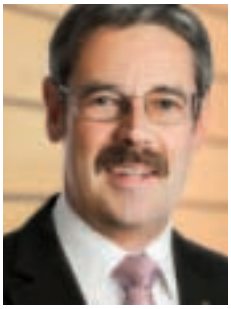
CYBERSICHERHEIT IN ÖSTERREICH

Risikopotenziale und Handlungserfordernisse am Beispiel ausgewählter Infrastruktursektoren

KURATORIUM SICHERES ÖSTERREICH

VORWORT



KSÖ-Präsident Mag. Erwin Hameseder

Die Relevanz des Themas Cybersicherheit steigt täglich. In Europa entsteht laut Interpol durch Cyberkriminalität inzwischen ein Schaden von 750 Milliarden Euro pro Jahr. Cyberbetrug wird inzwischen wie der Drogenhandel im großen Stil von internationalen Banden organisiert. Zum Vergleich: Amerikanische Banken haben im vergangenen Jahr 900 Millionen Dollar (691 Mio. Euro) durch herkömmliche Diebe verloren, aber rund zwölf Milliarden Dollar durch Cyberkriminelle.

Als Industrie- und Dienstleistungsstandort steht Österreich im internationalen Wettbewerb. Investitionen in die Informations- und Kommunikationstechnologie leisten einen entscheidenden Beitrag, um in der digitalen Ökonomie Schritt zu halten. Der Einsatz von Informations- und Kommunikationstechnologie verschafft unseren Unternehmen Effizienzgewinne und lässt neue Märkte entstehen: E-Mobility, intelligente Netze und digitales Gesundheitswesen sind nur einige der Stichworte, die ich in diesem Zusammenhang nennen möchte.

Je mehr wir die Entwicklungschancen unserer Wirtschaft und damit auch unserer Bürgerinnen und Bürger an den Einsatz von Informations- und Kommunikationstechnologie knüpfen, desto stärker müssen wir uns gleichzeitig mit der Sicherheit der entsprechenden Anwendungen beschäftigen. Deshalb ist Cybersicherheit auch für die Attraktivität und die Wettbewerbsfähigkeit Österreichs von entscheidender Bedeutung. Als Präsident des KSÖ habe ich mich daher gemeinsam mit KSÖ-Generalsekretär Christian Kunstmann seit letztem Herbst aktiv darum bemüht, dass wir zusammen mit unseren staatlichen Partnern einen Prozess anstoßen, der konkrete Impulse setzt, um Österreich „cybersicherer“ zu machen. Eine wichtige Basis für alle weiteren Schritte bildet der vorliegende Bericht zur Cyberrisikoanalyse für Österreich.

Es ist ein Kernanliegen des KSÖ, die Zusammenarbeit zwischen Staat und Wirtschaft im Bereich der Cybersicherheit zu verbessern. Mit Vorlage der Cyberrisikoanalyse für Österreich und den daraus abgeleiteten Handlungserfordernissen tritt der gesamte Prozess in eine neue Phase ein, in der basierend auf einer fundierten Analyse Handlungserfordernisse geprüft und konkrete Handlungsstränge verfolgt werden können.

Ich bin davon überzeugt, dass die staatliche und die unternehmerische Sicherheitsvorsorge durch Informationen des jeweils anderen Partners erstens zur Risikoanalyse und -bewertung, zweitens zu konkreten Sicherheitsstrategien und drittens zu vorhandenen sicherheitsrelevanten Fähigkeiten wesentlich verbessert werden können. Das KSÖ will als Kompetenzzentrum in Zukunft dazu beitragen, diesen Informationsaustausch systematisch zu gestalten.

