der Einschleusung zu zurückzubezahlen, schließt das organisierte Verbrechen z.B. „Arbeitsverträge“ mit den Einwanderern ab (Quelle: BKA Herbsttagung 2009)
- Systemische Risiken der Wirtschaftsordnung
  - Abhängigkeit von Energie, Wasser, Finanzmitteln, Lebensmittelverteilung
  - Abhängigkeit von Hauptlieferanten für Energie Russland, Norwegen, Algerien, Nigeria, Venezuela (teils internationale Brennpunkte!)
  - Kaukasus Region und Kaspisches Meer: Bodenschätze und Krisenherde (Georgien, Iran, Tschetschenien, etc.)

Mega-Trends im globalen Sicherheitsumfeld

- Technologiewandel
  - Hin zur Massenkommunikationsgesellschaft:
    - 43,5 Mio. Deutsche sind “online“ (+67% im Vergleich zu 2008)
    - es existieren 107 Mio. Mobilfunkverträge in Deutschland
- Gesellschaftlicher Wandel abgeleitet von der Diskussion um gerechte Verteilung und Diskriminierung
  - Militanz u.a. bei technologischen- und Umweltthemen
  - Verrohung der öffentlichen Räume (z.B. U-Bahn Stationen, Sportarenen)
- Neue Formen von transnationaler Organisierter Kriminalität als Globaler Wirtschaftsfaktor
  - Global agierende Mafia (z.B. Geschäftsbeziehungen zwischen Mexikanischen Drogenkartellen und Italienischer Mafiaorganisation)
  - Informations- und Kommunikationskriminalität
    - Datenmanipulation / Datenspionage steigen stark an – hohe Dunkelziffer
    - Bedingt durch verstärkte weltweite technische Vernetzung durch das Internet
    - Intellectual Property
  - Produkt- und Markenpiraterie
    - 70% der weltweit verkauften Plagiate stammt aus Asien (China)
    - Angezeigte Fälle in Deutschland haben sich in den letzten 10 Jahren verdreifacht

Mega-Trends im globalen Sicherheitsumfeld

- Mega-Cities
  - 2015 wird es weltweit 60 Mega-Cities mit mehr als 700 Mio. Einwohnern geben
  - Mega-Cities zerfallen in Schichten: eine Unterwelt, die eine eigene Gesellschaft bildet, eine dünne Mittelschicht, die sich mit aller Macht abschottet, darüber die Schicht der Reichen und der Mega-Reichen
  - Mega-Cities sind Heimat der Hauptsitze vieler Auslandsgesellschaften der Global Player
    - Beispiel Mexico City: Bevölkerung 21,2 Mio.; Drittgrößtes Ballungsgebiet der Welt
      - Zusammentreffen von Überfluss und Elend
      - Explosives Bevölkerungswachstum
    - Beispiel Sao Paulo: Bevölkerung 11 Mio.; größte Stadt auf der Südhalbkugel
      - gilt als Schlüsselstadt für das globale Wirtschaftssystem („Alpha City“)
      - Das organisierte Verbrechen (PCC – „Erstes Hauptstadtkommando“) löste – teils aus Gefängnissen heraus gesteuert – in 2006 eine heftige Welle der Gewalt in der Stadt aus (180 Tote, Straßenschlachten, Plünderungen)
      - 20% (2,2 Mio.) der Bevölkerung lebt in einer Favela (Armenviertel), entspricht der Einwohnerzahl von Hamburg und Frankfurt am Main zusammen
      - Gleichzeitig besitzt die Stadt die meisten Hubschrauberlandeplätze

Mega-Trends im globalen Sicherheitsumfeld

- Failing States und Regionalkonflikte
  - 40-60 Staaten weltweit gelten als von einer Erosion des staatlichen Gewaltmonopols geprägt
  - 1,2 Mrd. Menschen leben in diesen Staaten, was 20% der Weltbevölkerung entspricht → Nährboden für Bürgerkriege, Organisiertes Verbrechen und rechtsfreie Räume
  - Viele Failing States sind gleichzeitig Ressourcen-Staaten für Bodenschätze (z.B. Iraq, Nigeria, Venezuela)
  - Organisierte Kriminalität etabliert sich in Failing States durch Korruption und mangelnde Handlungsfähigkeit der Staaten/Justiz/Polizei → parasitäre Ausbreitung → Angriff auf westliche Demokratien
  - Ungelöste Konflikte in Europa (Balkan) und Nah- und Fernost (Afghanistan, Pakistan, Somalia, etc.) berühren die weltweite Sicherheitslage und damit auch global agierende Unternehmen

