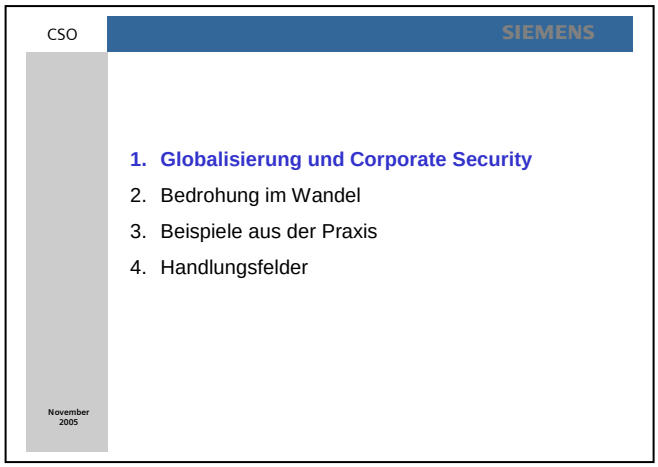
Norbert Wolf
Head of Corporate Security

03. November 2005

„Sicherheitskooperationen als weltweite Zweckbündnisse aus Sicht der Wirtschaft“



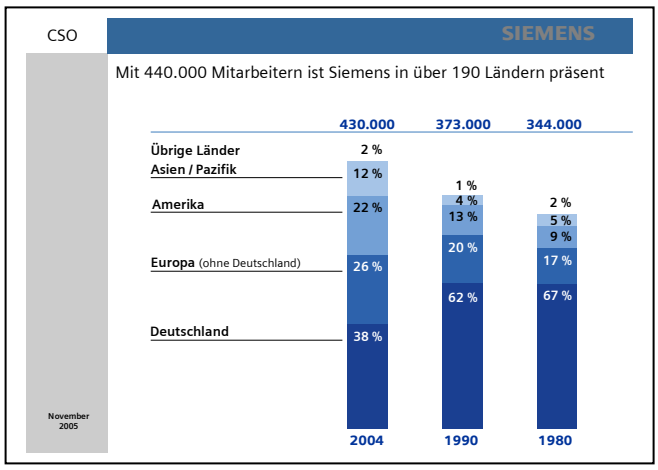
Ich kann hier natürlich nicht für die deutsche Wirtschaft sprechen. Jedoch bin ich Mitglied in zwei Arbeitskreisen der Sicherheitsverantwortlichen großer deutscher Unternehmen. Darin sind u.a. vertreten: die Deutsche Bank, Lufthansa, die Deutsche Telekom, BMW, die Deutsche Bahn, aber auch Konzerne mit nicht-deutschen Muttergesellschaften wie IBM oder Philips. Im Sinne von „Best Practice“ arbeiten wir erfolgreich zusammen.

Aufgrund meiner Tätigkeit als Vorsitzender des Ausschuss für Sicherheitsfragen beim Bundesverband der Deutschen Industrie, der Arbeit in einer Reihe von Wirtschaftsverbänden sowie mit ausländischen Global Playern habe ich einen guten Einblick in das Aufgabenspektrum und die Arbeitsweise der Security-Abteilungen anderer Unternehmen.

Sehr viele persönliche Erfahrungen habe ich in 10 Jahren im Vorstand des Verbandes der deutschen Wirtschaft in der Russischen Föderation (VdWRF) als

Leiter des Komitees für Sicherheit gesammelt. Der Verband hat fast 500 deutsche Firmen als Mitglieder, die auf Wunsch in allen Sicherheitsfragen beraten werden. Bereits das ist meiner Meinung nach ein gutes Beispiel für unser Thema, denn eine solche Aufgabe kann natürlich nur durch Kooperationen, Bündnisse und Netzwerke erfüllt werden.

Jedes Unternehmen hat unterschiedliche Gefahrenschwerpunkte und braucht daher eine eigene, den Bedürfnissen angepasste Security Policy. Und natürlich hat dies auch Einfluss auf die Anforderungen an internationale Zweckbündnisse, oder allgemein formuliert, Art und Umfang der globalen Sicherheitsvernetzung.



Unser 158 Jahre altes Unternehmen ist mit 440.000 Mitarbeitern – davon ca. 160.000 in Deutschland und 280.000 im Ausland – in über 190 Ländern präsent und damit immer auch in den besonders sicherheitskritischen Regionen tätig. 45.000 Mitarbeiter arbeiten allein in Forschung und Entwicklung.

Und wir sind stolz darauf, dass wir schon ein Global Player waren, bevor überhaupt jemand wusste, was dieser Terminus bedeutet. Nur die Fifa, der Vatikan oder Coca Cola sind globaler.

Siemens bietet ein umfangreiches Portfolio in sechs Arbeitsgebieten:

Das Spektrum reicht vom Transrapid bis zum Kfz-Bordsystem, von der Windkraftanlage bis zum Großkraftwerk, von der Produktionsanlagensteuerung für eine Joghurt-Fabrik bis zur IT-Dienstleistung und vom Verkehrsleitsystem bis zum Computertomographen, um nur einige Beispiele zu nennen.

