Der Umgang mit den Bedrohungen entlang der Supply Chain

2

Osama bin Laden bestätigt, dass die Weltwirtschaft vorrangiges Ziel von Anschlägen ist. Kernfrage ist daher: Wie kann dieses Risiko minimiert werden? Zur Beantwortung der Frage ist erforderlich, die einzelnen Komponenten der Supply Chain in Bezug auf mögliche Schwachstellen und Sicherheitsvorkehrungen zu analysieren. Beispiel Seeschifffahrt: Rund 90 % des globalen Handels und Warenverkehrs wird über die Weltmeere abgewickelt. Dort sind die globalen Warenströme am verwundbarsten. Dies haben auch die Terroristen erkannt: Schon vor dem Aufstieg von *al-Qaida* haben Gruppierungen wie die *Tamil Tigers* aus Sri Lanka oder die proiranische Terrorgruppe *Hisbollah* maritime Terroroperationen durchgeführt [45].

Die Achillesferse der „ökonomischen Lebenslinien" – wie bin Laden die Lieferkette bezeichnete – ist die Versorgung der Weltwirtschaft mit Öl. 80 % wird durch den Suez-Kanal und über die Straßen von Hormus und Malakka transportiert [46]. Daher verwundert der Angriff auf den französischen Öltanker Limbourg im Golf von Aden im Oktober 2002 wenig. Einen Monat nach dem Angriff wird der Terrorist Abd al-Nasheri, *al-Qaida*-Spezialist für maritime Operationen, von amerikanischen Fahndern gefasst. Er soll während der anschließenden Verhöre zahlreiche Pläne von Anschlägen auf die maritime Wirtschaft enthüllt haben. Zudem soll nach seiner Aussage ein spezielles Handbuch für Anschläge auf See existieren, das detailliert auf die Umsetzung und die ökonomischen Folgen eingeht [47].

Besonders anfällig in Bezug auf die Supply Chain ist das Just-in-Time-Konzept, das weitgehend auf die Bevorratung zeitkritischer Teile am Ort der Produktion verzichtet. Dies bringt den Unternehmen – die reibungslos funktionierende Supply Chain vorausgesetzt – erhebliche Kostenvorteile. Gleichzeitig macht allerdings dieses Konzept die Wertkette auch störanfälliger, da die reibungslose

© Springer Fachmedien Wiesbaden 2017

W. Lehmacher, *Steht unsere Versorgung auf dem Spiel?,* essentials,
DOI 10.1007/978-3-658-14688-7_2

Produktion von der kontinuierlichen Anlieferung der Teile abhängt. Selbst dann, wenn die eigene Lieferkette nicht von einer Störung betroffen ist, aber die Supply Chain eines einzelnen Zulieferers, kann die Produktion ins Stocken geraten. Die Reduzierung der Risiken in der Lieferkette bedarf gesonderter Strategien.

Eine Sicherheitsstrategie beginnt mit der Vision. Die naheliegendste Vision einer sicheren Welt ist eine Welt ohne Bedrohungen. Zur Realisierung dieser Vision ist das Problem an der Wurzel zu fassen – nämlich Armut und Ungerechtigkeit zu eliminieren. Jedoch selbst bei Erreichung dieses Zieles bedarf es zur präventiven Sicherstellung des Schutzes von Wirtschaft und Gesellschaft umfangreicher Sicherheitskonzepte, einschließlich der Identifikation und Beobachtung extremistischer und krimineller Gruppierungen.

Ausgangspunkt aller Sicherheitskonzepte ist die Auflistung und Beschreibung der potenziellen Risiken. Diese sind anschließend in Bezug auf die Wahrscheinlichkeit ihres Eintretens und ihre potenziellen Auswirkungen zu bewerten, bevor geeignete Sicherheitsmaßnahmen abgeleitet und ausgearbeitet werden können. Die Erstellung von Risiko-Szenarien hilft bei diesem Prozess.

2.1 Risiko-Szenarien

Tatsächlich braucht es nicht viel Phantasie und Analyse, sondern lediglich den Blick auf verschiedene Ereignisse der vergangenen Jahre, um die Folgen eines Anschlags auf die Supply Chain grob einschätzen zu können: Naturkatastrophen wie der Ausbruch des Vulkans Eyjafjallajökull auf Island, der Tsunami von Fukushima oder der Blizzard in den USA im Februar 2013, aufgrund dessen in fünf Bundesstaaten der Ausnahmezustand ausgerufen wurde, zeigen eindrucksvoll, wie Störungen in der Supply Chain zu einer erheblichen Beeinträchtigung der Wirtschaft führen.

Grundsätzlich gilt: je komplexer die Wertkette, umso mehr Schnittstellen und damit mögliche Angriffspunkte. Je konzentrierter die Produktion, je wichtiger eine Passage, je angehäufter das Gefahrgut, umso größer der mögliche Schaden, umso größer das Risiko. Aber was sind die Angriffspunkte und Schwachstellen, was konkret kann sich entlang der Supply Chain alles ereignen?

1) Produktion, Lagerung und Umschlag

Betriebsstätten, wie Produktionsstandorte, Lager, insbesondere Gefahrgutlager, Umschlagsanlagen, aber auch Datenzentren, einschließlich der Warenwirtschaftssysteme, sind potenzielle Ziele terroristischer Anschläge. Da das Risiko primär von Menschen ausgeht, zählen zu den möglichen Risiko-Szenarien der unbefugte

Zugang zu Gebäuden zur Ausführung terroristischer Anschläge beziehungsweise zum Diebstahl gefährlicher Substanzen sowie der unbefugte Zugriff auf Computer-Systeme zum Diebstahl von Informationen oder zur Manipulation der Abläufe.

Terrorziel Betriebsstätte Das Risiko besteht darin, dass von Mitarbeitern, Kunden und Zulieferern oder anderen Externen, die sich (unbefugt) Zugang zu Betriebsstätten beschaffen, Material entwendet und für spätere Anschläge genutzt wird, oder aber explosive Stoffe eingeschmuggelt werden, die dann während der Verwendung, Lagerung oder eines Transports explodieren. Für die verschiedenen Betriebsstätten, wie Fabriken, Montageanlagen oder logistische Einrichtungen, lassen sich unterschiedliche detaillierte Risiko-Szenarien ausarbeiten.

Missbrauch von Gefahrgut und Anschläge auf Gefahrgutlager Zum Teil werden hochexplosive und andere gefährliche Stoffe gelagert, umgefüllt oder für den Transport vorbereitet. Diese lassen sich für Anschläge nutzen. Die Gefahr, bei einem Einbruch in ein Gefahrgut-Lager gefasst zu werden, ist aufgrund der gewöhnlich bereits bestehenden Sicherheitsvorkehrungen jedoch relativ hoch. Da für terroristische Anschläge zudem teilweise nur kleinere Mengen Giftstoffe – beispielsweise zur Herstellung des chemischen Kampfstoffs Sarin – benötigt werden, ist die legale Beschaffung wahrscheinlich einfacher als der doch risikoreichere Einbruch in ein Lager [48].

Wie gefährdet sind die Betriebsstätten selbst? Lager, Distributionszentren und Hubs, die sogenannten Umschlagsbasen der Logistik-Unternehmen, sind meist in Gewerbegebieten angesiedelt, so dass bei einer Explosion hauptsächlich Sachschaden verursacht wird – ein Szenario, das für Terroristen eher unattraktiv ist. Auch die Auswirkungen auf die Akteure innerhalb der Lieferkette sind wahrscheinlich denkbar gering. Zwar kann es zu Lieferverzögerung – beispielsweise von zeitkritischen Lacken – kommen, allerdings erfordert eine derart gezielte Störung fundierte Kenntnisse der gelagerten Güter und der jeweiligen Supply Chain. Zudem können Unternehmen derartige Engpässe vermutlich schnell wieder beheben. Die ökonomischen Folgen sind daher in der Regel eher gering.

Einen größeren Schaden könnte allerdings der Anschlag auf Gefahrgutlager in Seehäfen oder Flughäfen anrichten. Während die Sicherheitsvorschriften an den Flughäfen eher strikt sind, besteht in den Seehäfen ein höheres Risiko. Grundlage für ein mögliches Szenario ist die Explosion im chinesischen Hafen Tianjin Port im Jahr 2015.

Warenwirtschaftssysteme Die Warenwirtschaftssysteme, englisch Enterprise Resource Planning (ERP) Systems, enthalten Informationen über Produkte, Aufträge, Absatz, Warenbestände, Transport sowie Lieferanten und Kunden. Das *Internet der Dinge* und *Big Data* werden die Menge und Qualität dieser Datenbasis noch erheblich erhöhen. Supply Chain Visibility, das heißt die nahezu lückenlose Verfügbarkeit von Informationen über Verkehrs- und Warenströme, ermöglicht bessere Kontrolle und Steuerung. Allerdings bietet sie Terroristen auch eine weitere Angriffsfläche. Angesichts immer größerer Schiffe und immer höherer Anforderungen an die Lieferkette sind die Abläufe in den Häfen heute ohne umfangreichen Daten- und Informationsaustausch nicht mehr möglich [49]. Leicht lässt sich ausmalen, welche Möglichkeiten sich ergeben, sollte detailliertes Daten- und Informationsmaterial über Güter, Ankunftszeiten und Stauplätze beziehungsweise Lagerstätten in die falschen Hände gelangen. Ein weiteres Szenario ist die Fremdsteuerung bestimmter Prozesse im Stadtverkehr, Lager oder Hafen durch Terroristen.

2) Der Transport auf dem Wasser

Was sind die Risiko-Szenarien in der Schifffahrt? Beispielsweise die Blockade von Meerengen, Kanälen und wichtigen Wasserstraßen, Angriffe auf See, Häfen und Umschlagsanlagen, Diebstahl oder Missbrauch spezieller Güter sowie die kriminelle Nutzung von Umschlags- und Transporthilfsmitteln.