Mega-Trends im globalen Sicherheitsumfeld

- <u>Entwicklungen in der Kriminalitätslage und Megatrends in der Gesellschaft erfordern angepasste sicherheitsbehördliche Antworten</u>
  - Kernaussagen von Prof. Dr. Dr. Hans J. Gießmann (Herbsttagung des BKA 2009) zum Thema „Internationale Brennpunkte der Kriminalität“:
    - Die „Globalisierung der Kriminalität“ beeinflusst die Voraussetzungen für Kriminalitätsprävention, Gefahrenabwehr und Strafverfolgung
    - Nationale Verbrechensbekämpfung nicht mehr ausreichend!
    - Wachsende Flexibilisierung, Vernetzung und Internationalisierung der Sicherheitseinrichtungen notwendig
    - Ganzheitliches Konzept für die internationale Zusammenarbeit erforderlich

Sicherheitsdienstleister

- Streitpunkt Qualifizierung der privaten Sicherheitsdienstleister - konträre Ansichten:
- **Deutschland:** strengere Zulassungsregeln für Sicherheitsdienstleister europaweit gefordert. Derzeit findet weder eine Überprüfung der Straflosigkeit statt, noch ist ein Nachweis der fachlichen Qualifikation gefordert. (Vortrag des Vizepräsidenten des Bundesverbandes Deutscher Wach- und Sicherheitsunternehmen)
- **Europa:** Eingrenzung der Aufgaben von privaten Sicherheitsdienstleistern (Tagung der European Police Union, Luxemburg)
  - klare Abgrenzung zu den Aufgaben der staatlichen Sicherheitsbehörden
  - Verstärkte Privatisierung staatlicher Aufgaben kritisch
  - Sicherheit nur noch für die „Reichen“
- Beispiel aus der Praxis für Anforderungen / Versprechen:
  - Zuverlässiger Partner beim Objekt-, Veranstaltungs- und Personenschutz
- Realität bei einem gefährdeten Projekt

99

Private Sicherheitsdienstleister

- Aktueller Presse-Artikel März 2010: Beruf „Problemlöser“
- „Ich biege Dinge wieder gerade“
- „Springerstiefel, Handschellen, Schlagstock am Gürtel, Revolver am Halfter, Pfefferspray, Gasmaske, Nachtsichtbrille vorm guerillamäßig geschwärztem Gesicht“
- „Seine Auftraggeber sind Führungskräfte aus der Industrie, die ein Problem aus der Welt geschafft haben möchten. Ohne Anzeige, ohne Polizei“
- „Sie sitzen in verdeckten Büros über den Globus verstreut und operieren nach den „Zellentaktik“: Wie aus dem Nichts auftauchen, Job erledigen, verschwinden, ohne Spuren zu hinterlassen“
- „ Ist doch klar, dass ich bei Einsätzen schon mal in die Randbereiche des gesetzlich erlaubten abtauche. Ich nenne das legale Grauzonentaktik. Oder aggressive Angriffsverteidigung“
- „Das Abseilen trainiert der Problemlöser in einem Steinbruch im Schwarzwald, Häuserkampf in einer verlassenen Siedlung in den Vogesen, das Überwältigen und Festnehmen von Verdächtigen in abgelegenen Gewerbegebieten

Herausforderungen für Corporate Security

- Äußere und Innere Einflussfaktoren, globale Risiken und Mega-Trends erfordern eine wachsende Internationalität von Corporate Security in folgenden Bereichen:
  - Mitarbeiterqualität
    - Interkulturelle Kompetenz
    - Behördenkompetenz
    - Wirtschaftskompetenz
  - Analysekompetenz
  - Kenntnisse des Geschäftsmodells und der Organisationsstrukturen

89

Kommunale Infrastrukturen / Einrichtungen

- Trends: Zunehmende Vernetzung von kommunalen Einrichtungen und privaten Investoren
- „Stadtliche“ Geschäfte: Kommunen verkaufen an US-Investoren wichtige Infrastruktur und mieten diese dann teuer zurück (Quelle: Zeit Magazin)
- Langfristig an US-Investoren verleaste Einrichtungen, z.B.:
  - Infrastrukturanlagen des ÖPNV
  - Wasserver- und -entsorgungsanlagen
  - Messe- und Veranstaltungshallen
  - Müllverbrennungsanlagen
  - Krankenhäuser
  - Flughafeninfrastruktur