Die Sicherheit im Cyberspace und die Sicherheit der Menschen im Cyberspace sind ein Rechtsgut, das mit allen rechtsstaatlichen Mitteln geschützt werden muss. Cyberattacken finden zwar virtuell statt, haben aber höchst reale Auswirkungen auf unsere Sicherheit sowie das Funktionieren von Staat, Wirtschaft und Gesellschaft. Die Anzahl der Angriffe steigt rasant, der angerichtete Schaden geht weltweit jährlich in Milliardenhöhe.
Um sich bestmöglich dagegen zu wappnen, bedarf es eines umfassenden gesamtstaatlichen Konzepts zum Schutz des Cyberspace und der Menschen im virtuellen Raum. Mitte Mai 2012 hat die österreichische Bundesregierung daher den Beschluss gefasst, bis Ende 2012 eine nationale Cybersicherheitsstrategie vorzubereiten.
Eine nationale Cyberstrategie kann aber nicht im Elfenbeinturm entwickelt werden; vielmehr braucht man dazu die Erfahrungen und das Know-how von möglichst vielen ExpertInnen und Betroffenen aus unterschiedlichsten Bereichen. Daher wurde innerhalb der KSÖ-Cybersecurity-Initiative unter Mitwirkung von VertreterInnen aus dem Behördensektor und aus Sektoren kritischer Infrastruktur die vorliegende Cyberrisikoanalyse für Österreich durchgeführt. Damit wurde eine ganz wichtige Basis für die Entwicklung einer nationalen Cybersicherheitsstrategie gelegt.
Aus den Ergebnissen der Analyse wurden konkrete Handlungserfordernisse abgeleitet, die ich als Sicherheitsministerin auf jeden Fall begrüße.
Ein bereits nächster Schritt, dessen Aufgabenstellung aus der Risikoanalyse abgeleitet wurde, war das Cybersecurity-Planspiel am 12. Juni 2012, das in seiner Dimension bisher einzigartig ist. Erstmals wurden VertreterInnen aus der Wirtschaft, der Politik und von Behörden in einem Szenario vereint, um gemeinsam an einem Strang zu ziehen und konkrete Handlungserfordernisse aus der Risikoanalyse zu überprüfen.
Diese Art von Planspiel ist eine einzigartige Chance für eine neue Form des Dialogs zwischen allen AkteurInnen, die wir brauchen, um die benötigten Spielregeln zu definieren. Damit haben wir eine ganz neue Qualität in der Zusammenführung und Kooperation der ExpertInnen aus den unterschiedlichsten Bereichen erreicht.
Unsere Erfahrungen unterstreichen den Stellenwert und den Mehrwert einer unabhängigen Plattform, wie sie das KSÖ darstellt, als Vermittler zwischen den verschiedenen Welten. Ich möchte mich an dieser Stelle daher ganz herzlich beim KSÖ bedanken und würde es sehr begrüßen, wenn das Kuratorium Sicheres Österreich auch in Zukunft die verantwortungs-volle Rolle, hier als zentrale Informationsplattform zu agieren, wahrnehmen würde.

© Alexander TUMA

Innenministerin Mag.a
Johanna Mikl-Leitner

Cyberrisiken und Österreichs Energiesektor 28

Cyberrisiken und Österreichs Finanzsektor 40

Cyberrisiken und Österreichs IKT-Sektor 50

1. Zusammenfassung 6

2. Cyberrisikolandschaft Österreich: Übersicht 15

3. Cyberrisiken und Österreichs Energiesektor 28
3.1. Österreichs Energiesektor: Relevanz in Zahlen 29
3.2. Cyberrisiken im Energiesektor: Allgemeine Bewertung und Trends 30
3.3. Cyberrisiken im Energiesektor: Österreichische Bewertung 34

4. Cyberrisiken und Österreichs Finanzsektor 40
4.1. Österreichs Finanzsektor: Relevanz in Zahlen 41
4.2. Cyberrisiken im Finanzsektor: Allgemeine Bewertung und Trends 42
4.3. Cyberrisiken im Finanzsektor: Österreichische Bewertung 45

5. Cyberrisiken und Österreichs IKT-Sektor 50
5.1. Österreichs IKT-Sektor: Relevanz in Zahlen 51
5.2. Cyberrisiken im IKT-Sektor: Allgemeine Bewertung und Trends 52
5.3. Cyberrisiken im IKT-Sektor: Österreichische Bewertung 57

6. Cyberrisiken und Österreichs Transportsektor 62
6.1. Österreichs Transportsektor: Relevanz in Zahlen 63
6.2. Cyberrisiken im Transportsektor: Allgemeine Bewertung und Trends 64
6.3. Cyberrisiken im Transportsektor: Österreichische Bewertung 68