Blockaden von Meerengen, Kanälen und wichtigen Wasserstraßen Für Rolf Tophoven, deutscher Journalist und Direktor des Instituts für Krisenprävention (IFTUS), sind dabei vor allem die Küsten Somalias, Nigerias, Indonesiens, Malaysias und der Philippinen durch Terroranschläge gefährdet. Als ein Szenario gilt dabei der Anschlag in der Malakka-Straße – einem strategischen Nadelöhr, das den Persischen Golf und den Indischen Ozean mit dem Südchinesischen Meer und dem Pazifik verbindet. Mit etwa 90.000 Schiffspassagen jährlich nutzt fast die Hälfte des weltweiten Seehandels die Meerenge. Eine Sperrung der Seestraße würde für die Frachtschiffe einen fast 1000 km langen Umweg durch die indonesischen Straßen von Flores und Sunda bedeuten [50]. Auch der Suez-Kanal gehört zu den Nadelöhren der Weltwirtschaft. Hier wird Ende August 2013 ein Anschlag auf ein Containerschiff verübt, der fehlschlägt. Es gibt Explosionen, das Schiff bleibt nach Behördenangaben jedoch unbeschädigt und der Schiffsverkehr wird nicht beeinträchtigt. Weitere Angaben macht die zuständige Behörde nicht. Allerdings wird bereits in den Tagen vor dem Anschlag die Präsenz der ägyptischen Polizei im Nordsinai entlang des Suez-Kanals verstärkt [51]. Weitaus negativer hat sich der Anschlag auf den Tanker Limbourg vor der Küste des Jemen auf

die maritime Wirtschaft und darüber hinaus ausgewirkt – angefangen von der Verdreifachung der Versicherungsprämien für Schiffe, die jemenitische Häfen anfahren, bis hin zur Einstellung von Liniendiensten in den Jemen. Als Folge gehen Import und Export des Jemen zurück, der Umschlag in den jemenitischen Häfen sinkt von 43.000 Containern im Monat vor den Anschlägen auf 3000 pro Monat nach dem Vorfall. 3000 Hafenarbeiter und Bedienstete verlieren ihre Arbeit und das Bruttoinlandsprodukt geht um rund 1 % zurück [52].

Angriffe auf See Zu den Szenarien, auf die sich Regierungen, Behörden und Wirtschaft ebenfalls vorbereitet haben, zählen Terrorangriffe auf Schiffe und andere Objekte auf See – beispielsweise Ölplattformen –, aber auch der Einsatz von Massenvernichtungsmitteln von der See aus sowie Terrorangriffe auf Hafenanlagen oder andere Ziele an Land, bei denen Schiffe als Transportmittel oder auch als Waffe eingesetzt werden können. Werden beispielsweise Gastanker gekapert und vor oder in einem Hafen zur Explosion gebracht, kann dies angesichts von bis zu 125.000 m^3 Gas pro Schiff erhebliche Folgen haben.

Angriffe auf Häfen und Umschlagsanlagen Auch Gasanlagen in den Häfen sind potenzielle Ziele. Nicht zuletzt deshalb haben die Häfen ihre Sicherheitsmaßnahmen nach den Anschlägen 2001 erhöht. Im Duisburger Hafen, einem der weltweit wichtigsten Binnenhäfen, müssen alle ansässigen Firmen ihre Anlagen mit Zäunen, gesicherten Toren, Video-Überwachung und Beleuchtungsanlagen versehen [53]. Die Explosionen im Tianjin Port führt vor Augen, was sich in einem Hafen ereignen kann: Dort explodieren aus noch ungeklärter Ursache im August 2015 mit Chemikalien beladene Container. Sie lassen eine Lagerhalle für Gefahrgüter zusammenbrechen. Eine zweite Explosion soll eine Sprengkraft von 21 Tonnen TNT haben. Sie ist kilometerweit zu hören, es gibt Hunderte Verletze und Dutzende Tote. Zeitungen melden, dass die Druckwelle und das Feuer rund 1000 Neuwagen auf einem Renault-Lagerplatz zerstört hat. Hinzu kommen weitere 1748 VW-Importwagen, die auf ihre Zollabfertigung und Abholung warten [54]. Insgesamt entstehen Kosten in Höhe von 1,5 Mrd. USD [55]. Ein spektakuläres Szenario. In Anbetracht der großen Ladekapazität birgt auch die mögliche Explosion eines Schiffes in einem Hafen – möglicherweise im Zentrum einer Stadt – ebenfalls erhebliches Bedrohungspotenzial [56].

Diebstahl oder Missbrauch spezieller Güter Nicht nur Pkw, Textilien und andere Zivilgüter reisen via Container – auch militärisches Gerät, Waffen und Munition. So wurden allein 2015 im Hafen Hamburg Waffen im Wert von 360 Mio. EUR umgeschlagen, dies waren 13,2 % mehr als im Jahr zuvor. Die

Flugabwehrpanzer, U-Boote, Gewehre und militärischen Ersatzteile sind ein potenzielles Ziel für Terroristen – ebenso wie die schätzungsweise rund 1000 Container pro Jahr, die beladen mit Granaten, Minen und Patronen von Hamburg aus exportiert werden [57]. Eine Explosion während des Umschlags von Munition hätte erhebliche Folgen für den Hafen und die Anrainer. Generell sind Militärgüter besonders vor Diebstahl zu schützen.

Kriminelle Nutzung von Umschlags- und Transporthilfsmitteln Der Container ist eine Black Box. Einmal verschlossen gibt er in der Regel seinen Inhalt erst wieder beim finalen Empfänger preis. Damit birgt der Container ein Risiko. Die Explosion eines oder mehrerer Container kann an Bord eines Schiffes oder in einem Hafen – wie im Tianjin Port gesehen – viele Menschenleben kosten und erheblichen Sachschaden anrichten oder aber den Verkehr in einem Kanal zum Erliegen bringen.

3) Luftfracht

In der Luftfracht umfassen mögliche Risiko-Szenarien Güter, beziehungsweise Bomben und biologische Waffen in Transportgütern, Angriffe in der Luft, Angriffe auf Frachtflughäfen und Luftfrachtlager und die unbefugte Steuerung des Luftverkehrs.

Güter, beziehungsweise Bomben und biologische Waffen in Transportgütern Mittels Luftfrachtsendungen können Bomben und explosive Stoffe an Bord eines Flugzeuges geschmuggelt werden, die dann in der Luft explodieren oder bestimmte Empfänger treffen sollen – wie im November 2011 geschehen, als Paketbomben im Berliner Kanzleramt, in Dubai und in Großbritannien gefunden wurden. Da Luftfracht auch in Passagierflugzeugen transportiert wird, gefährden explosive Sendungen nicht nur Piloten, sondern auch Passagiere. Verschärft werden kann dies, wenn die Bomben mit biologischen Waffen kombiniert werden, die sich beispielsweise über Wohngebieten entladen können.

Angriffe in der Luft Aufsehen erregt der Flug MH17, der am 17. Juli 2014 mit 283 Passagieren an Bord, davon 80 Kindern, über das umkämpfte Gebiet der Ost-Ukraine fliegt und abstürzt. Wie durch das Dutch Safety Board nach 15-monatigen Nachforschungen bestätigt, wird das Verkehrsflugzeug von einer Rakete getroffen und zerbricht in der Luft [58]. Auch wenn hier nicht unbedingt von einem gezielten Angriff auf ein Passagierflugzeug ausgegangen werden muss, zeigt es die Verwundbarkeit der Flugzeuge auch in der Luft.

Anschläge auf Frachtflughäfen und Luftfrachtlager Neben den Flugzeugen sind auch Flughäfen und Luftfrachtlager potenzielle Ziele. Zum Beispiel können durch Explosionen Menschen getötet und der Flughafenbetrieb unterbrochen werden, wodurch wirtschaftlicher Schaden entsteht.

Unbefugte Steuerung des Luftverkehrs Insbesondere bei Start und Landung werden Daten zwischen Flugzeugen und Boden ausgetauscht. Damit ist die Gefahr einer Cyberattacke dort auch am größten [59]. Die Szenarien reichen hier von bewusst herbeigeführten Kollisionen in der Luft bis hin zu gezielt verursachten Abstürzen in Wohngebiete.

4) Schienentransport
Beim Schienenverkehr sind nicht nur Lokomotiven und Waggons, Bahnhöfe und Umschlagsanlagen, Schienenstränge und Eisenbahnbrücken Gegenstand der Szenarien, sondern auch die Steuerung des Schienenverkehrs, beispielsweise die digitale Manipulation von Signalanlagen und Weichen.

Anschläge auf Lokomotiven und Waggons, Bahnhöfe und Umschlagsanlagen Anfang Dezember 2003 entdecken russische Sicherheitsbehörden im Bahnhof Kropotkin an einem Güterzug einen Sprengsatz mit Zeitschaltuhr, der direkt entschärft wird. Einige Tage zuvor werden bei einem Anschlag auf einen Vorortzug im russischen Nordkaukasus 42 Menschen getötet [60]. In der ukrainischen Stadt Charkiw wird im März 2015 ein Anschlag auf einen Güterzug verübt. Bei der Explosion springen zwei leere Waggons aus den Gleisen.

Sabotage von Schienensträngen und Eisenbahnbrücken In der Ukraine wird im März 2015 ein Gleisabschnitt durch einen Sprengsatz zerstört. In der Stadt Izum hat der ukrainische Geheimdienst im selben Monat einen Anschlag auf eine Eisenbahnbrücke verhindern können [61].

Eingriffe in die Steuerung des Schienenverkehrs Die digitale Steuerung von Verkehrssystemen nimmt zu. Das Cyber-Risiko steigt – ein Thema, das in Zukunft nicht nur eine immer größere Rolle spielen, sondern durch den Einsatz von autonomen, das heißt führerlosen, Zügen eine weitere Verschärfung erlangen wird. Mögliche Szenarien sind Kollisionen und Entgleisungen sowie beispielsweise das Rasen eines unbemannten Zuges in einen Sackbahnhof.