Innerhalb dieses Spektrums bietet Siemens zahlreiche Sicherheitsprodukte und –lösungen an und tritt weltweit als Partner für Security auf:

Hier gibt es einen sehr klaren Markttrend: Heute werden ganzheitliche, integrierte Lösungen gefordert, die sowohl die physikalische Sicherheit als auch die IT-Sicherheit berücksichtigen. Die Zusammenführung beider Bereiche ist zunehmend entscheidend für den Erfolg eines Sicherheitsanbieters, und darin eben liegt eine Stärke von Siemens.

- So hat unser Unternehmen beispielsweise zusammen mit Boeing bereits 2002 den Auftrag zur Ausrüstung von 438 kommerziellen Flughäfen in den USA mit ***Systemen zur Erkennung von Sprengstoffspuren*** erhalten. Dies umfasste Lieferung und Inbetriebnahme von rund 6.000 Einzelsystemen und die Schulung von 30.000 Airport-Mitarbeitern.

- Bei den ***Olympische Spielen 2004*** in Athen war Siemens Systemlieferant für einen Großteil der Sicherheitssysteme, z.B. die Videoüberwachung am Flughafen und an öffentlichen Plätzen.

- Das ***Trusted Traveler-System*** zeigt, dass es durchaus möglich ist, zugleich den Komfort der Reisenden und das Sicherheitsniveau zu erhöhen: Es ermöglicht Passagieren, die ihren Fingerabdruck zuvor biometrisch haben erfassen lassen, schneller an Bord zu gelangen. Durch sichere Authentifizierung wird zugleich die Sicherheit an Bord verbessert. Der Praxistest wurde erfolgreich durchgeführt.

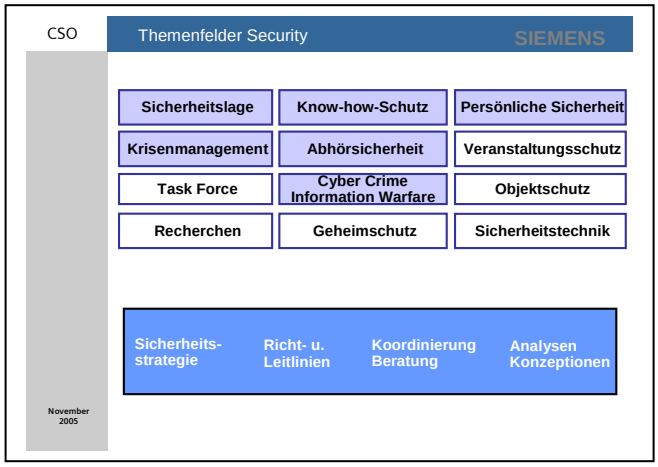
- Zunehmend kursieren gefälschte Arzneimittel auf dem Markt. Siemens hat Lösungen entwickelt, mit denen ***Medikamente eindeutig identifiziert*** und ***fälschungssicher*** gemacht werden können. Hier kooperieren wir mit Herstellern und Verpackungsfirmen gegen eine Form der Organisierten Kriminalität.

Dies sind nur einige Beispiele für erfolgreiche Kooperationen im Rahmen unserer sicherheitsrelevanten Produkte und Lösungen.

Mit unserer umfassenden geografischen Präsenz und multikulturellen Organisation wissen wir um die speziellen Herausforderungen des Umganges mit unterschiedlichen Kulturen. Niemand sollte diese kulturellen Unterschiede unterschätzen. Sicherheit ist kein universaler Standard, es hängt entscheidend davon ab, wo man sich befindet!

Wir glauben, dass nur solche Sicherheitsmaßnahmen und -vorgaben erfolgreich sind, die sich in die Firmenkultur einpassen und auch die regionalen Gegebenheiten berücksichtigen. Ohne Akzeptanz von Kunden, Besuchern und Mitarbeitern kann eine Unternehmenssicherheit keinen andauernden Erfolg haben.

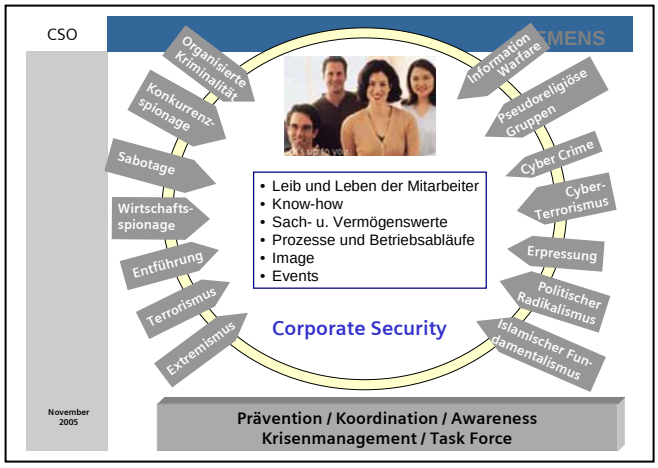
Die speziellen Aufgaben der Unternehmenssicherheit sind in meiner Abteilung, dem Corporate Security Office (CSO) zusammengefasst und umfassen folgende Themenfelder:



Diesen Themenfeldern widmen sich auch die Sicherheitsabteilungen anderer vergleichbarer Global Player.

