Die Security-Funktion...

Die Security-Funktion in einem globalagierenden Konzern am Beispiel der BASF-Gruppe
Von Dieter K. Sack M.A., Vice President, Leiter Corporate Security BASF-Gruppe

Dieter K. Sack M.A. Vice President Leiter Corporate Security BASF-Gruppe

Es dürfte weltweit kaum ein nennenswertes aktuelles Securityereignis oder eine Securitylage (langfristig) geben, wovon die BASF nicht in irgendeiner Weise betroffen ist.

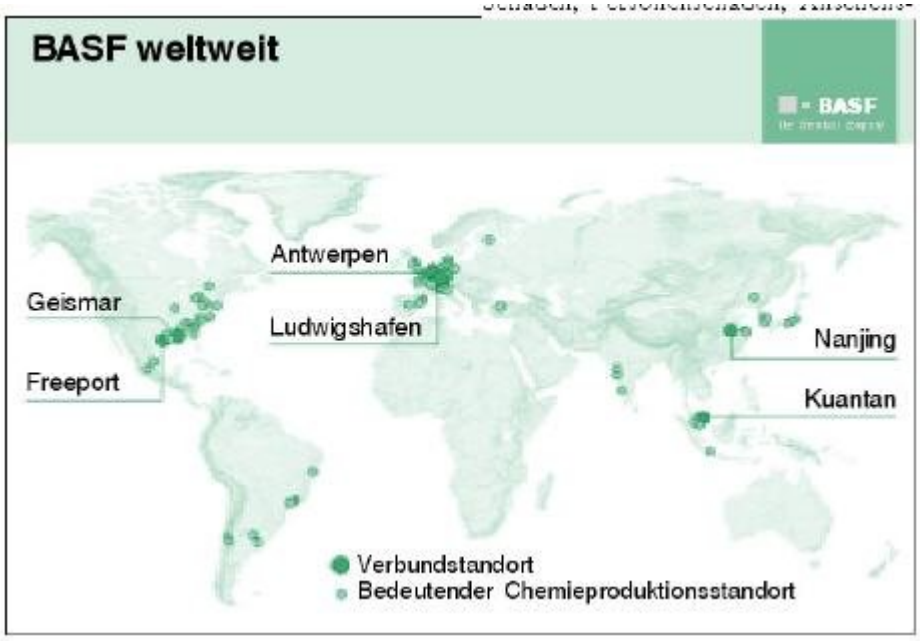
Dies gilt sowohl für die **allgemeine Kriminalität** (Eigentumsdelikte, Betrug/Unterschlagung) als auch für die **organisierte Kriminalität** wie(Schutzgeld-) Erpressung, Entführung, Produktfälschungen (Medikamente, Ersatzteile, Markenprodukte) oder Transportdiebstahl. Hinzu kommen Gefahren durch den **militanten Extremismus** (Angriffe auf Repräsentanten des Unternehmens, Störung von Firmen-Veranstaltungen) und den **(islamistischen) Terrorismus,** bei dessen (Bomben-) Anschlägen auf Transportmittel, Infrastruktur und Objekte mit symbolischer Bedeutung (Regierungsgebäude, Wirtschaftszentrum, religiöse Einrichtung) auch Mitarbeiter (Ortskraft, Delegierte, Reisende) Zufallsopfer eines Anschlages werden können.
Ein weiteresRisiko stellen der **Informations- und Know-how-Verlust** dar, sei es durch Wirtschaftsspionage, Patentverletzungen oder Angriffe auf Netzwerke und Rechner durch Hacker und Viren.
Und schließlich erfordern **politische Unruhen, Bürgerkrieg, Krieg** die Evakuierung des Firmenpersonals aus der Unruheregion.
Besonders kritisch wird die Situation immer dann, wenn zu einer hohen Kriminalitätsbelastung in einem bestimmten Land auch noch eine allgemeine **Rechtsunsicherheit** und/oder eine weitgehende Unfähigkeit/Korruption der Sicherheitsbehörden kommt. So gibt es eine Reihe von Ländern in Mittel- und Südamerika oder Schwarzafrika, wo es nach einem Raubüberfall oder einer Entführung wenig Sinn macht (oder sogar gefährlich ist), die Polizei zu kontaktieren, da die Polizisten selbst häufig in diese Straftaten verwickelt sind.
Bei der Betrachtung der gerade dargestellten Risiken kommen wir zu meiner zweiten Arbeitshypothese:

Der Globalisierung der Wirtschaft ist die Globalisierung der Kriminalität gefolgt. Was bisher nicht erfolgte, ist eine Globalisierung staatlicher Sicherheitsstrukturen.