5) Straßengütertransport
Beim Straßengüterverkehr steht das Szenario Zweckentfremdung, d. h. der Missbrauch von Transportmitteln als Lager für Bomben und Sprengstoffe, im

Vordergrund. Darüber hinaus nimmt im digitalen Zeitalter das Risiko im Bereich der digitalen Steuerung des Straßenverkehrs zu.

Zweckentfremdung Fahrzeuge wie Lkw und Pkw werden als Transportmittel und Lager für Sprengstoffe und Bomben genutzt. Im Fahrzeug am Zielort gelagert, explodieren die Sprengsätze zur vorbestimmten Zeit. Da Zustellfahrzeuge und Lkw zum alltäglichen Straßenbild gehören, erzeugen sie in der Regel keinen Argwohn – selbst dann nicht, wenn sie über längere Zeit an einem belebten Platz parken. So kommen im März 2015 Dutzende Menschen bei der Explosion einer Lkw-Bombe auf dem Marktplatz von Bagdad ums Leben, etwa 200 werden verletzt. Zu dem Anschlag bekennt sich *Daesh* [62]. Ähnlich wie Frachtschiffe und Güterzüge könnten auch Tankfahrzeuge, die mit chemischen oder giftigen Stoffen beladen sind, als Waffen gegen Objekte und bestimmte Ziele eingesetzt werden. Dabei lassen sich Lkw in der Regel leichter kapern als Güterzüge – beispielsweise, wenn der Fahrer schläft. Ladungsdiebstähle während der Fahrt gehören heute zum Alltagsrisiko der Lkw-Fahrer [63].

Unbefugte Steuerung des Straßenverkehrs Die digitale Steuerung des Verkehrs, beispielsweise im Rahmen von Smart-City-Projekten, nimmt zu. Zudem steigt die Wahrscheinlichkeit des Einsatzes autonomer Fahrzeuge. Die Risiko-Szenarien erstrecken sich von verrückt spielenden Ampelsystemen bis zum unkontrollierten Agieren autonomer Fahrzeuge.

6) Künstliche Intelligenz

Das Cyber-Risiko zieht sich durch fast alle Szenarien. Dies, weil die Digitalisierung in nahezu alle Bereiche von Wirtschaft und Gesellschaft Einzug genommen hat. Dass in jedes System eingedrungen werden kann, ist uns bewusst. Dass künstliche Intelligenz eine neue Dimension des Terrors eröffnet, ist einigen vielleicht nicht so geläufig.

Im März 2016 besiegt der Roboter AlphaGo den Südkoreanischen Grand Master Lee Sedol im Spiel Go, das ein hohes Maß an Intuition und hoch entwickelte Fähigkeiten der Mustererkennung voraussetzt. Seit dem Sieg von AlphaGo ist klar: Computer nutzen Lösungen, die Menschen nicht finden oder nicht in Erwägung ziehen – dies nicht nur durch Logik und Heuristik, sondern auch durch Verstärkungslernen, englisch reinforcement-learning. Dies kann in vielen Bereichen sehr hilfreich sein. Gleichzeitig stellt sich die Frage: Wie können wir ethisches Verhalten sicherstellen, wenn wir die Methoden nicht mehr kennen und vielleicht gar nicht mehr verstehen [64]? Das Thema Ethik und Maschine wird auch bei

der Entwicklung von autonomen Fahrzeugen diskutiert. Welche Ethik soll den Fahrzeugen ‚einprogrammiert' werden – insbesondere wenn es um Entscheidungen um Leben und Tod geht? Schnell liegt aber auch eine andere Frage auf der Hand: Wie können wir verhindern, dass selbstlernende Programme in die falschen Hände fallen? Denn Terroristen würden dadurch nicht nur neue Werkzeuge zur Spekulation und Finanzierung an den Börsen, sondern auch Zugriff auf Vernichtungswaffen einer ganz neuen Dimension erhalten.

Solange die Maschinen noch zu einem erheblichen Grad von Menschen gesteuert und kontrolliert werden, bleibt auch der Mensch der einzige Ausgangspunkt des Terrors. Denn Verbrechen werden derzeit noch ausschließlich von Menschen erdacht, geplant und durchgeführt – nicht von Fahrzeugen, Paketen und Paletten oder selbstlernenden Programmen. Der Mensch ist aber nicht nur Ausgangspunkt, sondern auch wesentliche Schwachstelle im System. Gesicherte Betriebsstätten und Transportmittel können von kriminellem oder käuflichem Personal trotz aller Schutzmaßnahmen zugänglich gemacht werden und geschützte Computer-Systeme durch die Weitergabe der Codes durch an der Entwicklung derselben beteiligte Programmierer dennoch wieder manipulierbar werden.

2.2 Sicherheit entlang der Supply Chain

Die Verantwortlichen in der Wirtschaft und den Behörden sind aufgrund der neuen Gewalt sowie der rasanten technologischen Entwicklung gefordert, sicherzustellen, dass die Strategien und Konzepte entlang der Supply Chain stets den neuesten Standards entsprechen und möglichst keine Schwachstellen aufweisen. Aufgrund der Dynamik der Digitalisierung kann die Cybersicherheit als Achillesferse angesehen werden.

Dabei stehen Regierungen und Unternehmen mit den Sicherheitsstrategien keineswegs am Anfang. Im Gegenteil: Die aktuellen Konzepte beinhalten ein breites Spektrum an Vorkehrungen und Maßnahmen – angefangen bei der sorgfältigen Auswahl der Mitarbeiter, dem Gebäudeschutz bis hin zur Zusammenarbeit mit Behörden und anderen Organisationen. Auch die Cyber-Sicherheit gewinnt zunehmend an Beachtung. Zudem werden Wirtschaftsakteure zu Experten qualifiziert. Ein Prädikat für Sicherheit ist der Zugelassene Wirtschaftsbeteiligte.

Der Zugelassene Wirtschaftsbeteiligte bzw. Authorized Economic Operator (AEO)

Zugelassene Wirtschaftsbeteiligte sind Logistik-Dienstleister, die aufgrund der Erfüllung spezieller Voraussetzungen verschiedene Vergünstigungen bei der

Zollabwicklung in Anspruch nehmen können. Sie sind für das Thema Sicherheit besonders sensibilisiert. Der AEO muss u. a. sicherstellen, dass von der Fracht keine Bedrohung für den Luftverkehr ausgeht. Demnach geht es nicht nur um die Einhaltung von Zoll- und Außenhandelsvorschriften. Auch das Thema Sicherheit steht im Fokus – angefangen bei der Frage, ob Waren als Dual-Use-Güter, das heißt Güter mit ziviler und (potenzieller) militärischer Nutzung, eine besondere Genehmigung benötigen.

Logistik-Dienstleister, die als AEO zertifiziert sind, müssen beispielsweise Luftfrachtsendungen derart verpacken, dass eine nachträgliche Manipulation ohne sichtbare Spuren ausgeschlossen ist. Dadurch wird verhindert, dass Verpackungen nach erfolgter Sicherheitsüberprüfung ohne Weiteres wieder geöffnet und verschlossen werden können. Zudem ist der AEO dazu verpflichtet, die Einhaltung der Sicherheitsmaßnahmen ebenfalls bei Sub-Unternehmern und Unterauftragnehmern – beispielswiese im Bereich der Lagerung – sicherzustellen.

Der Status des AEO wird von den USA seit Frühjahr 2013 anerkannt. Im Gegenzug erkennt die EU das amerikanische Sicherheitsprogramm C-TPAT an [65].

Supply Chain Mapping – Basis des Sicherheitsmanagements

Schützen beginnt mit Verstehen. Nach dem Erdbeben im Jahre 2011 in der japanischen Region Tohoku musste Toyota die Supply Chain neu überdenken und war überrascht, zu erkennen, dass die Lieferkette nicht – wie gedacht – pyramidenförmig aufgestellt war, sondern der Form einer Tonne glich. Die Katastrophe half dem Unternehmen, seine Supply Chain zu verstehen [66]. Die klare Vision der Supply Chain ist die Voraussetzung für das optimale Design bzw. das Re-Design – auch aus Sicherheitsgesichtspunkten. Ein wichtiges Instrument zum Verstehen der Lieferkette ist das Mapping beziehungsweise die Supply Chain Map.

Um sich gegen die Bedrohungen entlang der Supply Chain zu schützen, müssen die Verantwortlichen die Lieferkette in Gänze und als Netz abbilden sowie den jeweiligen Status in Bezug auf Fertigungs-, Bestands- und Bewegungsdaten erfassen können. Dieses sogenannte Supply Chain Mapping kann zum einen die Struktur, wie Lieferanten (über alle Stufen) und Logistikpartner, Produktinformationen, Produktionsstätten und Lager, einschließlich der Standorte, (alternative) Routen, Umschlagspunkte, Zollstellen, Distributionslager, Kundeninformationen und benötigte Zeiten für die einzelnen Abschnitte sowie zum anderen die Bewegungsdaten, wie Bestellmengen, Produktionsdaten und Produktionsstatus, Bestände und im Transport befindliche Güter sowie Absatzzahlen einschließen.

Nur auf Basis dieses Wissens können Lieferanten, Kunden und andere Akteure, Standorte und Güter, Routen und Systeme auf Risiken hin analysiert und entsprechende Sicherheitsmaßnahmen entwickelt werden.