2. Bedrohung im Wandel

Die folgende Übersicht zeigt das vielfältige Bedrohungsspektrum, dem auch globale Wirtschaftsunternehmen ausgesetzt sind:



Vor dem Hintergrund dieses Bedrohungsspektrums sind alle unsere Bemühungen darauf ausgerichtet, Gefahren abzuwehren für

- Leib und Leben
- Know-How
- Sach- und Vermögenswerte
- Prozesse und Betriebsabläufe
- Umwelt sowie das
- Image unseres Unternehmens

Unternehmenssicherheit darf nicht als Bremser, als Verhinderer erscheinen. Sie muss mitgehen mit den Unternehmenszielen, diese begleiten. Alle dazu notwendigen Maßnahmen müssen angemessen eingebracht werden. Sicherheit lebt von Akzeptanz!

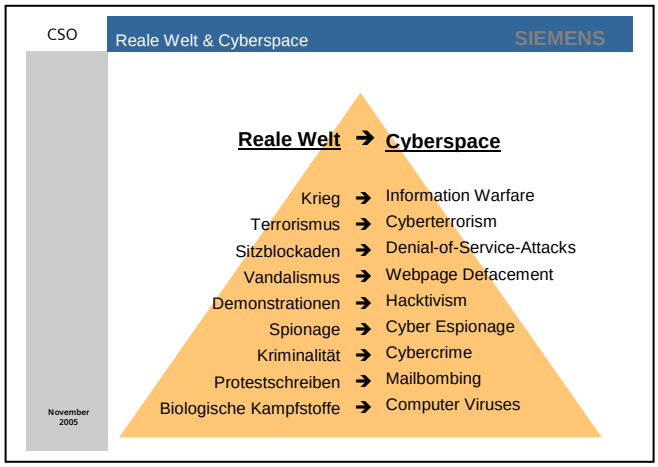
Moderne Unternehmenssicherheit versteht sich als Risikomanagement, das Sicherheitsaufgaben nicht mehr inselartig, sondern ganzheitlich als „integrale betriebliche Gefahrenabwehr“ durchführt. Dabei spielt das präventive und operative Krisenmanagement eine immer wichtigere Rolle.

Die Risikoszenarien durch Terrorismus, durch Wirtschaftsspionage, politischen und religiösen Radikalismus sowie Organisierte Kriminalität erfordern mehr denn je integrierte Lösungsansätze und Strategien auch in Unternehmen.

Der 11. September 2001 hat gezeigt, dass wir uns in der Sicherheit immer stärker auch auf vermeintlich unvorstellbare Szenarien einstellen müssen. Dabei rücken neben den bisher bekannten kriminellen und terroristischen

Vorgehensweisen „Cybercrime“ und „Information Warfare“ in den Fokus der Risikobetrachtungen.

Die technischen Voraussetzungen für derartige Angriffe sind gegeben; es ist daher möglicherweise nur eine Frage der Zeit, bis entsprechend motivierte Tätergruppen auch im „Cyberspace“ das enorme Potential erkennen und katastrophale Schäden gezielt herbeiführen.



Diese Darstellung soll verdeutlichen, dass sich alle klassischen Security-Themen auch in den Cyberspace ausbreiten. Der Cyberspace kennt aber bekanntlich keine Grenzen. Umso wichtiger sind zur Bekämpfung dieser Ausprägungsformen behörden- und länderübergreifende Kooperationen.

ShareNets und Wissens-Communities gehören heute zum Alltag in der Wirtschaft.

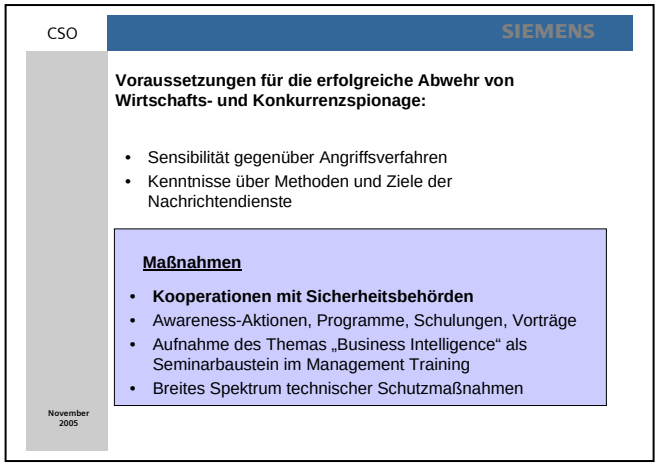
Wir nehmen die Themen Wirtschafts- und Konkurrenzspionage im Rahmen des Themenfeldes ***Business Intelligence*** sehr ernst. Jedoch müssen wir zugleich sorgfältig prüfen, wo und wie der Informationsfluss aus Sicherheitsgründen eingeschränkt werden muss. Jede Übertreibung würde den vitalen Know-how-Fluss existentiell beschneiden!