7. Cyberrisiken und Österreichs Behördensektor 74
7.1. Österreichs Behördensektor: Relevanz in Zahlen 75
7.2. Cyberrisiken im Behördensektor: Allgemeine Bewertung und Trends 76
7.3. Cyberrisiken im Behördensektor: Österreichische Bewertung 80

8. Handlungserfordernisse 86
8.1. Bewusstsein für Cyberrisiken fördern und Nutzer qualifizieren 88
8.2. Aktuelle und künftige Cyberrisiken erkennen, verstehen und bewerten 91
8.3. Zusammenarbeit im Umgang mit Cyberrisiken systematisch organisieren 94
8.4. Cyberrisikoprävention stärken 98
8.5. Cybersicherheit mit Verhaltensanreizen fördern 100

9. Anhang 104
9.1. Abbildungs- und Tabellenverzeichnis 105
9.2. Interviewpartner 106
9.3. Literatur 108
9.4. Glossar 116
9.5. Autorenhinweise 122

Cyberrisiken und Österreichs Transportsektor 62

Cyberrisiken und Österreichs Behördensektor 74

Handlungserfordernisse 86

IMPRESSUM:
KSÖ - Kuratorium Sicheres Österreich
Generalsekretär Christian Kunstmann
Herrengasse 7, Postfach 100, A-1014 Wien
Email: kunstmann@dasmachichsicher.at
ZVR-Zahl: 444 913 001

DRUCK: BM.I

FOTOS: Kuratorium Sicheres Österreich
Bundesministerium für Inneres

GRAFIK: creativedirector.cc lachmair gmbh.

Cobyright © 2012 BM.I

ZUSAMMENFASSUNG

© violetkaipa – Fotolia.com

1

Zielsetzung

- Aufbauend auf der im September 2011 vorgestellten Cyberrisikomatrix des Kuratoriums Sicheres Österreich zeigt die vorliegende Ausarbeitung auf, wie relevant die in der Matrix dargestellten Cyberrisiken aus der Sicht ausgewählter Vertreter verschiedener strategischer Infrastruktursektoren in Österreich sind. Soweit aufgrund der Interviews verfügbar, wurde der Stand der Sicherheitsvorsorge durch Unternehmen und Behörden ebenfalls beachtet.
- Zusätzlich zeigt die Studie auf, wie vorhandene Defizite in der Erkennung, der Abwehr und der Bewältigung von Cyberrisiken in Österreich überwunden und vorhandene Stärken ausgebaut werden können.

Vorgehen

- Die Studienergebnisse wurden in Zusammenarbeit mit Expertinnen und Experten aus strategisch relevanten Infrastruktursektoren Österreichs erarbeitet. Der Schwerpunkt lag dabei auf dem Energie-, Finanz-, Informations- und Kommunikationstechnologie (IKT) sowie Transport- und Behördensektor.
- Die erste Gesprächsrunde diente der vertieften Risikobewertung aus der jeweiligen Sektorperspektive. In der zweiten Runde wurden künftige Handlungserfordernisse für Österreich diskutiert. Die erste Interviewrunde umfasste 31 Interviews mit 55 Gesprächspartnern, die zweite Runde 26 Interviews mit 45 Gesprächspartnern. Alle Gespräche wurden schriftlich protokolliert.
- Darüber hinaus wurde für die in einem Fünf-Punkte-Programm zusammengefassten Handlungserfordernisse (Kapitel 8) ein elektronisches Konsultationsverfahren durchgeführt. Von mehr als 500 eingeladenen Teilnehmerinnen und Teilnehmern beteiligten sich 155 an der Konsultation und gaben knapp 4.300 Stimmen sowie gut 170 Kommentare ab.

Wichtige Ergebnisse im Überblick

- Die vorliegende Studie stellt eine grundsätzliche Risikopotenzialanalyse, nicht eine konkrete Bedrohungsanalyse dar. Daher sind die Studienergebnisse vorsichtig zu interpretieren. Wenn in der Folge ein Risiko für einen strategisch bedeutenden Infrastruktursektor als relevant betrachtet wird, dann ist das eine allgemeine Aussage aus Sicht aller befragten Expertinnen und Experten. Ob und in welchem Umfang ein einzelner Infrastrukturbetreiber sowie die Verfügbarkeit seiner Leistungen von einem Risiko tatsächlich betroffen sind, kann nur in einer konkreten Einzelfallbetrachtung ermittelt werden, die nicht Gegenstand der Untersuchung war. Insofern beschreiben die Ergebnisse tendenzielle Gefährdungen und keine konkreten Bedrohungen einzelner Sektoren.