Schwachstelle Mensch: Die Gratwanderung zwischen Vorsicht und Misstrauen

Mit Hilfe sozialer Medien rekrutieren Terrormilizen wie *Daesh* weltweit – auch in Europa. Rolf Tophoven weist in seinem Beitrag „Der Terror eskaliert – neue Varianten des militant islamistischen Phänomens. Paris und die Folgen" darauf hin, dass nach Angaben der Sicherheitsbehörden etwa 600 kämpfende Unterstützer nach Syrien gereist sind. Nicht alle bleiben Anhänger der Milizen – so sollen 180 von ihnen traumatisiert zurückgekommen sein. Weitere 30 Heimkehrer gelten jedoch als militärisch ausgebildet und kampferprobt. Hinzu kommen etwa 260 Gefährder [67]. Diese könnten den Zugang zu Betriebsstätten und Transportmitteln dazu nutzen, Terrorakte vorzubereiten oder durchzuführen.

Nach den Anschlägen vom 11. September 2001 wurden viele bestehende Sicherheitskonzepte verschärft und neue Maßnahmen eingeführt. Dazu zählen auch die Sanktionslisten der USA und der EU, speziell die VO (EG) 881/2002 vom 27.05.2001 und die VO (EG) 2580/2001 vom 27.12.2001. Personen-Embargo-Listen sollen helfen, die Finanzströme terroristischer Gruppen auszutrocknen. Zu diesem Zweck sind Handels- und Wirtschaftstreibende verpflichtet, jeden Handelspartner mit den Sanktionslisten abzugleichen. Findet sich der Name eines aktuellen oder potenziellen Partners auf der Liste, darf mit der entsprechenden Person oder Firma kein Geschäft mehr getätigt werden.

Diese Regelung betrifft potenzielle zukünftige Mitarbeiter ebenso wie das bestehende Personal. Dies bedeutet: Erscheint ein Mitarbeiter auf der Liste, darf kein Gehalt mehr ausgezahlt werden. Bewerber, die auf einer dieser Listen stehen, dürfen nicht eingestellt werden [68]. Wer dagegen verstößt, muss mit Freiheitsstrafen zwischen sechs Monaten bis fünf Jahren sowie Geldbußen von bis zu einer Millionen Euro rechnen. Geschäftsführer und Vorstand können für die Missachtung haftbar gemacht werden. Auch eine Gewerbeuntersagung wegen Unzuverlässigkeit (§ 35 I GewO) kann verhängt werden, oder es kann eine Eintragung in das Gewerbezentralregister (§ 149 II Nr. 1 lit. b GewO) erfolgen [69].

Der Abgleich von Geschäftspartnern, Mitarbeitern und Bewerbern ist eine Maßnahme der Prävention. Denn werden bestehende Kontakte zu Terrororganisationen frühzeitig bekannt, können zukünftige Anschläge vermieden werden. So sehen die Betriebsvereinbarungen von Daimler unter anderem vor, dass Mitarbeiter, die auf einer Sanktionsliste stehen, sofort freigestellt werden und

gegebenenfalls die Behörden zu informieren sind [70]. Dabei sind die Personen-Embargo-Listen keinesfalls lückenlos und fehlerfrei. Gefährder, die den Behörden nicht bekannt sind, sind logischerweise nicht aufgeführt, während andererseits in Einzelfällen Personen unbegründet aufgenommen werden.

Die Unternehmen sind gefragt, ihre Mitarbeiter für Gefahren zu sensibilisieren. So kann beispielsweise das Hinnehmen der Radikalisierung einzelner Mitarbeiter verheerende Folgen haben – für Unternehmen und Gesellschaft. Daher sind ungewöhnliche Entwicklungen den Vorgesetzen bzw. der Personalabteilung zu melden. Nur so kann frühzeitig das Gespräch gesucht und bei Bedarf entsprechend reagiert werden. Dies ist von besonderer Wichtigkeit, wenn Zugriff auf sensible Daten besteht oder im Rahmen der Tätigkeiten u. U. Anschläge direkt unterstützt oder sogar selbst ausführt werden könnten.

Regelmäßige Informationen in Form von Flyern, Postern und in internen Medien helfen dabei, die Aufmerksamkeit der Mitarbeiter zu schärfen. Durch die redaktionelle Aufbereitung können dabei Informationen über potenzielle Risiken und die Möglichkeiten der Risikominderung, aber auch das situationsgerechte Handeln bei Gefahr vermittelt werden. Updates in Bezug auf die Sicherheitsvorschriften können auf diesem Weg ebenfalls kommuniziert werden.

Auch externe Personaldienstleister müssen überprüft und auf ihre Verantwortung in Bezug auf die Sicherheit verpflichtet werden.

Neue Mitarbeiter sollten in der Einarbeitungsphase von einem festen Ansprechpartner persönlich betreut werden. Dieser muss entsprechend geschult und sensibilisiert sein und bei auffälligem Verhalten den Sicherheitsbeauftragten informieren. Generell gilt: Je besser der persönliche Draht unter Kollegen und zu Vorgesetzen, umso schneller werden finanzielle, familiäre oder persönliche Schwierigkeiten bekannt. Auch Ausnahmesituationen wie lange Streiks, Unzufriedenheit mit der Einkommenssituation sowie als unfair empfundene Arbeitsbedingungen können zur Destabilisierung von Menschen beitragen. Alle Akteure sind gefragt, zum verantwortungsvollen Miteinander beizutragen [71]. Das frühzeitige Anbieten von Unterstützung kann helfen, zu verhindern, dass persönliche Schwierigkeiten oder das Gefühl von Ungerechtigkeit zum Auslöser extremistischen Denkens und Handelns werden. So kann u. U. auch vermieden werden, dass sich Mitarbeiter allein, isoliert oder überfordert fühlen – ein Zustand, der von Terrororganisationen durchaus ausgenutzt werden kann [72].

Die Führungskräfte haben hierbei eine ganz besondere Rolle und Verantwortung. Denn zwischen Vorsicht und Misstrauen verläuft ein schmaler Pfad.

Auch Überreaktionen sind zu vermeiden. Am Genfer Flughafen verlieren nach den Anschlägen von Paris 30 Mitarbeiter ohne weitere Begründung ihren

Arbeitsplatz. Auffällig sind dabei die Gemeinsamkeiten: Mit zwei Ausnahmen haben alle einen französischen Pass, einen arabischen Namen und sind zum Großteil Muslime. Ein Zusammenhang zwischen Herkunft, Religion und Kündigung wird vom Flughafenbetreiber ausgeräumt [73].

Jegliche Maßnahme gegen Mitarbeiter sollte juristisch geprüft sein, um Verstöße gegen bestehende Gesetze, wie das Allgemeine Gleichstellungsgesetz (AGG), zu vermeiden. Das AGG untersagt beispielsweise in § 9 die Benachteiligung von Personen aufgrund von Religion und Weltanschauung. Ein pauschaler Ausschluss von bestimmten Tätigkeiten ist damit in Deutschland ohne Weiteres nicht möglich – ebenso wenig wie eine unbegründete Kündigung.

Exemplarische Übersicht: Sicherheitsvorkehrungen bei Mitarbeitern

- Regelmäßiger Abgleich der Mitarbeiter- und Bewerberdaten sowie der Namen der Geschäftspartner mit den Personen-Embargo-Listen der EU und der USA
- Persönliche Begleitung neuer Mitarbeiter in der Einarbeitungsphase
- Regelmäßige Schulungen und Informationen rund um das Thema Sicherheit und Gefahrenabwehr
- Nutzung der internen Kommunikation zur Sensibilisierung von Management und Mitarbeitern sowie zur Vermittlung von Informationen zum Risiko-Management
- Bei Auffälligkeiten von Mitarbeitern Rücksprache mit früheren Arbeitgebern
- Bei ernsten Verdachtsmomenten Einschaltung der Behörden
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse

Schutz von Betriebsstätten

Allein schon aufgrund des materiellen Wertes der Produkte und Güter werden Immobilien gesichert – durch Zäune, Video-Überwachung, verschließbare Tore, unternehmenseigene und externe Sicherheitsdienste und viele weitere Maßnahmen.

Eine wesentliche Schwachstelle ist der Mensch: Wie kann ein Unternehmen sicherstellen, dass bei jedem Besucher, Lieferanten und Pizzaboten die Zugangsberechtigung geprüft wird? Dass Papiere auch dann vorgezeigt werden, wenn es schnell gehen muss? Dass Mitarbeiter besonnen den Sicherheitsdienst bzw.

Sicherheitsbeauftragten informieren, wenn sich ein Unbefugter Zutritt verschafft oder sich eine Person auffällig verhält? Schlussendlich hängt von den Mitarbeitern ab, ob und wie schnell ein Risiko erkannt wird und welche Maßnahmen ergriffen werden können. Wird die Zugangskontrolle automatisiert beziehungsweise digitalisiert, setzt das Cyber-Risiko ein.

Die Betreiber von Immobilien ergreifen verschiedene Sicherheitsvorkehrungen, um sich vor Diebstahl und unbefugtem Zugang zu schützen. Dazu zählen u. a.: geschulte Sicherheitsbeauftragte und Security Teams, Zugangskontrollen, Chip-Karten für die Mitarbeiter, Drehkreuze, Video-Überwachung sowie Gitter und detektierte Zäune. Auch Drohnen können zur Überwachung eingesetzt werden. Kontinuierliche Sensibilisierung und Information der Mitarbeiter hilft der Verankerung von Sicherheitsdenken im Arbeitsalltag. Auch die enge Zusammenarbeit zwischen Unternehmen und Behörden gehört in der Regel zur Routine.

Das Sicherheitsniveau lässt sich testen – beispielsweise durch im Unternehmen unbekannte Personen, die im Auftrag des Managements versuchen, das Gelände zu betreten und sich Sicherheitsbereichen zu nähern, ohne sich auszuweisen.