Und genauso könnte dadurch die Atmosphäre des Vertrauens beschädigt werden, die Voraussetzung für ein weltweites erfolgreiches Geschäft ist.

Wirtschaftsspionage und Konkurrenzspionage sind in den letzten Jahren zu einer massiven Bedrohung gerade für international tätige Unternehmen geworden.

Neben Wettbewerbern und so genannten Informationsbrokern sind Nachrichtendienste aktiv. Die Schwerpunkte ihrer Tätigkeit haben sich von der militärisch-politischen auf die wissenschaftlich-technische und vor allem wirtschaftliche Ebene verlagert.

„Es herrscht Wirtschaftskrieg. In dieser Schlacht dienen Informationen und Desinformationen als Waffe“, sagte Benoit de Saint-Sernin, einer der Gründungsväter der „Ecole de guerre economique“ in Paris, die im Oktober 1997 eröffnet wurde. „Wir lehren, wie sich Firmen gegen solche Angriffe schützen können.“



3. Beispiele aus der Praxis

In großen global tätigen Unternehmen müssen die Herausforderungen zum Thema Sicherheit auf Managementebene innerhalb übergreifender Gremien bewältigt werden. Wir haben bereits vor einigen Jahren ein so genanntes Security Council ins Leben gerufen, in dem z.B. Unternehmenssicherheit, Rechtsabteilung, Unternehmenskommunikation, IT, die Personalabteilung sowie Bereiche und Regionalgesellschaften vertreten sind.

Voraussetzung für eine positive Entwicklung unseres Geschäfts ist der Erfolg in einem globalen Markt und Erfolg gegen globale Konkurrenz. Globalisierung bedeutet für ein Wirtschaftsunternehmen, Wegfall von Zollschranken, Deregulierung, eine umfassende Öffnung der nationalen Märkte und deren Zusammenwachsen zu einem Weltmarkt.

Die Märkte haben sich dramatisch verändert. Mega-Fusionen, Privatisierung im Osten, Wirtschaftsmärkte wie NAFTA, Mercosur sind nur einige Stichworte. Dieses globale Umfeld setzt uns heute mehr unter Druck als je zuvor. Bei Siemens heißt das: Jeden Tag brauchen wir rund 350 Millionen Euro Auftragseingang, um unsere 440.000 Mitarbeiterinnen und Mitarbeiter in Arbeit und Brot halten zu können. Und wir brauchen Erfolg überall auf der Welt. 80% der Geschäfte von Siemens finden im Ausland statt, nur noch 20% in Deutschland. Bei jeder unternehmerischen Entscheidung bewegen wir uns in einem komplizierten Interessensgeflecht von Kunden, Lieferanten, Subunternehmen, Aktionären, Mitarbeitern und auch Regierungen – und das weltweit. Auch dies belegt die Unabdingbarkeit umfassender Kooperationen.

Wir haben nach dem 11.09.2001 weltweit die Sicherheitskonzepte unserer Objekte, Projekte, Produktions- und Entwicklungsstandorte überprüft und wo nötig angepasst. Dabei wurden auch unsere Lieferanten mit einbezogen, insbesondere wenn es sich um so genannte ***Single-Source-Lieferanten*** handelt bzw. wo wir stark abhängig von einem einzigen Zulieferer sind.

Auch hier bilden wir Zweckbündnisse, indem wir diese Geschäftspartner in die Sicherheitskette einbinden und auch von ihnen angemessene Sicherheitsmaßnahmen verlangen.

Das oberste Ziel eines jeden Wirtschaftsunternehmens ist, erfolgreiche Geschäfte zu tätigen. Da aber das Business dem Markt folgen muss, tun wir dies auch zunehmend in Ländern und Regionen mit instabiler Sicherheitslage.

Die Verlegung von Kabeln in Ägypten, die Metro in Medellin (Kolumbien), der Bau von Stromleitungen in Nigeria, die Errichtung eines Kraftwerks in Pakistan oder die Aufstellung von GSM-Masten in Algerien – sicherheitskritischen Gebieten können unsere Mitarbeiter oft nicht ausweichen und trotz vieler Sicherheitsmaßnahmen bleibt ein nicht unerhebliches Restrisiko für Leib und Leben.