- Auf den ersten fünf Plätzen der besonders relevanten Risikokategorien[1] liegen aus Sicht der Gesprächspartner die potenziellen Risiken manipulierter IKT-Systeme der Energieerzeugung und -versorgung, Cybercrime, Social Engineering, fahrlässiges Verhalten in strategischen Infrastrukturbetrieben und mangelndes Sicherheitsbewusstsein. Diese Ergebnisse zeigen, wie wichtig aus Sicht der Experten der Faktor Mensch ist. Die Experten lassen damit keinen Zweifel daran, dass alle Bemühungen im Bereich der Cybersicherheit mit der Expertise der Mitarbeitenden – und in weiterer Folge aller IKT-Nutzer – stehen und fallen.
- Dass sektorübergreifende Abhängigkeiten durch den allgegenwärtigen Einsatz von IKT verstärkt werden, kommt in der Beurteilung ebenfalls deutlich zum Ausdruck. Stellvertretend dafür steht an erster Stelle das potenzielle Risiko, das mit der Manipulation von IKT-Systemen der Energieerzeugung und -versorgung verbunden ist. Im Zusammenhang mit den sektorübergreifenden Abhängigkeiten ist auch die hohe Relevanz potenziell fehlender unternehmerischer Notfallvorsorge (Business Continuity Management, BCM) zu erwähnen. Dabei sehen die Experten vor allem bei sektorübergreifenden BCM-Anstrengungen einen entsprechenden Handlungsbedarf.
- Mit Blick auf die technischen Risikokategorien sehen die Befragten die hauptsächlichen Risiken in den inhärenten Schwächen und Qualitätsmängeln der eingesetzten Hard- und Softwareprodukte. Dafür stehen Risikokategorien wie fehlerhafte bzw. inkompatible Codes und Software, geknackte digitale Schlüsselsysteme sowie nicht erkannte (IKT-)Anomalien.
- Während sich die Befragten bei der hohen Relevanz der Cyberkriminalität (Durchschnittswert 2,95) und der Cyberspionage (2,68) einig sind, gehen die Meinungen bezüglich der Relevanz des Cyberterrorismus (2,50) und des Cyberwar (2,32) auseinander. Vor allem bei der Gefahr des Cyberwar zeigte sich ein markanter Unterschied zwischen der Einschätzung der privatwirtschaftlichen Vertreter und den Experten der Behörden. Diese Feststellung deutet auf Wahrnehmungsdifferenzen hin und verdeutlicht einen entsprechenden Diskussionsbedarf, um zu vermeiden, dass Unterschiede in der Risikobewertung zu divergierenden Sicherheitsmaßnahmen führen.

Bewertung der Experten des Energiesektors

- Mit potenziell unsicheren Steuerungssystemen und der möglichen Gefährdung durch manipulierte IKT-Systeme rücken die Gesprächspartner des Energiesektors zwei Top-Cyberrisiken in den Mittelpunkt ihrer Risikobetrachtung. Die Energieexperten sprechen damit zwei Risikokategorien an, die gerade für die Betrachtung der Abhängigkeit anderer strategischer Infrastruktursektoren von der Energieversorgung große Bedeutung haben.

„Die hohe Relevanz der Cyberkriminalität ist ein Spiegel der aktuellen Gefährdungslage.“

- Die Energieexperten bewerten die Phänomene Cyberwar und Cyberterrorismus als hochrelevant. Dies ist Ausdruck der Betroffenheit des Sektors beispielsweise im Falle der flächendeckenden Lahmlegung des Internet als mögliches Ziel eines kriegerischen oder terroristischen Angriffs im Informationsraum.
- Auffällig ist zudem, dass die Gesprächspartner mögliche Lücken in der präventiven Sicherheit als sehr relevant erachten, was in der Betonung von Risiken wie dem fahrlässigen Verhalten in strategisch relevanten Infrastrukturbetrieben, fehlenden bzw. nicht aktuellen rechtlichen Grundlagen (z.B. mit Blick auf das Risikopotenzial neuer Technologien) oder einer nicht systematischen Technologiefolgeabschätzung zum Ausdruck kommt.