Zum Schutze besonders gefährdeter Gebäude und Gelände oder in Ländern mit hohem Risiko setzen US-Behörden spezielle Barrieren ein, die in der Lage sind, Lkw nicht nur aufzuhalten, sondern gar zu spalten. Die unter dem Namen Terror-Bügel bekannt gewordene Konstruktion aus Stahl und Beton wurde vom *Texas A&M Transportation Institute* (TTI) in Zusammenarbeit mit dem amerikanischen Außenministerium entwickelt. Der Terror-Bügel ist fast einen Meter dick, erstreckt sich über 15 m Länge und wiegt rund 22,600 kg. Verankert wird er mit einem 18 cm dicken Betonfundament, so dass ein fast 7000 kg schwerer Lkw aufgehalten werden kann, wie ein Video eindrucksvoll zeigt [74].

Exemplarische Übersicht: Schutz von Betriebsstätten

- Zugangskontrolle, Sicherheitsdienste, detektierte Zäune, Sicherheitsbeauftragte und/oder Security-Dienste, Video- und Wärmbildkameras, Drohnen
- Abgleich aller Bewerber und Mitarbeiter mit den Personen-Embargo-Listen der EU und der USA
- Chipkarten für Mitarbeiter, Zugang über Drehkreuze
- Schulung der Mitarbeiter in Bezug auf Sicherheit

- Schutz der Computer-Systeme, im Wesentlichen Warenwirtschaftssysteme, Warehouse Management Systems und Inventory Management Systems
- Bei hoch gefährdeten Betriebsstätten Barrieren wie Terror-Bügel
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse
- Gefahrenabwehr- und Business-Contingency-Pläne
- Erfahrungsaustausch und Abstimmung der Sicherheitskonzepte zwischen den verschiedenen Akteuren entlang der Supply Chain

Sicherheit im Luftverkehr

Sowohl der Anschlag auf das russische Passagierflugzeug im Sinai Ende Oktober 2015 als auch der Anschlag Anfang Februar 2016 in Mogadischu soll mit Hilfe von Flughafenpersonal verübt worden sein [75]. Die sorgfältige Bewertung und Auswahl aller Mitarbeiter und Kandidaten, unabhängig von Funktion und Dauer des Einsatzes, ist damit Grundvoraussetzung für Sicherheit. Auch bei Aushilfspersonal ist das Einholen des polizeilichen Führungszeugnisses Pflicht. Veränderungen im Verhalten einzelner Mitarbeiter sind zeitnah zu hinterfragen und gegebenenfalls zu melden.

Nicht nur das Personal, auch die Luftfracht unterliegt strikten Kontrollen. So werden auf einem Teil der Flughäfen seit 2013 unter anderem speziell ausgebildete Sprengstoffspürhunde eingesetzt [76]. Diese kommen vor allem dann zum Einsatz, wenn große und sperrige Fracht kontrolliert werden muss, die für die Röntgendetektoren zu sperrig ist. Stehen keine Hunde bereit, wird voluminöse Fracht mit einem Sprengstoffdetektor untersucht. Dieser kommt beispielsweise auf dem Flughafen Stuttgart zum Einsatz. Der Logistik-Dienstleister Logwin kontrolliert dort seit April 2012 Luftfracht mit einem 1,80 m $\times$ 1,80 m großen Röntgenscanner – größer dürfen die Geräte nach Vorgaben des Luftfahrt-Bundesamtes nicht sein [77].

2014 wird im Vergleich zu 2013 auf deutschen Flughäfen 2,6 % mehr Luftfracht umgeschlagen – und damit insgesamt 4,4 Mio. Tonnen [78]. Allein am Fraport-Flughafen in Frankfurt – dem deutschen Flughafen mit dem höchsten Frachtaufkommen – waren dies 2014 etwas über 2,1 Mio. Tonnen [79]. Zum Schutz von Wirtschaft und Gesellschaft hat der Fraport – aufbauend auf den Vorgaben und Empfehlungen der Zivilluftfahrtorganisation ICAO – ein umfassendes Sicherheitskonzept entwickelt und umgesetzt [80].

Während der ältere Teil des Fraports mittels herkömmlicher Maschendrahtzäune geschützt ist, umgibt die Landebahn Nordwest ein detektierter Zaun. Die

ruhestromüberwachten Drähte geben Alarm, wenn jemand versucht, den Zaun zu beschädigen, zu übersteigen oder unter dem Zaun auf das Flughafengelände zu gelangen. Auch das Anlehnen einer Leiter löst Alarm aus und erreicht direkt die Sicherheitszentrale. Von dort aus haben die Mitarbeiter dank 2500 installierter Videokameras die Geschehnisse sofort im Blick. Ist auf den Live-Bildern nichts zu erkennen, können sie auf die gespeicherten Aufnahmen zurückgreifen. Für die Überwachung in der Nacht ist das Gelände hell erleuchtet. Ergänzend dazu sind Wärmebildkameras im Einsatz. Zudem fahren Bundespolizei und das Sicherheitspersonal des Fraports auf dem Gelände regelmäßig Streife. Im Jahr 2014 kam es nach Angaben des Betreibers am Frankfurter Flughafen zu 202.784 sicherheitsrelevanten Vorkommnissen, die alle erfasst und dokumentiert wurden. Dazu gehören unter anderem Versuche von Mitarbeitern, mit abgelaufenem Ausweis Türen zu öffnen [81].

Flughafenbetreiber und Luftfahrtunternehmen arbeiten u. a. mit der Bundespolizei und EU-Inspektoren zusammen. Schwerpunkte sind dabei beispielsweise die Prozessoptimierung von Fluggaststeuerungs- sowie Sicherheitskontrollverfahren. Um Sicherheitslücken zu schließen werden von der Buchung bis zum Abflug alle Prozesse überprüft – inklusive der Wegführung, der Beschilderung und der Sicherheitskontrollen [82].

Im Kampf gegen den Terrorismus arbeiten auch internationale Sicherheitsbehörden immer enger zusammen [83]. Daten sowie Informationen von Geheimdiensten werden bilateral ausgetauscht, um Anschläge zu verhindern. Seit Jahren bereits werden die Daten von Flugreisenden in die USA übermittelt, um Reisebewegungen nachvollziehbar zu machen. Auch auf europäischer Ebene werden seit neuerem Daten von Flugpassagieren gespeichert [84].

Exemplarische Übersicht: Sicherheitsvorkehrungen auf Flughäfen

- Zugangskontrolle in den Frachtbereichen durch Sicherheitspersonal, Beleuchtung des Geländes in den Nachtstunden, Sicherheitsdienste, detektierte Zäune, Video- und Wärmbildkameras, Drohnen
- Abgleich aller Bewerber und Mitarbeiter mit den Personen-Embargo-Listen der EU und der USA
- Schulung der Mitarbeiter in Bezug auf Sicherheit
- Chipkarten für Mitarbeiter, Zugang über Drehkreuze, Mitarbeiterschulungen
- Prozessoptimierung von Fluggaststeuerungs- und Sicherheitskontrollverfahren

- Überprüfung der Frachtsendungen mittels Röntgengeräten, Sprengstoffhunden und Sprengstoffdetektoren
- Sicherheitszentrale zur schnellen Reaktion bei Gefahr
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse
- Cyber-Sicherheit
- Gefahrenabwehr- und Contingency-Pläne
- Erfahrungsaustausch und Abstimmung der Sicherheitskonzepte zwischen den verschiedenen Akteuren entlang der Supply Chain
- Zusammenarbeit mit der Bundespolizei und anderen Behörden, beispielsweise mit EU-Inspektoren

Der sichere Güterversand über die Schiene

Ansatzpunkte bei der Risikominderung im Güterschienenverkehr liegen vor allem im Bereich der Beladung – hier ist darauf zu achten, welche Güter verladen werden. Besondere Beachtung gebührt den Gefahrgütern, da von diesen das größte Risikopotenzial ausgeht. Um bewusste Manipulationen bei der Fracht zu vermeiden, müssen Mitarbeiter geschult und sensibilisiert sowie Hallen und Flächen mit modernster Technologie überwacht werden – Drohnen können ebenfalls zum Einsatz kommen.

Aber auch die Güterzüge erfordern Aufmerksamkeit. Entsprechende Sicherheitskonzepte bestehen bereits bei Verladern mit Gleisanschluss – um zu verhindern, dass Waggons mit Sendern oder Sprengstoffsätzen versehen werden. Waggons sollten grundsätzlich auf bewachten Gleisen, die nach Möglichkeit mit Videokameras ausgestattet sind, abgestellt werden. Dabei ist die Zusammenarbeit von Bahn-Unternehmen und Logistik-Dienstleistern gefragt.

Bei der zunehmenden Digitalisierung der Steuerung des Zugverkehrs sind entsprechende Cyber-Sicherheitskonzepte zu entwickeln. Eine weitere Verschärfung des Cyber-Risikos steht mit dem zu erwartenden Einsatz autonomer Züge an.

Exemplarische Übersicht: Sicherheitsvorkehrungen für den Schienentransport

- Zugangskontrolle in den Umschlagterminals, Beleuchtung des Geländes in den Nachtstunden, Sicherheitsdienst, detektierte Zäune, Video- und Wärmbildkameras, Drohnen
- Sicherung der Gleisanschlüsse bei Verladern und Logistik-Unternehmen

- Abstellen von Waggons nur auf überwachten Gleisen
- Sicherheitsprozess für die Beladung
- Abgleich aller Bewerber und Mitarbeiter mit den Personen-Embargo-Listen der EU und der USA
- Mitarbeiterschulungen in Bezug auf Sicherheit
- Cyber-Sicherheit
- Gefahrenabwehr- und Contingency-Pläne
- Erfahrungsaustausch und Abstimmung der Sicherheitskonzepte zwischen den verschiedenen Akteuren, beispielsweise Verladern, Logistikern und Bahn-Unternehmen
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse

Sicherheitsmaßnahmen im Straßengüterverkehr

Ein erhebliches Risiko resultiert aus der Zweckentfremdung von Fahrzeugen. Um zu verhindern, dass beispielsweise Lkw für terroristische Anschläge genutzt werden, sind entsprechende Sicherheitsvorkehrungen zu treffen – beispielsweise das Abstellen von Lkw auf bewachten Parkplätzen, die nach Möglichkeit mit Videokameras gesichert sind. Ist dies nicht möglich, sollten Lkw-Fahrer – auch im eigenen Interesse – die Parkplätze für die Ruhezeiten sorgfältig auswählen, beispielsweise gut beleuchtete und bewachte Gelände.