69

Vernetzte Strukturen

- Moderne und professionelle nationale Verbandsstrukturen für Wirtschaft und Behörden als Grundlage für die Zusammenarbeit
- Verstärkte Europäisierung der Verbandsstrukturen für Zusammenarbeit mit dem behördlichen Sektor
  - Zusammenarbeit mit privaten Parteien und Personen erstmals für Europol (neuer Status als EU-Behörde) beschrieben. Die Behörde will vor allem im Bereich der Früherkennung vermehrt auf die Expertise von Universitäten und Unternehmen zurückgreifen (Ratsbeschluss zu Europol der EU-Kommission)
- Zersplitterung der deutschen Verbandsstrukturen
- Europäisches Strafrecht ein „Flickenteppich von unterschiedlichen Vorschriften“ → Entwicklung einer „Strafrechtsarchitektur der EU“ erforderlich (Prof.Dr.Dr.h.c. Sieber, BKA-Hersttagung 2009)
  - Schaffung einer europäischen Staatsanwaltschaft
  - Ausweitung des Kooperationsrecht
  - Integration von OLAF und Europol in das europäische Strafjustizsystem etc.

Konsequenzen (1)

- "Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen" des Bundesministerium des Inneren (überarbeitet am 01.07.2008)
  - Austausch sicherheitsrelevanter Informationen („Hohl- und Bringschuld“) zwischen der Wirtschaft und den Behörden (Bundeskanzleramt, Auswärtiges Amt, Verfassungsschutz, BKA, Amt für den Militärischen Abschirmdienst, Zollkriminalamt, BSI, BBK, Presse- und Informationsamt) mit Koordinierungsstelle ASW
  - Ressortkreis „Wirtschaftsschutz“ (Wirtschaftsspionage und Koordinierung von Gegenmaßnahmen) des BMI
  - SPOC Regelung mit BKA / Global Player Initiative
- Zusammenarbeit mit den nationalen Behörden nicht nur in Sicherheitsfragen sondern auch
  - Bei Qualifizierung / Qualität (z.B. EBS, HfÖV Bremen) im Bereich Unternehmenssicherheit
  - Bei gegenseitigen Hospitationen (z.B. BKA, Auswärtiges Amt)
  - Bei Etablierung eines „legalen“ und „verdachtsfreien“ Roundtable mit Behördenleitung der nationalen Sicherheitsbehörden
  - Grundlegende Akzeptanz der Rolle der Wirtschaft als Partner der inneren / äußeren Sicherheit bei wichtigen Themenfeldern

Konsequenzen (2)

- Stärkung der Verbindung zwischen ASW, BDI und DIHK
- Stärkung und Entwicklung des ASW als „Center of Competence“
- Stärkung der Funktion Corporate Security durch Etablierung ethischer und gesetzeskonformer Verhaltensgrundsätze gemeinsam mit Behörden
  - „Code of Ethics“ für das Thema Sicherheit in Unternehmen
  - Schaffung der Funktion des Bundesbeauftragten für („Wirtschafts-“) Sicherheit?
  - Anerkennung von Qualitätsstandards (analog Ö-Normen)

Qualitätsstandards

ÖNORMEN S 2400 - 2403

- Die Definition von Mindestanforderungen für die Ausgestaltung des Security Managements in Form von Normen schafft Transparenz hinsichtlich der Anforderungen an das Security Management insbesondere bei international agierenden Unternehmen. Normen schaffen eine Basis für die Beurteilung eines wirksamen Security Managements
- Guter Ansatz, der jedoch in Kooperation von Behörden und Unternehmen weiterentwickelt werden sollte

73

Selbstverständnis Corporate Security

- Von der reinen Sicherheitsexpertise und „Konzernpolizei“ zum **Business Partner**
  - des Unternehmens
    - Ableitung der Sicherheitsstrategie von der Unternehmensstrategie
    - Schutz von Prozessen und Infrastrukturen
    - Berücksichtigung von spezifischen Sicherheitsaspekten in Wachstums- und Krisenzeiten
    - Zusammenarbeit / Austausch / Kommunikation von Unternehmen und Behörden