Es gibt keine Weltpolizei, noch nicht einmal eine europäische. EUROPOL mag ein Anfang sein, aber bis zu einer wirklichen europäischen Polizei mit exekutiven Befugnissen im gesamten EU-Raum ist es noch ein weiter Weg.
Und dies gilt auch auf internationaler Ebene: An wen soll sich ein Unternehmen wenden, dessen Rechenzentrum in Deutschland von einem Virus attackiert wurde, der über einen Netzserver aus den USA kam und vermutlich in Südostasien geschrieben wurde? Stellen Sie sich die Situation vor, Sie würden bei Ihrer zuständigen lokalen Polizeidienststelle eine entsprechende Anzeige aufgeben wollen!
Damit komme ich zu meiner dritten These:

Da weder europäische noch globale staatliche Securitystrukturen vorhanden sind, müssen sich die international agierenden Unternehmen selbst helfen.

So wie sie auf ihren Werksgeländen auch schon immer selbst für ihre Sicherheit sorgen (Werkschutz), werden sie es auch auf absehbare Zeit global tun müssen. Dabei muss, wie auf dem Werksgelände, der Schwerpunkt auf der Prävention liegen, also der Verhinderung des Eintritts eines Schadens (wirtschaftlicher Schaden, Personenschaden, Ansehensverlust). Auch Weltunternehmen können nicht Weltpolizei spielen!



Global agierende Konzerne brauchen eine Corporate Security

International agierende Unternehmen müssen deshalb eine schlagkräftige und global aufgestellte Securityfunktion (Corporate Security) aufbauen und unterhalten. Sie ist Teil des unternehmensinternen Risikomanagements. Risiken aus Securitygründen sind genauso zu bewerten wie beispielsweise Finanzrisiken. Von den verantwortlichen Führungskräften der Corporate Security muss sowohl ein professioneller Hintergrund (Ausbildung und Berufserfahrung) als auch die intime Kenntnis des Konzerns erwartet werden.

Die BASF hat bereits Mitte der neunziger Jahre das Konzept einer „Corporate Security" im Konzern realisiert. 2001 kamen dann Aufgaben im Rahmen des globalen Informations- und Know-how-Schutzes hinzu.

Eine solche Aufgabenstellung lässt sich natürlich nicht allein von einer Abteilung Security in der Unternehmenszentrale bewältigen. Deshalb gibt es an jedem größeren Standort einen Security-Verantwortlichen (häufig der Leiter des örtlichen Werkschutzes). Er ist für die „klassischen" Aufgaben der Standort-Security zuständig (Torkontrollen, Streifendienst, physische Absicherung des Standortes durch Zäune, Zutrittskontrollanlagen). Er berichtet fachlich dem Leiter der regionalen Security („Region" meist identisch mit einem Erdteil), dieser wiederum der zentralen „Corporate Security". Damit ist sichergestellt, dass auch die Erfahrungen und vor allem die kulturellen und vielleicht auch rechtlichen Unterschiede in den einzelnen Regionen und an den vielen Standorten der Unternehmensgruppe in Entscheidungen der Security einfließen. Umgekehrt wird über dieses Netzwerk die Einhaltung von zentralen Vorgaben der Corporate Security („Richtlinienkompetenz") sichergestellt.

Der Verantwortungsbereich einer „Corporate Security" in allen Großkonzernen – auch in der BASF-Gruppe – umfasst im Wesentlichen folgende Aufgabenstellungen:

Informationsgewinnung, Lagedarstellung, Securityberatung

Zentrale Aufgabe der Corporate Security ist die Informationsgewinnung und Auswertung. Sie muss permanent und sie muss global erfolgen. Auch hier lassen sich natürlich Teile zukaufen.

Die Informationsbewertung ist Basis jeder Risikoeinschätzung und damit jeder Prävention. Dies gilt sowohl für langfristige Entwicklungen als auch für aktuelle Situationen.

Bei dieser Sammlung und vor allem der Bewertung securityrelevanter Informationen sind die Unternehmen in hohem Maße auf die Mitwirkung der staatlichen Sicherheitsbehörden angewiesen. Hier hat in den letzten Jahren – wenn auch noch zögernd – unter dem Schlagwort der „Public-Private-Partnership" ein Bewusstseinswandel eingesetzt. Sowohl auf Bundesebene, als auch in mehreren Bundesländern (z.B. Hessen und Rheinland-Pfalz), gibt es mittlerweile schriftlich fixierte „Sicherheitspartnerschaften" zwischen den jeweils zuständigen Bundes- bzw. Landesbehörden und den Spitzenverbänden der privaten Sicherheit.

Die gesammelten und bewerteten Informationen werden zu Risiko-Lagebildern verdichtet, die sich sowohl auf bestimmte Phänomene (z.B. Terrorismus) als auch auf einzelne Regionen (z.B. Lagebild Sicherheit Nahost) beziehen können. Sie werden dem Management zur Verfügung gestellt. Auch die Beratung von Mitarbeitern, die für einige Jahre als Delegierte ins Ausland gehen, oder von Reisenden in Krisenregionen, erfolgt durch Corporate Security auf Basis dieser Lagebilder.