Weitere Vorsichtsmaßnahmen sind das regelmäßige Abschließen des Fahrzeugs – auch bei kurzem Halt – sowie die Kontrolle des Fahrzeugs und der Ladung nach jeder Pause. Auch das Nichtmitnehmen von Anhaltern oder unbekannten Personen trägt zum Schutz bei. Bei ungewöhnlichen Straßensperren oder (scheinbar) verletzten Personen auf der Fahrbahn ist ebenfalls Vorsicht geboten. Fahrer sollten durch Sicherheitsfahrtrainings auf Gefahrensituationen im Verkehr vorbereitet werden – dies schützt unter anderem vor provozierten Unfällen.

Zu den weiteren Präventionsmaßnahmen zählt Verschwiegenheit. Denn auch die Ladung des Lkw macht diesen für Terroristen interessant. Ist nicht bekannt, was wann über welche Strecken transportiert wird, verringert sich das Risiko. Interessant wird es, wenn bekannt wird, welche Route ein Lkw geladen mit Smartphones im Wert von 1,5 Mio. EUR – mehr als der Wert der Ladung eines Geldtransporters – nehmen wird [85]. Die Beute wird von Terroristen für die Finanzierung ihrer Tätigkeiten genutzt [86].

Da die Wert- und Routinginformationen in den Datenbanken der Dispositionsprogramme vorgehalten werden, spielt die Cyber-Sicherheit, d. h. der Schutz der Computer-Systeme, ebenfalls eine große Rolle. Das Risiko erstreckt sich dabei

nicht nur auf den unbefugten Zugriff auf die Daten, sondern auch auf die Manipulation derselben zur Fremdsteuerung der Abläufe. Durch Cyber-Sicherheitsmaßnahmen wird beispielsweise vermieden, dass Lkw abgefangen oder Waren von Kriminellen gezielt in einem Umschlagsterminal auf eigene Lkw verladen und damit gestohlen werden.

Exemplarische Übersicht: Sicherheitsvorkehrungen für den Straßengüterverkehr

- Abgleich aller Bewerber und Mitarbeiter mit den Personen-Embargo-Listen der EU und der USA
- Sicherheitsprozesse für die Beladung
- Schulung von Mitarbeitern und Fahrern in Bezug auf Sicherheit
- Aufsuchen bewachter und gut ausgeleuchteter Parkplätze
- Abschließen der Fahrzeuge auch bei kleinen Pausen – gegebenenfalls Lkw mit Sensoren an den Türen und Kameras ausrüsten, zur Real-time-Überwachung
- Kontrolle des Fahrzeugs und der Ladung nach jeder Pause
- Keine Mitnahme von Anhaltern oder unbekannten Personen
- Keine Gespräche mit Dritten über Ladung, Wert oder Routen
- Sofortige Meldung ungewöhnlicher Routenänderungen aufgrund Sperrungen o. Ä. – gegebenenfalls Lkw mittels Sicherheitssystemen in Real-time nachverfolgen
- Cyber-Sicherheit: Schutz der Computer-Systeme, zum Beispiel vor unerlaubtem Zugriff auf die Routenplanung und Beladungsinformationen
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse
- Gefahrenabwehr- und Contingency-Pläne
- Erfahrungsaustausch und Abstimmung der Sicherheitskonzepte zwischen den verschiedenen Akteuren entlang der Supply Chain

Sicherheitsmaßnahmen in der Schifffahrt

In den USA sind Häfen Hochsicherheitsgebiete, zu denen die Öffentlichkeit keinen Zugang hat. In Deutschland ist dies mit den zahlreichen Binnenhäfen, auch mit dem Hamburger Hafen anders: Bei Touristen und Einheimischen ist der Hafen beliebtes Ausflugsziel. Da dieser mitten in der Stadt liegt, ist er leicht zu erreichen und kann auch nicht ohne Weiteres vom Stadtleben getrennt werden.

Dennoch reagiert der Hamburger Hafen auf die Terrorgefahr. Der Betreiber schützt sich unter anderem durch die konsequente Umsetzung des ISPS-Codes (Internationale Schiffs- und Hafenanlagen-Sicherheit). So sind beispielsweise die Kaianlagen des Hamburger Hafens Hochsicherheitsgebiet. Angesiedelte Unternehmen sind dazu verpflichtet, diverse Vorgaben einzuhalten. Sie müssen beispielsweise überwachen, wer Firmenräume und Firmengelände betritt. Um dies zu gewährleisten, wird von den Unternehmen auf dem Hafengelände in entsprechende Sicherheitstechnik wie Videokameras, Drehkreuze und Chip-Ausweise investiert. Bei den Personenkontrollen sind am Hamburger Hafen die Flughafenkontrollen der Maßstab. Dazu wird das Sicherheitspersonal der Unternehmen entsprechend geschult [87].

Überprüft werden nicht nur Besucher, sondern auch das Personal im Hafen und in den Unternehmen – und dies bereits, bevor sie ihre Arbeit aufnehmen. Vor allem Personen, die in besonderen Sicherheitsbereichen der Hafenanlagen arbeiten oder mit Sicherheitsaufgaben betraut sind, werden von der Hafensicherheit überprüft. Darüber hinaus gehören zu den Aufgaben der Hafensicherheit die Risiko- und Schwachstellenanalyse der Hafenanlagen und die Beratung der Hafenanlagenbetreiber bei der Erstellung der Gefahrenabwehrpläne. Die Prüfung und Genehmigung dieser Pläne liegt auch in ihrem Verantwortungsbereich. Das Wissen und die Erkenntnisse der Hafensicherheit fließen in Gremien wie die Hafensicherheitskommission und den Bund-Länder-Ausschuss Maritime Security mit ein [88].

Gefahr droht nicht nur auf dem Land, sondern auch vom Wasser aus. Deshalb schreibt der ISPS-Code nicht nur Sicherheitsoffiziere in den Häfen und Reedereien, sondern auch auf den Schiffen vor. Wichtig ist, zu wissen, welche Schiffe den Hafen ansteuern. Daher arbeitet der Hamburger Hafen seit 2003 – und damit als erster Hafen weltweit – mit dem neuen Automatischen Identifikationssystem (AIS). Eine Blackbox an Bord der Schiffe sendet via UKW-Funk alle nötigen Informationen wie Kurs, Geschwindigkeit, Identifikationsnummer, Länge, Breite, Tiefgang und das Funkrufzeichen an die relevanten Stellen an Land und an entgegenkommende Schiffe [89].

Ein besonderes Risiko besteht beim Passieren von Meerengen oder in Gewässern, in denen Schiffe häufiger gekapert werden. Seeleute werden in Bezug auf Gefahren sensibilisiert und geschult. Zusätzliche Möglichkeiten zur Sicherung von Schiff und Ladung eröffnet das *Internet der Dinge* – theoretisch könnte nicht nur jedes Schiff nahezu nahtlos am Bildschirm überwacht werden, sondern auch die Ladung jedes einzelnen Containers. Auch Regierung und Behörden leisten Unterstützung – beispielsweise die deutsche Marine, die zum Schutz vor den

Küsten patrouillieren kann, um bei Bedarf schnell eingreifen zu können. Damit derartige Interventionen nicht zu politischen Spannung führen, müssen im Vorfeld zwischen den beteiligten Staaten die Motive, Vorhaben und Kompetenzen abgesprochen und die möglichen Interventionen gebilligt werden.

Weiteres Bedrohungspotenzial geht von Hilfsmitteln für den Umschlag und Transport aus. Beispiel Seecontainer: Einmal verschlossen, gibt dieser in der Regel den Inhalt erst wieder beim Empfänger preis. Daher verabschieden die USA im Jahr 2007 ein Gesetz, nach dem Container ab 2012 zu 100 % gescannt werden müssen [90]. Angesichts der hohen Transportmengen, die über Meere und Ozeane befördert werden, ist dies allerdings wenig praktikabel und würde zu Staus in den Häfen führen. Zur Erleichterung der Wirtschaft erfolgt die Umsetzung der Vorgabe nicht wie ursprünglich geplant, sondern wird verschoben – im Jahr 2014 erneut um zwei weitere Jahre [91].

Aufgrund des nicht zu unterschätzenden Bedrohungspotenzials beteiligt sich der Hafen Hamburg an einem Projekt zur Entwicklung einer Alternative zum Scan: die weltweite Einführung eines elektronischen Siegels an allen Containern – basierend auf der RFID-Technik (Radio Frequency Identification Data).

Auch ohne Container-Scan und Siegel erreichen Seehäfen wie beispielsweise der Smart Port Hamburg mittels Gebäude- und Anlagenschutz, leistungsfähiger IT-Lösungen und der konsequenten Weiterbildung der Mitarbeiter bereits ein hohes Sicherheitsniveau [92]. Allerdings ist das Beispiel Hamburg keineswegs globaler Standard.