Quellen

- Bundesministerium des Inneren: „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“, 2008
- DIE ZEIT Magazin, „Stadtliche Geschäfte“, Matthias Stolz, 2010
- DER SPIEGEL, „Das Gewaltlabor“, Ralf Hoppe, 2006
- CD Sicherheitsmanagement 6/09
- SUEDDEUTSCHE Zeitung, „Megacity Mexiko-Stadt: Eine harte, verlockende Droge“, Guillermo Fadanelli, 2007
- „Weltweite Brennpunkte der Kriminalität – Auswirkungen auf Deutschland“, Petra Volkmer, Bericht über die BKA-Hersttagung 2009
- „Internationale Brennpunkte der Kriminalität“, Jörg Ziercke, Vortrag im Rahmen der BKA-Herbsttagung 2009
- „Neue Rechtsgrundlage für Europol“, Michael Niemeier und Markus Walter, Kriminalistik 1/2010
- LE MONDE diplomatique: „Atlas der Globalisierung“, 2009
- KPMG: Wirtschaftskriminalität in Deutschland“, Studie, 2010

Danke für Ihre Aufmerksamkeit

77

Informationsschutz-Angebote in Deutschland

- *Aus Sicht der Nachfrager* -

4. Sicherheitstagung des BfV und der ASW am 18. März 2010 in Köln
A. Huber - Beuth Hochschule für Technik Berlin

Beuth Hochschule für Technik Berlin

staatliche Hochschule
gegründet 1971
10.000 Studierende
300 Professuren
70 Studiengänge

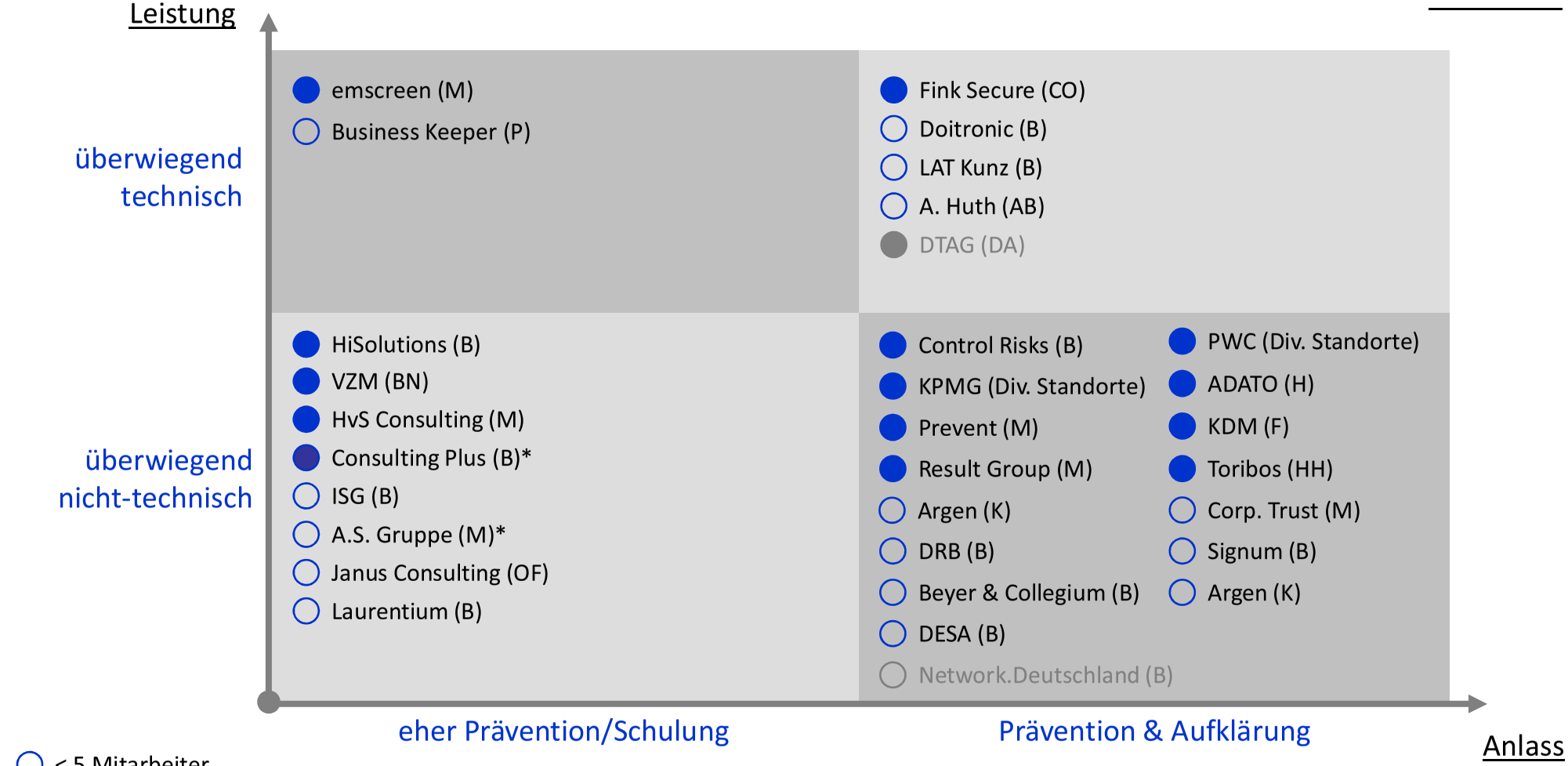
Forschungsschwerpunkte:

- Übersicht und Bewertung der **deutschen Studiengänge** im Bereich „Sicherheit“ und „Security“
- **Spionage-** und **Social Engineering-Techniken** des ehemaligen MfS bzw. der JHS (in Kooperation mit der BStU)
- **Corporate Security-Organisationen** in deutschen KMU und MNU (Entstehung, Formen, Vor-/Nachteile)
- **Informationsschutz Prüf- und Maßnahmenkatalog** (ISPM): Self-Audit von Unternehmen (inkl. Präventions-Spiel zur Awareness)
- Inländische **Informationsschutz-Angebote**: Dienstleister, Ausrüster und Behörden (Markt, Profile, Entwicklung)

Fokus heute

Anbieterlandschaft: inländische Dienstleister (keine überwiegenden IT-Dienstleister, keine reinen Detekteien)

Auswahl



○ < 5 Mitarbeiter
● 5 bis 20 Mitarbeiter

Quelle: Unternehmensangaben, JA (2007-09), Schätzungen
* Relevante Geschäftsbereiche (sofern abgrenzbar)

Aussagen über Qualität und Vertrauenswürdigkeit der Anbieter werden durch diese Darstellung nicht gegeben

Anbieterlandschaft: inländische IuK-Security Ausrüster (i. W. HW, ohne Identity/Access)

Auswahl

Siemens COM & SBS	→ COM zersplittert (i. W. NSN) – Zukunft SIS?
Utimaco	→ Größtenteils verkauft an Sophos (UK/US)
Infineon	→ kleiner Geschäftsbereich
VODA	→ Insolvent – größtenteils zum Verkauf beim Insolvenzverwalter
Secunet*	~ 40 M€ Umsatz (BS- & HS-Bereich)
R&S SIT	~ 25 M€ Umsatz
AVIRA	~ 25 M€ Umsatz
Astaro	~ 25 M€ Umsatz
DERMALOG	~ 12 M€ Umsatz
T-Systems*	~ 10 M€ Umsatz (Security-Bereich)
GeNUA	~ 7 M€ Umsatz
ATMedia	~ 5 M€ Umsatz
cryptovision	~ 3,5 M€ Umsatz
Sirrix	~ 3 M€ Umsatz
CE-Infosys	~ 2,5 M€ Umsatz