Security-Audits

Eine wichtige Informationsquelle für Corporate Security sind auch die (regelmäßig) durchzuführenden Security-Audits an den (zumindest größeren) Standorten der Unternehmensgruppe. Sie sind Ausfluss der oben bereits erwähnten steuernden Funktion mit Richtlinienkompetenz (neudeutsch „Governance Function") von Corporate Security. Sie dient in erster Linie der Vermeidung von Doppelarbeit (Know-how-Transfer) und der Herstellung eines einheitlichen Schutzniveaus (nicht: Schutzstandards!) an allen Standorten. Dabei gelten neben dem Grundsatz „so wenig Zentralismus wie möglich" vor allem auch die Prinzipien der Angemessenheit und der Wirtschaftlichkeit!

Informations- und Know-how-Schutz
Nicht mehr die klassischen Produktionsfaktoren Arbeit, Kapital und Boden bestimmen heute in erste Linie den wirtschaftlichen Erfolg eines Unternehmens, sondern Informationen und Wissen. Diese Informationen sollen möglichst allen Berechtigten im Unternehmen (aber nur denen!) jederzeit und auf globalen Netzwerken, überall auf der Welt, vollständig und unverfälscht, zur Verfügung stehen.
Um dies sicherzustellen, bedarf es eines integrierten Informationsschutzkonzeptes für die gesamte Unternehmung. Neben einer Fülle von zumeist technischen und software-basierten Maßnahmen, für die in erster Linie die EDV-Abteilung zuständig ist, muss sich Corporate Security zentral um die Umsetzung des Gesamtkonzeptes in der Unternehmensgruppe kümmern, zumal es auch eine Fülle von Informationen außerhalb der EDV-Systeme gibt. Besonders wichtig ist es, das Thema Informationsschutz auch in den Köpfen aller Mitarbeiter zu verankern, denn ohne das richtige Bewusstsein bei den Mitarbeitern bleiben alle technischen Vorkehrungen nur Stückwerk.

Personen- und Veranstaltungsschutz
Auch wenn die Situation für die persönliche Sicherheit von Führungskräften der Wirtschaft heute deutlich entspannter ist als in den 70er und 80er Jahren, unterliegen sie als „Symbolfiguren“ auch weiterhin einer Gefährdung. Erwähnt seien die aktuellen Anschläge extremistischer Gruppen mit Schwerpunkt Norddeutschland und Berlin auf Wohnhäuser und Fahrzeuge von Managern, die Aktionen militanter „Tierschützer“ oder mögliche Attentate verwirrter Einzeltäter (wie gegen Lafontaine und Schäuble). Hinzu kommen die zahlreichen Auslandsreisen der Führungskräfte.
Deshalb unterhalten alle großen Unternehmen eigene Personenschutzgruppen. Diesen obliegt auch häufig der Schutz von größeren Veranstaltungen des Unternehmens im In- und Ausland (z.B. die jährliche Aktionärshauptversammlung oder internationale Treffen der Führungskräfte), zumal ihre Schutzpersonen meist ohnehin anwesend sind.

Kontakt zu (Sicherheits-) Behörden
Den Kontakt zu den obersten (Sicherheits-) Behörden des Landes und des Bundes zu halten, ist ebenfalls eine Aufgabe von Corporate Security. Das gilt auch für Behörden und Institutionen auf Ebene der EU oder bei globalen Organisationen, die sich mit securityrelevanten Fragestellungen beschäftigen. Gerade die Fülle von „Initiativen“ und Regelungen, die in der Folge der Anschläge vom 9. September 2001 von den USA, aber auch von anderen supranationalen Organisationen „erlassen“ wurden, und die fast alle Security-Charakter haben, macht ein Agieren von Corporate Security auch auf der politischen Bühne unerlässlich.

Aus dem dargestellten Verantwortungsbereich dürfte deutlich geworden sein, dass die zentralen Aufgaben der Corporate Security vom Unternehmen selbst wahrgenommen werden müssen. Dies schließt den Einsatz von externen Beratungsfirmen oder Wachunternehmen für bestimmte Teilaufgaben oder in aktuellen Fällen keineswegs aus.

Für alle Aktivitäten von Corporate Security gilt, dass sie wirtschaftlich vertretbar sein müssen. Oder umgekehrt: Sie müssen zum langfristigen wirtschaftlichen Erfolg des Unternehmens beitragen. Die Corporate Security-Abteilungen in den Unternehmen leisten so auch ihren Teil zum Erhalt von Hunderttausenden von Arbeitsplätzen in unserem Land.