Unser ehemaliger CEO und jetziger Vorsitzender des Aufsichtsrats Herr Dr. von Pierer, drückte dies im April 2004 in seinem Vortrag vor dem Sicherheitsrat der Vereinten Nationen in New York, wo er als erster und einziger Wirtschaftsvertreter sprach, so aus:

„In kritischen Regionen folgt das Geschäft einigen grundsätzlichen Regeln. Dazu gehört zum Beispiel die starke Abstützung auf lokale Mitarbeiter, denn diese kennen ihr Land, ihre Kultur und die lokalen Gegebenheiten am besten. Und wir brauchen einige sog. Expatriates [d.h. entsandte Mitarbeiter, Anm. des Verf.] um die Prozesse anzustoßen. Unser Grundprinzip an dieser Stelle ist, Mitarbeiter nur auf freiwilliger Basis zu entsenden. Diese Leute werden sehr sorgsam und unter Berücksichtigung aller religiösen, ethnischen und kulturellen Faktoren ausgewählt – und sie müssen nicht zwingend aus Deutschland kommen. Die enge Sicherheitskooperation mit lokalen Behörden ist eine Grundvoraussetzung für alle Aktivitäten. Vor allem braucht man aber gesunden Menschenverstand, Vorsicht und Besonnenheit, aber auch Mut. Leider reichen diese Regeln nicht immer aus. Wenn das Risiko zu groß wird, müssen wir uns manchmal auch zurückziehen. Nur so lange wie nötig, möchte ich ergänzen. Denn unsere grundlegende Philosophie ist: Wir sind hier um zu bleiben.“[We are here to stay]

Aber wann ist das Risiko zu groß? Wann ist der Zeitpunkt eines Rückzuges aus einem Land oder einer Region gekommen? Grundlage ist ein sauberes, lokal differenziertes und permanent aktualisiertes **Lagebild**. Bei der Beschaffung der dafür benötigten Informationen können uns zum einen unsere eigene weltweite Security-Organisation, zum anderen aber Kooperationen mit Behörden, befreundeten Unternehmen, Verbänden und Consultants helfen. Die Interpretation und die Ableitung notwendiger Sicherheitsmaßnahmen von Reisebeschränkungen bis zur Evakuierung ist aber Aufgabe des jeweiligen Unternehmens.

Lassen Sie mich die Komplexität dieser Aufgabe anhand der Beispiele ***Afghanistan***, ***Irak*** und ***Saudi-Arabien*** erläutern.

Seit den 20er Jahren ist Siemens in Afghanistan tätig. Unsere Präsenz wurde durch den Krieg dort unterbrochen. Nach dem Ende des Krieges hatte die Wiederversorgung des Landes mit Wasser, Energie und Kommunikation oberste Priorität. Z.B. erhielt Siemens den Auftrag, zwei Wasserkraftwerke zu restaurieren, die wir vor mehr als 50 Jahren gebaut hatten. Wir holten einfach die Original-Konstruktionspläne aus unserem Archiv und konnten sofort mit der Arbeit beginnen. Langjährige Kooperationen und tragfähige Bündnisse überstehen auch solche kritischen Zeiten.

Allerdings müssen für die deutschen und lokalen Ingenieure detaillierte Schutzmaßnahmen durchgeführt werden.

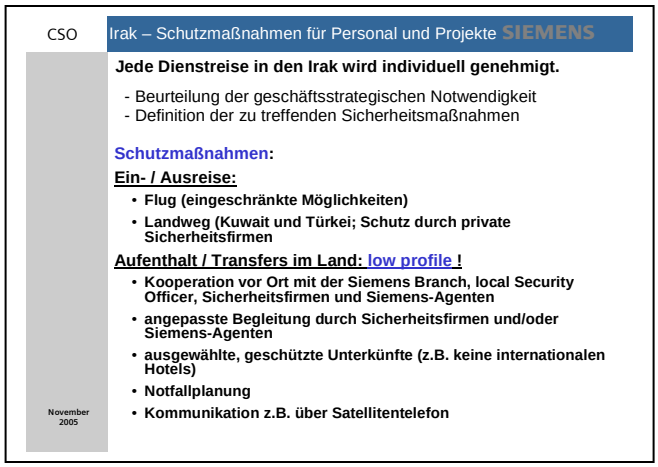
Als ich vor 6 Wochen mit dem Leiter unserer Landesgesellschaft in ***Afghanistan***, der fließend Paschto, Farsi, Deutsch und Englisch spricht, im Lande unterwegs war, konnte ich mich erneut davon überzeugen, wie wichtig für die Sicherheit unserer Mitarbeiter der Kontakt zu regionalen Stammesfürsten ist.

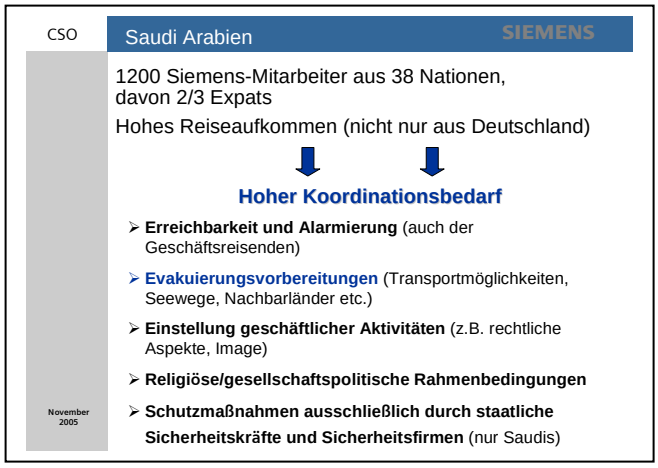
Im ***Irak*** helfen wir mit verschiedenen Projekten die Energieversorgung und die Kommunikation trotz der hohen Sicherheitsrisiken zu verbessern.