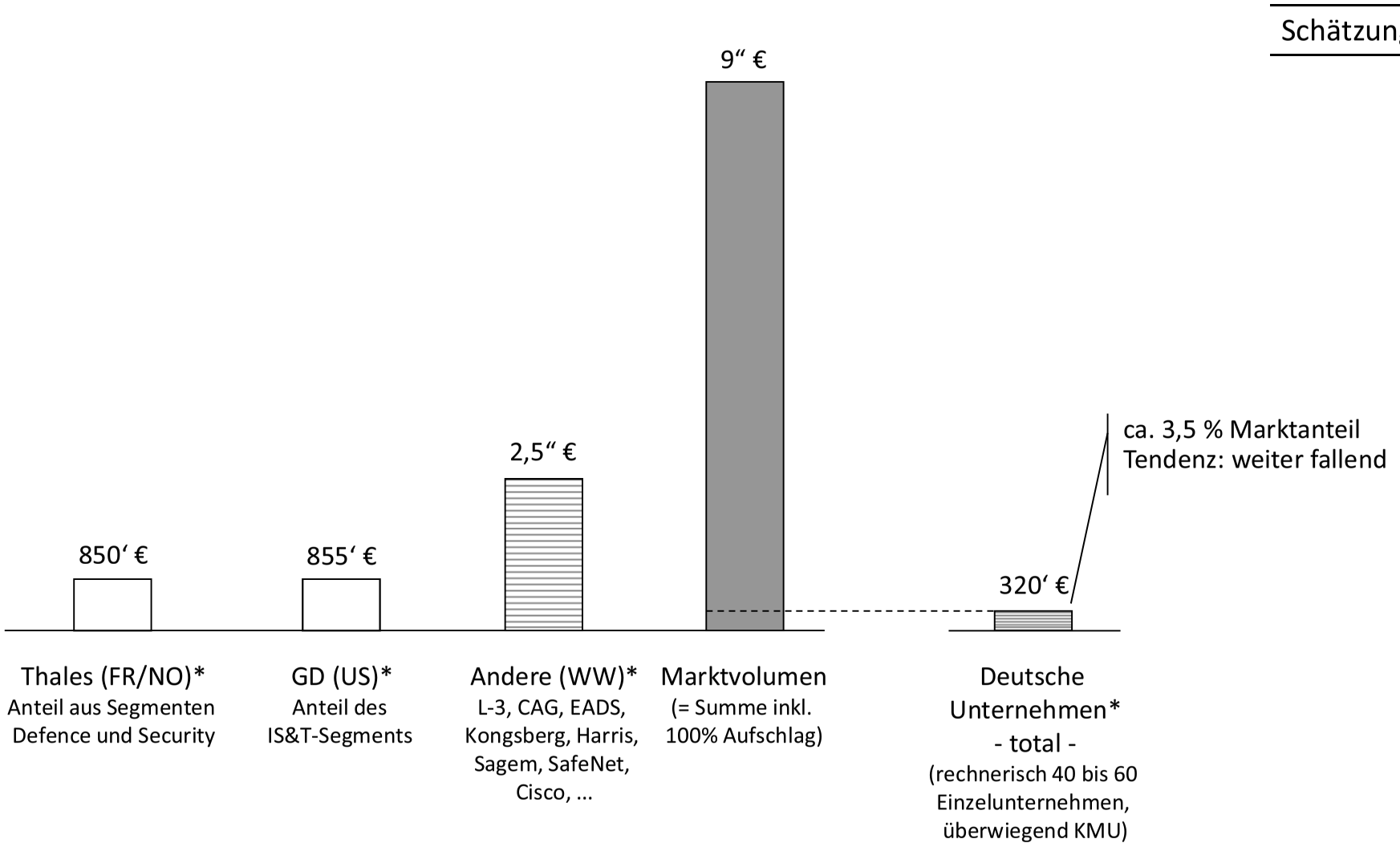
Nettovolumen: ca. 160 M€ p.a.

+ 100%

Bruttovolumen: ca. **320 M€** p.a.

Quelle: Unternehmensangaben, JA (2007-09), Schätzungen
* Relevante Geschäftsbereiche (sofern abgrenzbar)

Anbieterlandschaft: inländische IuK-Security Ausrüster auf dem Weltmarkt

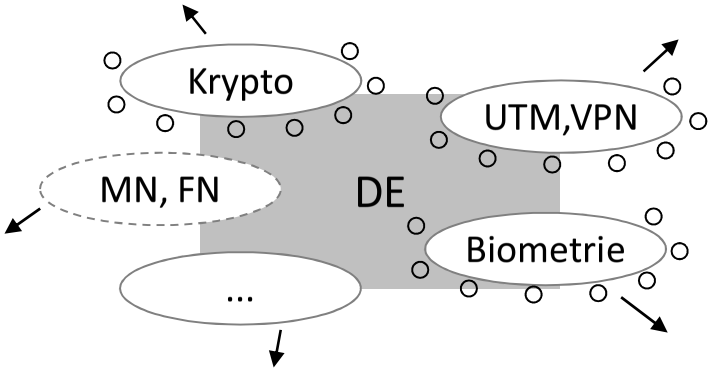


Quelle: Unternehmensangaben, JA (2007-09), Schätzungen
* Relevante Geschäftsbereiche (sofern abgrenzbar)

Anbieterlandschaft: inländische IuK-Security Ausrüster (Soll- und Ist-Zustand)