Exemplarische Übersicht: Sicherheitsvorkehrungen auf Schiffen und in Häfen

- Umsetzung des International Ship and Port Facility Security (ISPS) Codes
- Umwandlung von Hafengebieten und Kaianlagen in (Hoch-)Sicherheitsgebiete mit entsprechendem Schutz
- Beleuchtung des Geländes in den Nachtstunden, Sicherheitsdienste, detektierte Zäune, Video- und Wärmbildkameras, Drohnen
- Abgleich aller Bewerber und Mitarbeiter mit den Personen-Embargo-Listen der EU und der USA
- Chipkarten für Mitarbeiter, Zugang über Drehkreuze, Leibesvisitationen
- Einsatz von Sicherheitsoffizieren im Hafen, in Reedereien und auf Schiffen

- Automatisches Identifikationssystem für Schiffe (AIS)
- Schulung der Mitarbeiter in Bezug auf Sicherheit
- Überprüfung der Frachtsendungen mittels Röntgengeräten, Sprengstoffhunden und Sprengstoffdetektoren
- Schutz der Computer-Systeme vor Cyber-Angriffen
- Dokumentation und Auswertung sicherheitsrelevanter Vorkommnisse
- Gefahrenabwehr- und Contingency-Pläne
- Erfahrungsaustausch und Abstimmung der Sicherheitskonzepte zwischen den verschiedenen Akteuren entlang der Supply Chain

Software-Lösungen und der Einsatz neuer Technologien

80 % der Logistiker haben in einer Umfrage des Logistikmarktforschers Transport Intelligence fehlende Transparenz in der Lieferkette bemängelt. Vor diesem Hintergrund entwickeln Logistik-Dienstleister gemeinsam mit traditionellen IT-Unternehmen wie AEB, Manhattan oder SAP Lösungen, um die Visibility entlang der Supply Chain zu erhöhen. Vermehrt werden Cloud-basierte Systeme eingesetzt, auf die die Zugriffsberechtigten jederzeit und an jedem Ort zugreifen können. Dies ist nicht nur für kleinere und mittlere Unternehmen aufgrund der geringeren Investition, der einfacheren Wartung und Handhabung sowie der höheren Flexibilität interessant, sondern auch für Großkonzerne [93].

Die DHL nutzt *Resilience 360°* – eine Eigenentwicklung, die den Mitarbeitern und internen Teams seit 2014 zur Verfügung steht. Das Tool bietet einen ganzheitlichen Blick auf die Lieferkette – und dies in Fast-Echtzeit. Analysiert werden Bio-Daten, Einschätzungen der DHL-Mitarbeiterinnen und DHL-Mitarbeiter vor Ort sowie Informationen der Rückversicherer und aus den Social-Media-Kanälen. Die sozialen Medien sind ein Frühwarnindikator. In der Regel wird in diesen schneller über Ereignisse berichtet als über traditionelle Kanäle. *Resilience 360°* kann auf Wunsch auch von Kunden der DHL genutzt werden. Zudem soll das Tool künftig auch anderen Interessenten offenstehen.

Neue Dimensionen eröffnet auch hier das *Internet der Dinge*, das heißt das weitgehende Ersetzen des Computers durch intelligente Geräte [94]. Mittels *Internet der Dinge* können durch Sensorentechnologie intelligente Objekte Informationen über Situationen und Sachverhalte – beispielsweise das Öffnen und Schließen von Toren, Türen und Fenstern – aufnehmen, analysieren und weitergeben. So können Lkw, Containerschiffe und Flugzeuge technisch nahezu lückenlos nachverfolgt werden. Der Malaysian-Airlines-Flug MH370 zeigt jedoch, dass die Systeme gewollt oder ungewollt noch Lücken aufweisen [95].

Beginnt das Internet der Dinge selbstständig zu denken, spricht man vom kognitiven Internet der Dinge [96]. Der Einsatz kognitiver Datenverarbeitung ermöglicht, große Mengen strukturierter und unstrukturierter Daten entlang der Supply Chain aufzunehmen, zu verarbeiten und daraus Schlussfolgerungen zu ziehen. Darüber hinaus können mittels Predictive Analytics [97] Aussagen über mögliche zukünftige Situationen und Zustände gemacht werden. Allerdings gibt es auch hier Nebenwirkungen. Da Predictive Analytics nicht auf Kausalität, sondern Korrelation beruht, können beispielsweise Unschuldige kriminelle Muster in ihrem Verhalten aufweisen und unbegründet in Verdacht geraten.

Was E-Commerce-Unternehmen wie Amazon und Paket-Dienstleister wie die Deutsche Post DHL auf dem Lande testen, probt Maersk in der Seeschiffart: Die Reederei hat mit dem Test von Drohnen zur Versorgung der Besatzungen von Schiffen mit kleinen Ersatzteilen, Medikamenten und Post begonnen [98]. Was für den Transport durch die Luft tauglich ist, kann auch zur Unterstützung bei der Überwachung von Betriebsstätten, Häfen, Meerengen und anderem eingesetzt werden. Mit Kameras bestückte autonome Fluggeräte können andere Sicherheitssysteme ergänzen.

Moderne Supply Chains sind ohne leistungsfähige IT-Systeme nicht mehr denkbar – die Steuerung erfolgt heute mittels Tastatur und Bildschirm, wenn nicht gar selbstregulierend im geschlossenen Kreislauf. Der Zugriff auf Daten und Systeme durch Unbefugte kann daher erhebliche Folgen haben. Cyber-Sicherheit ist von immenser Wichtigkeit. Diese erfordert Investitionen in qualifiziertes Personal, kontinuierliche Schulung und externe Experten.

Schutzgemeinschaft entlang der Supply Chain

Die Gewährleistung von Sicherheit entlang der Supply Chain ist nicht nur aufgrund der IT-Systeme, sondern auch wegen der zahlreichen Komponenten, Akteure und Einflussfaktoren ein umfangreiches und komplexes Unterfangen. Sicherheit lässt sich daher am effektivsten und effizientesten kollektiv sicherstellen. Daher wird der Austausch von Informationen und die Zusammenarbeit der Akteure – auch unter Wettbewerbern – im Supply-Chain-Ecosystem immer geläufiger. Diese Kollaboration beschränkt sich nicht auf Wirtschaftsakteure, sondern erstreckt sich auch auf die Zusammenarbeit der Unternehmen mit nationalen und internationalen Behörden.

Aber auch die Behörden untereinander arbeiten in der heutigen vernetzten Welt enger zusammen. So wird Ende 2004 in Berlin das *Gemeinsame Terrorismusabwehrzentrum* (GTAZ) eingerichtet, das sich als Kooperations- und Kommunikationsplattform von 40 nationalen Behörden aus dem Bereich Innere

Sicherheit versteht. An dem Projekt beteiligen sich unter anderem das Bundesamt für Verfassungsschutz, das Bundeskriminalamt, der Bundesnachrichtendienst, der Generalbundesanwalt, die Bundespolizei, das Zollkriminalamt, das Bundesamt für Migration und Flüchtlinge, der Militärische Abschirmdienst, die Landesämter für Verfassungsschutz und die Landeskriminalämter. Mit der *Nachrichtendienstlichen* und der *Polizeilichen Informations- und Analysestelle* (NIAS und PIAS) werden zwei wichtige Säulen geschaffen. Die Behörden arbeiten in verschiedenen Arbeitsgruppen zusammen. Zu den Aufgaben dieser Arbeitsgruppen zählen die Fallbearbeitung sowie das Erstellen von Gefahrenprognosen und mittel- bzw. längerfristigen Analysen. Die Arbeit zeigt Wirkung. Zu den Erfolgen des GTAZ zählt beispielsweise die Verhinderung von Anschlägen durch die sogenannte Sauerland-Gruppe [99].

Zur Schutzgemeinschaft entlang der Supply Chain kann auch die *Schutz- und Aktionsgemeinschaft zur Erhöhung der Sicherheit in der Spedition* (s. a. f. e.), eine Initiative des Deutschen Speditions- und Logistikverbands, gezählt werden. Dabei geht es in erster Linie um die gemeinsame Bekämpfung von Diebstählen.

Das Restrisiko absichern

Trotz aller Vorkehrungen bleibt ein Restrisiko. Um dieses abzudecken, schauen die Unternehmen auf die Versicherer. Dies insbesondere in Anbetracht der weitreichenden potenziellen finanziellen Folgen, die bei einem Anschlag und einer daraus resultierenden Störung oder Unterbrechung der Supply Chain drohen. Da reichen die eigenen Mittel – insbesondere von kleinen und mittleren Unternehmen – u. U. zur Deckung nicht aus.

Zudem wird die Terrorgefahr nach den Anschlägen in New York 2001 weltweit aus den Sach- und Berufsunfähigkeits-Deckungen ausgeschlossen. Infolgedessen entstehen in einzelnen Ländern Spezialversicherer. In Deutschland deckt seit 2002 die auf Initiative der Versicherungswirtschaft gegründete *Extremus Versicherungs-AG* das Risiko terroristischer Anschläge, sofern diese in Deutschland erfolgen – eine Einschränkung, die in der auf Deutschland beschränkten Staatsgarantie begründet liegt. Seit 2005 arbeitet der Spezialversicherer international mit Kooperationspartnern zusammen, so dass auch die Risiken der globalen Lieferkette abgesichert werden können [100].

Als Ergänzung sichern sich immer mehr Unternehmen gegen terroristisch motivierte Entführungen von Mitarbeitern im Ausland sowie Erpressung, Cyber-Attacken und Sabotagehandlungen ab – dies infolge der Zunahme der Gefahr von Wirtschaftsspionage durch Unternehmen und Staaten [101].

2.3 Spezielle Vorschriften und Initiativen

Um die Sicherheit entlang der Supply Chain zu gewährleisten, gibt es zahlreiche Vorschriften und Initiativen. Nachstehend einige Beispiele.