Wir führen dort und in anderen Ländern mit besonderen Risiken Sicherheitsanalysen und gezielte Beratungen mit Maßnahmenempfehlungen für

unsere Mitarbeiter und Projekte durch. Dabei hüten wir uns davor, deutsche Einstellungen zur Sicherheit sowie Taktiken und Techniken einfach zu übertragen, sondern tragen flexibel der Situation im Land Rechnung.

Dies fängt an bei der Qualität des Bewachungspersonals, geht weiter mit der Zuverlässigkeit und Berechenbarkeit von Sicherheitsbehörden und endet nicht zuletzt bei sehr unterschiedlichen Auffassungen und Einstellungen der Mitarbeiter und Führungskräfte zur Sicherheit.





Zunehmend rücken auch medizinische Themen wie Pandemien in den Fokus von Sicherheitskooperationen. Im Jahr 2003 war es das Thema SARS, derzeit ist es die Vogelgrippe. Maßnahmen im Vorfeld und bei Ausbruch solcher Erkrankungen bedürfen der Kooperation zwischen nationalen und internationalen Gesundheitsbehörden (z.B. RKI, WHO), Sicherheitsbehörden, den medizinischen Dienststellen von Unternehmen und ihren Krisenmanagementteams.

Für rein ***medizinische Notfälle*** haben wir Kooperationsabkommen mit verschiedenen Institutionen.

Wie kompliziert und brisant die Lage aus der ***Rechtssituation*** heraus sein kann zeigt folgendes Beispiel:

Auf einer Baustelle in Thailand arbeiten Siemens Mitarbeiter aus den USA, aus Deutschland und anderen europäischen Ländern sowie lokale Arbeitskräfte. Aufgrund einer nicht näher spezifizierten Bedrohung erlässt das US State Department eine Reisewarnung; die Australische Botschaft reagiert ähnlich, andere ausländische Vertretungen ermahnen lediglich zu verstärkter Aufmerksamkeit. Daraufhin verlassen die Mitarbeiter mit US-Staatsbürgerschaft die Baustelle, die anderen Nationalitäten bleiben zurück.

Wir können uns in solchen Fällen nicht allein auf die Lageeinschätzung des Auswärtigen Amtes verlassen. Wenn z.B. das Auswärtige Amt und das US State Department zu einer unterschiedlichen Beurteilung der Sicherheitslage kommen,

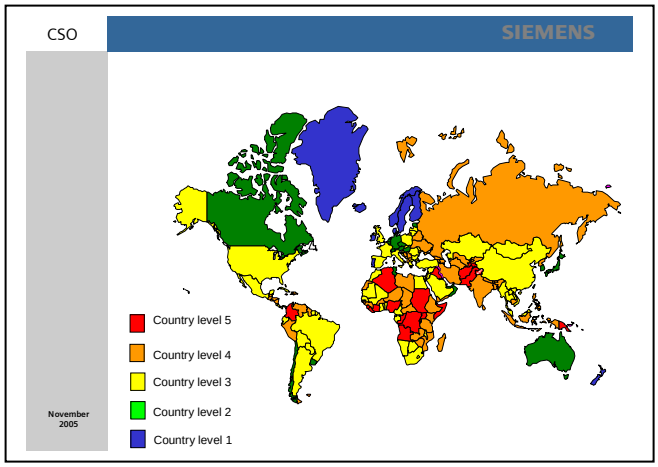
müssen wir dies bei anstehenden Entscheidungen wie z.B. Evakuierungen berücksichtigen. Auch dieses Beispiel belegt, wie wichtig Kooperationen, so z.B. auch mit international erfahrenen Rechtsberatern und Juristen, sind.

Eines unserer wichtigsten Ziele muss sein, sicherheitsrelevante Entwicklungen rechtzeitig zu identifizieren, die sich daraus ergebenden Trends und Probleme frühzeitig zu erkennen sowie notwendigen Handlungsbedarf abzuleiten. Ich glaube, darin stimmen wir alle überein.

Diese Herausforderung ist aber nur durch den sorgsamen, arbeits- und zeitintensiven Aufbau sowie die Pflege eines globalen Sicherheitsnetzwerkes zu bewältigen. Wichtigste Grundvoraussetzung sind Kooperationen mit Sicherheitsbehörden, den Verbänden und der Politik. Wir benötigen aber darüber hinaus in aller Regel auch vertrauenswürdige und professionelle Sicherheitsagenturen und Consultants, ohne die wir unsere Arbeit nicht machen könnten.