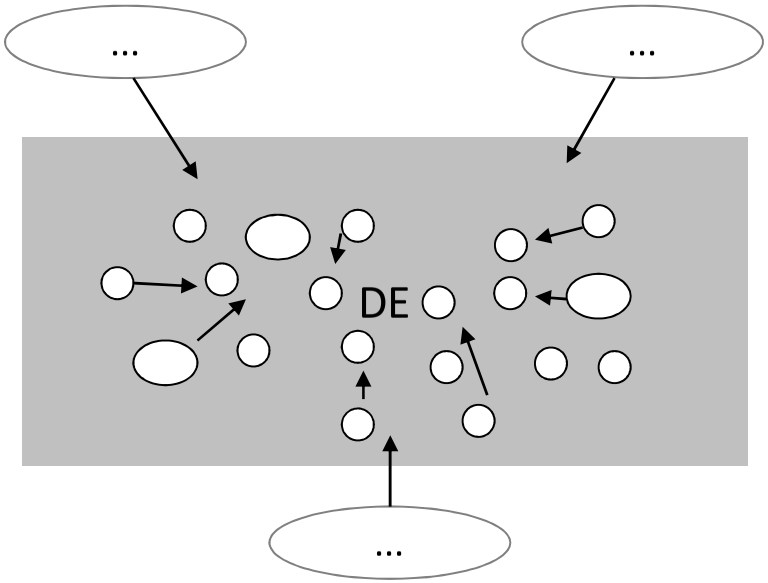
Soll-Zustand

- Portfolio an Unternehmen in signifikanter **Größe**, die auf dem Weltmarkt **wettbewerbsfähig** und von innovativen, flexiblen **Start-ups** umgeben sind.
- Dazu ist weniger ein Technologierückstand aufzuholen sondern vor allem weltweite **vertriebliche Präsenz**, **Vernetzung** in den internationalen Gremien und Investitionen in **Marketing** und den Bekanntheitsgrad auf- bzw. auszubauen.



Situation heute

- Relativ kleine deutsche Unternehmen machen sich **gegenseitig** im Inlandsmarkt Konkurrenz.
- Gleichzeitig bauen wesentlich größere und stärkere **ausländische Anbieter** Ihre Präsenz in Deutschland immer weiter aus.



Anbieterlandschaft: Marktattraktivität und Potenzial deutscher IuK-Security Ausrüster

Hohe **Marktattraktivität**: Volumen, Prestige, Marktwachstum (ca. 11% CAGR[1])

Inländische Unternehmen können daran nur **unterdurchschnittlich partizipieren**

- Keine „**Economies of Scale**“ nutzbar. Für bestimmte neue Technologien ist inländischer Markt zu klein, dadurch tlw. Investitionszurückhaltung und hohe Abhängigkeit von Staatsaufträgen
- Unterdurchschnittlich ausgeprägtes weltweites **Vertriebsnetz**
- Zu geringe Integration in internationale **Gremien** (Technologie, Standardisierung)
- Zunehmende Standardisierung (z. B. IP, SCIP, NINE) baut **Eintrittsbarrieren** für global Player im Inland ab
- **Trends** (z. B. Embedded Security, Software statt Hardware, COTS/MOTS) laufen HW-Ausrüstern entgegen
- Auch **ESB** Bw wird zunehmend mit Sicherheitsprodukten ausländischer global Player bedient
- Von vorhandenem hohem Vertrauen in „**Made in Germany**“-Produkte lässt sich kaum profitieren
- Deutschland ist bereits heute auf **Sicherheitsprodukte ausländischer Unternehmen** angewiesen

Schwächen deutscher Unternehmen basieren fast ausschließlich auf **Größennachteilen**

1) Analyse Umsatzwachstum internationaler Unternehmen, Auswertung von Marktstudien: u. a. IDC, Forrester, Experton

Anbieterlandschaft: Behörden

Über behördliche Angebote, die sich an die nicht-geheimschutzbetreute Wirtschaft richten, besteht in den Unternehmen hohe Unsicherheit.

Übergreifende Ergebnisse:

- **Zunahme der Aktivitäten/Angebote** – auch in Zusammenarbeit mit Organisationen (z. B. ASW)
- **Hohe Professionalität** und **gute Zusammenarbeit** mit einzelnen Behörden (**BSI** immer wieder hervorgehoben)
- Angst vor **fehlender Kontrollmöglichkeit** (z. B. hinsichtlich **Vorgehen** und **Veröffentlichung**)
- **Stark unterschiedlich** wahrgenommene **Qualität** von Präventionsmaßnahmen, Beratung und Information. Unterschiede lassen sich tlw. weniger an bestimmten Behörden, sondern an beteiligten Personen festmachen
- Behörden-Auftrag (aus Nachfragersicht) tlw. **unklar** („... können wir nur in Ausnahmefällen tätig werden“)
- Auch bei zuständigen Behördenvertretern bestehen tlw. **Unsicherheiten** bzgl. **eigener Angebote** und insbesondere der Angebote und des **Auftrags anderer Behörden**
- Starke **Fragmentierung** aus Nachfragersicht und schwierig zu überblickende **Zuständigkeiten**: Mit Ausnahme BSI Abt. 2 **kaum einheitliche Verantwortung** für Bund, Länder und geheimschutzbetreute Industrie