Im Seeverkehr gelten seit Juli 2004 umfangreiche, von der Internationalen Schifffahrtsorganisation (IMO), einer Sonderorganisation der Vereinten Nationen, erarbeitete Sicherheitsmaßnahmen zur Verbesserung der Abwehr von Bedrohungen – beispielsweise der International Ship and Port Facility Security (ISPS) Code. Anwendung findet der ISPS-Code bei Frachtschiffen mit einer Tonnage ab 500 Bruttoraumzahl (BRZ), Fahrgastschiffen in internationaler Fahrt sowie bei Hafenanlagen, an denen diese Schiffe abgefertigt werden. Jedes dieser Schiffe muss einen von der Verwaltung genehmigten Gefahrenabwehrplan an Bord mitführen. Dieser beschreibt die Maßnahmen, die im Ernstfall zu ergreifen sind [102]. Des Weiteren gibt es die EU-Verordnungen 725/2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen [103] und 2005/65/EG zur Verbesserung der Gefahrenabwehr in Häfen [104] sowie das *Übereinkommen zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Seeschifffahrt* (engl. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, kurz SUA). Mit dieser Konvention, die im Zuständigkeitsbereich der IMO liegt, verpflichten sich die unterzeichnenden Staaten, jedes Verhalten, das die Sicherheit der Seeschifffahrt bedroht, zu untersagen und zu sanktionieren.

Zudem etabliert die Initiative *The Common Information Sharing Environment (CISE)* der Europäischen Kommission Richtlinien für die kooperative Überwachung der maritimen Wirtschaft. Zur Realisierung des CISE wurden sechs fundamentale Schritte identifiziert: Feststellung aller Nutzer Gemeinschaften (unter Berücksichtigung des ISPS Codes); Mapping der Daten und Gap-Analyse sowie Feststellung, welche Daten verfügbar sind, aber noch nicht ausgetauscht werden; Identifikation gemeinsamer Datenklassifizierungsebenen: Entwicklung eines technischen Rahmenwerkes – basierend auf dem Konzept eines Netzwerkes aus verknüpften bestehenden Systemen; Bestimmung der Zugangsrechte sowie die Einhaltung der rechtlichen Gegebenheiten. Ziel ist, das CISE bis 2020 einzuführen [105].

Eine den Seeverkehr betreffende Maßnahme, die von den USA ergriffen wird, ist das bereits erwähnte Gesetz zur 100 %igen Containerdurchleuchtung (Public Law 110–53, Implementing the 9/11 Commission Recommendations Act of 2007). Nach diesem Gesetz sollte ab 2012 jeder Container, der in die USA verschifft wird oder diese beim Transport berührt, im Abgangshafen auf Kosten des

Absenderlandes vollständig durchleuchtet werden [106]. Diese Regelung wird mehrfach verschoben und ist somit bis heute noch nicht in Kraft getreten. Die Einführung würde wahrscheinlich zu Staus und Verzögerungen in den Häfen führen.

Die Sicherheit der maritimen Wirtschaft wird auch auf höchster Ebene diskutiert, so beispielsweise im April 2015 auf der G7-Konferenz in Lübeck. Das Ergebnis der Diskussion ist in der *G7 Foreign Ministers*' *Declaration on Maritime Security* zusammengefasst [107].

Im Luftverkehr bestehen traditionell strikte Sicherheitsvorschriften. Relevant für die Sicherheit der Lieferkette sind die EG-Luftsicherheitsverordnungen Nr. 300/2008 und Nr. 2320/2002. Im Jahre 2003 hat die EU zudem die Verordnung (EG) Nr. 1217/2003 zur Festlegung gemeinsamer Spezifikationen für nationale Qualitätskontrollprogramme für die Sicherheit der Zivilluftfahrt erlassen. Zu den weiteren Regelungen im Bereich der Sicherheitsvorschriften zählen das Luftsicherheitsgesetz (LuftSiG), das Luftverkehrsgesetz (LuftVG) und die Luftsicherheits-Schulungsverordnung (LuftSiSchulV) [108].

Des Weiteren dienen in Deutschland u. a. das Außenwirtschaftsgesetz, das Geldwäschebekämpfungsgesetz sowie die Sicherungsbestimmungen für Gefahrguttransporte dem Schutz der Supply Chain.

Auf europäischer Ebene zählt die Richtlinie 114/2008/EG zum Schutz europäischer kritischer Infrastrukturen zu den relevanten Vorschriften. Konkret geht es dabei um Infrastrukturen, bei denen durch eine gravierende Beeinträchtigung aufgrund terroristischer Anschläge die Grundversorgung der Bevölkerung gefährdet ist – und dies in mindestens zwei europäischen Ländern [109]. Dementsprechend zählen sowohl der Duisburger Binnenhafen als auch der Hamburger Hafen zu den europäischen kritischen Infrastrukturen.

Ergänzt werden die vorgenannten Sicherheitsvorschriften durch die geltenden Sicherheits-Initiativen der Wirtschaft wie ISO/PAS 28000 ff. – eine globale Norm bzw. ein Management-System. Zur Erhöhung der Sicherheit werden die Prozesse abgebildet und vereinheitlicht. Dies entspricht der Idee der Supply Chain Map. Anforderungen an Technik oder physische Sicherungseinrichtungen werden in dieser Norm nicht gestellt. Seit 1997 besteht zudem die *Transport Asset Protection Association (TAPA)*, die heute mehr als 600 Mitglieder zählt. Sie hat verschiedene Standards entwickelt, um die Sicherheitsbedrohungen innerhalb der internationalen Lieferketten zu reduzieren [110].

2.4 Aufklärung und Abwehr im digitalen Zeitalter

Die Prävention ist das ultimative Ziel der Sicherheitsstrategien. Im Jahr 2007 wird in Deutschland auf nationaler Ebene und nach dem Vorbild des *Gemeinsamen Terrorismusabwehrzentrums* (GTAZ) das *Gemeinsame Internetzentrum* (GIZ) eingerichtet. Hier arbeiten Vertreter des Bundesamtes für Verfassungsschutz, des Bundeskriminalamtes, des Bundesnachrichtendienstes, des Amtes für den Militärischen Abschirmdienst und der Generalbundesanwaltschaft zusammen. Gemeinsam beobachten und analysieren sie Veröffentlichungen mit radikalen Inhalten im Internet. Ziel ist es dabei, frühzeitig extremistische und terroristische Strukturen und Aktivitäten zu erkennen und zeitnah an die Entscheider zu berichten, um Anschläge zu verhindern oder bei Bedarf ein rasches Eingreifen zu ermöglichen [111].

Auch Organisationen wie beispielsweise *Search for International Terrorist Entities* [112] sammeln Daten und Informationen, werten diese aus und stellen sie den Geheimdiensten zur Verfügung. Die Geheimdienste sind im Bereich Internet ebenfalls aktiv. So soll das FBI mit Hilfe des Internet-Überwachungsprogramms *Carnivore* E-Mails von *al-Qaida*-Terroristen abgefangen haben. Durch diverse Trojaner auf den Computern der Terroristen sollen so mehrfach Anschläge verhindert worden sein [113]. Die Behörden können – je nach eingesetzter Technologie – bereits bei der Eingabe der Informationen auf dem Computer mitlesen. Möglich machen dies Keyboard Logging Systems (KLS). Diese zeichnen die Tastatureingaben auf und leiten diese in Echtzeit weiter [114]. Zusammen mit klassischen Ermittlungsmethoden dienen diese Tools der Aufklärung und Verhinderung terroristischer Anschläge im digitalen Zeitalter.

Auch Interpol engagiert sich in der Abwehr. Die Behörde sammelt, analysiert und speichert Informationen über verdächtige Personen und Terrorgruppen. Die Informationen und Hinweise werden mit den Mitgliedsländern über ein eigenes, sicheres globales Kommunikationsnetz ausgetauscht. Seit 2002 ist die *Fusion Task Force* (FTF) der Interpol aktiv. Sie verfolgt einen interdisziplinären Ansatz, um die Mitglieder internationaler Terrorgruppen zu identifizieren und ihre Beteiligung an Terrorakten nachzuweisen. Regionale Arbeitsgruppen des globalen Netzwerks bestehen in den Regionen Mittlerer Osten und Nordafrika, Süd- und Mittelamerika, Afrika, Zentral- und Südasien, Südost-Asien und Pazifik-Inseln sowie in Europa [115].

Terrorbekämpfung zählt auch zu den Prioritäten der Europol. Die europäische Polizeibehörde mit Sitz in Den Haag koordiniert die Arbeit der nationalen Polizeibehörden Europas in Bezug auf die grenzüberschreitende

Kriminalitätsbekämpfung und fördert den Informationsaustausch zwischen den einzelnen Behörden. Europol veröffentlicht einmal jährlich den *European Terrorism Situation & Trend Report* (TE-SAT). Der Report enthält Daten über terroristische Aktivitäten in der Europäischen Union, aber auch Analysen für die Polizeikräfte der Länder. Im Bericht werden die verschiedenen terroristischen Gruppierungen, beispielsweise Separatisten, durchleuchtet und Angaben, beispielsweise zu Altersstrukturen oder Anzahl der Festnahmen, gemacht [116]. Europol arbeitet mit Interpol zusammen. Mit den USA wird 2001 eine Vereinbarung zur strategischen und technischen Kooperation geschlossen. 2002 folgt ein Abkommen auf operativer Ebene. Dieses erlaubt den Austausch personenbezogener Daten – ein wichtiger Schritt für die grenzüberschreitende Präventionsarbeit [117].

Viele Staaten kooperieren auf dem Gebiet der Abwehr. So tauscht die EU mit arabischen Staaten Geheimdienstinformationen aus und sendet Sicherheitsexperten zum Zwecke des Erfahrungsaustausches in ausländische EU-Vertretungen [118]. Der Austausch von Daten ermöglicht beispielsweise die Analyse von Bewegungsmustern und das Erkennen von Gruppenzugehörigkeiten. Dadurch lassen sich Entwicklungen erkennen und somit Anschläge verhindern.

http://www.springer.com/978-3-658-14687-0

Steht unsere Versorgung auf dem Spiel?
Über terroristische Bedrohungen entlang der Supply Chain

Lehmacher, W.

2017, IX, 58 S., Softcover
ISBN: 978-3-658-14687-0