Aber es gibt auch schwarze Schafe in dieser Branche. Es ist z.B. äußerst unseriös, wenn eine international tätige Sicherheitsagentur westliche Firmen und Bürger vor dem Risiko von Entführungen in Moskau warnt und behauptet, dass es dort in einem Jahr 87 Entführungen gegeben habe. Bei genauem Hinsehen stellt man fest, dass unter den Entführten kein einziger Westeuropäer war.

Wenn andere Consultants in ihrer Risikoeinschätzung ganze Länder in grob vereinfachter Form in einer Farbe darstellen, dann kann das für uns sicherlich keine geeignete Arbeitsgrundlage sein.



Für ein präziseres Lagebild brauchen wir dringend die Unterstützung der Sicherheitsbehörden.

Oft ist es in der Praxis aber nicht so, dass wir zunächst in jedem Land ein engmaschiges Security-Netzwerk aufbauen, und dann im Bedarfsfall darauf zurückgreifen können. Netzwerke wachsen und die Keimzelle ist allzu oft ein Sicherheitsvorfall.

Ein Beispiel: Wir hatten vor mehr als 13 Jahren in Russland eine massive Schutzgelderpressung gegen unsere dortige Niederlassung. Nur durch lokale, vertrauliche Kontakte konnten wir diesen Fall lösen. Dies war mit Auslöser für mein bis heute andauerndes Engagement im Verband der Deutschen Wirtschaft in der Russischen Föderation.

Sicherheitskooperationen machen nur Sinn, wenn letztendlich alle Beteiligten einen Nutzen daraus ziehen können. Ein gutes Beispiel dafür auf internationaler Ebene ist die Customs-Trade Partnership Against Terrorism (C-TPAT), eine Initiative der US-Zollbehörden nach den Terroranschlägen in den USA vom 11.09.2001. Ziel ist der Schutz der USA vor Spreng- oder Giftstoffen, die z.B. in See-Containern ins Land kommen könnten. Firmen, die an diesem Programm teilnehmen wollen, müssen einen klar definierten weltweiten sicherheitlichen Standard hinsichtlich ihrer Sicherheitsorganisation und den Schutzmaßnahmen an ihren Standorten nachweisen und garantieren. Die Container dieser Firmen werden bereits vor dem Verladen z.B. im Hamburger Hafen vom US-Zoll

kontrolliert und freigegeben, wodurch sich der Abfertigungsprozess erheblich verkürzt. Durch diese Sicherheitskooperation sparen Firmen Zeit und Geld und für die USA ergibt sich ein Sicherheitsgewinn.

Siemens ist als einer der ersten Teilnehmer diesem Programm beigetreten.

4. Handlungsfelder

Vor einiger Zeit hat ein leitender Mitarbeiter einer deutschen Sicherheitsbehörde die Situation so beschrieben:

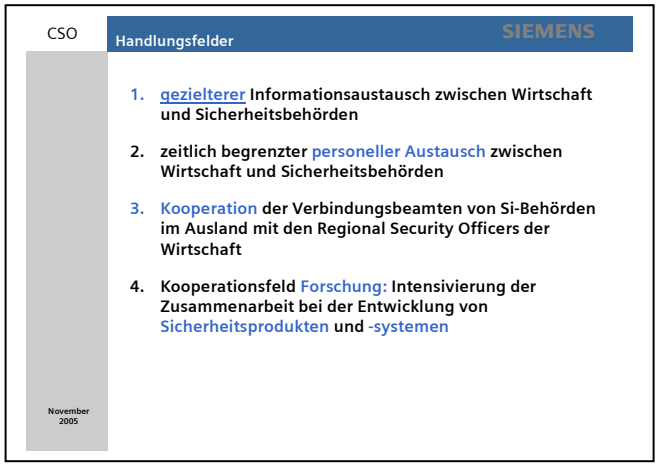
„Die Sicherheitspartnerschaft Staat – Wirtschaft ist noch weitgehend auf unbürokratische Kooperation, pragmatische Improvisation und juristische Hilfskonstruktionen angewiesen, statt auf klare gesetzliche Regeln gegründet zu sein!“

Schon auf Deutschland bezogen wissen wir alle, wie schwer es ist, dies zu ändern. Umso schwieriger fällt eine Übertragung auf eine europäische oder gar globale Ebene.

Die gegenwärtigen ***Public-Private-Partnership-Aktivitäten*** der verschiedenen Landes- und Bundesbehörden sowie von Verbänden [Beispiele: ASW, Sicherheitsausschuss des BDI, KRITIS, Sicherheitsforen in Baden-Württemberg und Bayern] sind ein wichtiger Schritt in die richtige Richtung. Vor allem im Zusammenhang mit der Privatisierung und dem Schutz kritischer Infrastrukturbereiche wie z.B. Telekommunikation, Energie und Verkehr ist die enge Zusammenarbeit zwischen Staat und Wirtschaft unerlässlich.