? „Liegt der Grund für zunehmende Wirtschaftsspionage in der mangelnden Unterstützung durch den BND?“

Im Rahmen einer WiKri-Studie von einer führenden WP-Gesellschaft an Unternehmen gestellt (Ende 2009)

? "Da Daten anders als Autos oder Handys keine Sachen sind, kann man sie nicht stehlen“

Eine Landes-Justizministerin (Februar 2010)

Fazit

- Einige der inländischen Anbieter spielen **technologisch** derzeit noch in der **Weltspitze** mit
- **Kompetenzen** einzelner **Behörden** weltweit **führend**
- Attraktiver Weltmarkt, der grundsätzlich „wie gemacht“ für Deutschland scheint, kann jedoch durch **Größennachteile** der Unternehmen nicht erschlossen werden. Deutscher Marktanteil sinkt
- Gefahr, nun auch den **technologischen Anschluss zu verlieren**
- Damit steht der **Ausgleich zunehmender nationaler Sicherheitsrisiken** (Staat/Wirtschaft) **auf dem Spiel**

85

Segment	Dienstleister	Ausrüster	Behörden
Ziel	Vertrauensbildung	Wettbewerbsfähigkeit, Ausgleich nat. Sicherheitsrisiken	Übergreifende Verantwortung
Ansätze	• Schaffung eines freiwilligen „Siegels“, mit objektiv-messbaren Kriterien (z. B. Nachweise über: Anzahl festangestellter Mitarbeiter, sicherheitsüberprüfte Mitarbeiter Ausbildungen, Gesellschafter, Unbedenklich-keitsbescheinigung, Pol. Führungszeugnis) • Selbstverpflichtung • Meldung/Aufnahme von Unregelmäßigkeiten (analog Hinweisgeber- bzw. Ombuds-mannsystemen) • ...	• Industrie-Konsolidierung • Bessere und vor allem direktere Vernetzung und Austausch zwischen Bedarfsträgern und Ausrüstern (nicht nur zu Mittlern wie z. B. IT-Amt). Einbindung in Langfristplanung • ...	• „Grenzschutz“ als hoheitliche Aufgabe muss in „Informations-Schutz“ umdefiniert werden (nicht nur für Behörden und geheimschutzb. Wirtschaft) • Eindeutige Verantwortungslage • Berücksichtigung existierender, übergreifender Verantwortung, Image und erwarteter Ver-schiebung von Angriffszenarien • ...

Profil & Kontakt

Prof. Dr.-Ing. Alexander Huber
seit 2006 Professor für Betriebswirtschaftslehre & Strategische Planung

Lebenslauf:
- Studium Wirtschaftsingenieurwesen TU Berlin und UC Berkeley (USA)
- Promotion in Informatik
- ab 1996: vier Jahre IT-Berater bei Accenture
- ab 2000: drei Jahre operatives Management bei Siemens
- ab 2003: drei Jahre strategische Unternehmensplanung bei Siemens
- Mitglied des Führungskreises der Siemens AG

Sonstige Tätigkeiten:
- Beirat zweier mittelständischer Unternehmen in Berlin
- Träger des »Hamburg Preis für Wirtschaftsinformatik«
- International Program Committee der »Information Resources Management Association« (IRMA), USA
- Gutachter der »International Sciences Conferences« (ISC - ITEE), Kanada

Mitgliedschaften:
- Transparency International (TI)
- Arbeitskreis für Unternehmenssicherheit Berlin-Brandenburg (AKUS)
- Gründungsmitglied der Hilfsorganisation *stars of tomorrow (SOT)

IHK AKUS

TRANSPARENCY INTERNATIONAL Deutschland e.V.

STARS OF TOMORROW

Kontakt:
- BHT Berlin, Fachbereich I, Luxemburger Str. 10, 13353 Berlin
- 030-4504-5247, 0163-16 444 61
- http://prof.beuth-hochschule.de/huber/
- a.huber@beuth-hochschule.de

Fotonachweis:
* Jörg Puchmüller, Wiesbaden
* http://www.everystockphoto.com
* Privat
* Beuth Hochschule für Technik Berlin
* ESV Verlag, Berlin

Wirtschaftsschutz
ist
Teamwork

BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Referat Wirtschaftsschutz
Merianstr. 100
50765 Köln
Telefon: 02 21 / 792 - 0
Fax: 02 21 / 792 - 29 15
E-Mail: wirtschaftsschutz@bfv.bund.de