Ein Beispiel dafür ist die Neufassung des Sicherheitsüberprüfungsgesetzes (SÜG), die es Unternehmen erlaubt, sicherheitskritische Bereiche zu definieren und dort tätige Mitarbeiter behördlich überprüfen zu lassen. Jedoch hat sich auch hier gezeigt, wie schwierig es ist, den unterschiedlichen Erwartungen und Bedürfnisse der betroffenen Unternehmen durch gesetzliche Regelungen gerecht zu werden.

Abschließend möchte ich einige Beispiele für mögliche Felder nennen, auf denen die Zusammenarbeit zwischen Staat und Wirtschaft intensiviert werden sollte:



Punkt 1: Ich könnte ich mir vorstellen, dass behördlicherseits vermehrt ***konkrete***, auf das jeweilige Unternehmen bezogene Aussagen über die aktuelle Bedrohung z.B. durch Wirtschaftsspionage, Organisierte Kriminalität und Terrorismus zur Verfügung gestellt werden.

Es ist ja nicht so, dass wir immer an einem Mangel an sicherheitlich relevanten Informationen leiden; die ***Verifizierung*** wird oft zu einem Hauptproblem. Umso wichtiger scheint es mir, geeignete Zweckbündnisse zu etablieren, die uns bei diesem Prozess arbeitsteilig entlasten. Wir müssen die unterschiedlichen beschriebenen privatwirtschaftlichen und staatlichen Netzwerke – wo immer möglich - zusammenführen.

Punkt 2: Vertrauensvolle Zusammenarbeit erfordert in erster Linie mehr Verständnis füreinander und Wissen voneinander, nämlich über Ziele, Aufgaben, Strukturen und Arbeitsweisen.

Dazu beitragen könnte der ***zeitlich begrenzte personelle Austausch*** zwischen Industrie und Sicherheitsbehörden. Dies ist in vielen Ländern bereits gelebte Praxis.

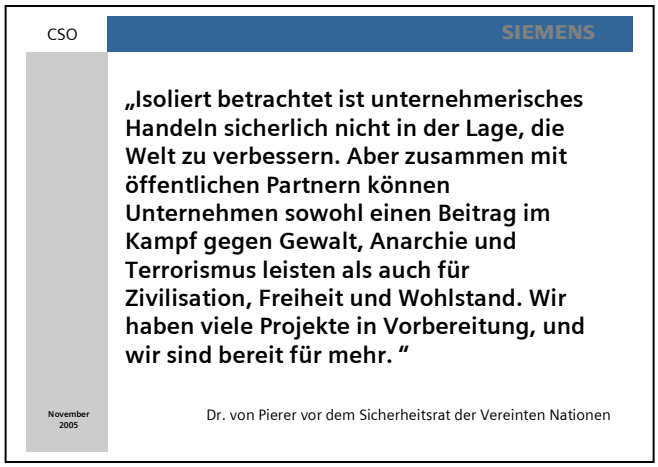
Punkt 3: Aus meiner Sicht sollten die Zusammenarbeit und der ***Informationsaustausch mit den Verbindungsbeamten*** der deutschen Sicherheitsbehörden im Ausland begonnen bzw. erheblich intensiviert werden.

Siemens hat in fast allen sicherheitskritischen Ländern professionelle Sicherheitschefs eingestellt, ob in USA, Irak, Saudi-Arabien oder Indonesien, die ihr jeweiliges lokales Netzwerk haben, die uns mit aktuellen Informationen zur Lage versorgen und bei der Lösung schwerwiegender Probleme (wie z.B. Entführungen) helfen. Ich könnte mir vorstellen, dass von diesem Netzwerk auch deutsche Sicherheitsbehörden profitieren können.

Punkt 4: Bei der Entwicklung von Sicherheitsprodukten und –systemen arbeiten die Behörden mit den entsprechenden Anbietern eng zusammen. Gerade im Bereich der Forschung und Entwicklung aber könnte die Wirtschaft aufgrund des breiten Know-how meines Erachtens einen noch intensiveren Beitrag leisten, um die Sicherheitsbehörden bei der Verbrechensverhütung und Terrorismusbekämpfung zu unterstützen.

Ich hoffe, Ihnen mit meinem Vortrag ein besseres Verständnis für die Vielfalt und Komplexität der Anforderungen an Sicherheitskooperationen aus Sicht eines global agierenden Unternehmens vermittelt zu haben. Die in diesem Zusammenhang bestehenden Interessenskonflikte, Interdependenzen und rechtlichen Rahmenbedingungen dürfen uns nicht davon abhalten, alle Anstrengungen zu unternehmen, bestehende Kooperationen zu intensivieren und dabei auch neue Wege zu gehen.

Schließen möchte ich mit diesem Zitat des Herrn Dr. von Pierer:



Norbert Wolf
Head of Corporate Security
Siemens AG
Tel.: + 49 89 636 - 34220
Fax: + 49 89 636 – 33505
norbertwolf@siemens.com