Bewertung der Experten des Finanzsektors

- Ähnlich wie im Energiesektor steht die Sorge um die Gefährdung der eigenen Geschäftsprozesse der Finanz- und Versicherungsdienstleister an der Spitze der als relevant erachteten Cyberrisiken. Daher werden die potenziellen Risiken manipulierter IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen sowie geknackter digitaler Schlüsselsysteme als besonders relevant erachtet.
- In dieses Bild passt auch der hohe Stellenwert, den der Finanzsektor der systematischen Technologiefolgenabschätzung einräumt, weil das eigene Geschäftsmodell unmittelbar von der Sicherheit und Funktionsfähigkeit neuer Technologien abhängt (Stichworte: E-Banking, Mobile Banking).
- Die hohe Relevanz der Cyberkriminalität ist ein Spiegel der aktuellen Gefährdungslage.

Bewertung der Experten des IKT-Sektors

- Auch die IKT-Experten erachten die Rolle des Menschen im Umgang mit IKT als besonders wichtig. Risiken, die mit fehlendem Fachpersonal und mangelndem Sicherheitsbewusstsein einhergehen, erhielten von den IKT-Experten die höchste Bewertung.
- Ebenfalls deutlich stärker als die übrigen Experten betonen die IKT-Fachleute die sektorübergreifenden Abhängigkeiten. Das Risiko fahrlässigen Handelns erhält von ihnen mit deutlichem Abstand die Höchstnote aller bewerteten Cyberrisiken. Auch die Relevanz fehlender bzw. unzureichender unternehmerischer Notfallvorsorge (BCM) wird von den Gesprächspartnern des IKT-Sektors stärker gewichtet als von den anderen Interviewpartnern. Das mag mit der besonderen Sensibilität für die unterneh-

1 Bewertet wurde anhand einer Relevanzskala von 1 (sehr niedrig) bis 4 (sehr hoch). Bei den Ergebnissen handelt es sich um Durchschnittswerte.

„Lösungen zur Verbesserung der Cybersicherheit eröffnen österreichischen Unternehmen und Instituten neue Marktchancen.“

© Srebrina Yaneva – iStockphoto.com

mensweiten und sektorübergreifenden Folgen der IKT-Störung bzw. des IKT-Ausfalls zusammenhängen.

- Ausdruck der Risiken für die eigenen Geschäftsprozesse durch technische Gefährdungen sind die als hochrelevant eingestuften Risikokategorien fehlerhafter bzw. inkompatibler Codes/Software, manipulierte Kommunikations- und Satellitenverbindungen, geknackte digitale Schlüsselsysteme und unsichere Steuerungsinstrumente. Dass die IKT-Unternehmen schließlich auch attraktive Ziele für Cyberspionage und Cyberkriminelle darstellen, verdeutlicht die entsprechende Bewertung dieser beiden Risiken. Auffällig ist dabei, dass das Risiko der Cyberspionage von den IKT-Experten deutlich höher bewertet wird als von den anderen privatwirtschaftlichen Gesprächspartnern.

Bewertung der Experten des Transportsektors

- Auch die Experten des Transportsektors messen der sektorübergreifenden Abhängigkeit hohe Bedeutung bei. Dementsprechend wird das Risikopotenzial einer potenziellen Manipulation der IKT-Systeme in der Energieerzeugung und -versorgung sogar noch höher bewertet als die eigene Abhängigkeit von IKT-Systemen. Damit einher geht auch die hohe Relevanz der Gefahr fahrlässigen Verhaltens in strategischen Infrastrukturbetrieben, deren Bedeutung als Sicherheitsrisiko nur im IKT-Sektor noch höher bewertet wird.
- Aufgrund des physischen Umfeldes, das den Transportsektor prägt, haben die Experten in diesem Bereich auch ein besonderes Bewusstsein für Naturgefahren entwickelt, die die Funktionsfähigkeit der IKT- und der Transportinfrastruktur gefährden können. Risiken für die IKT-Infrastruktur als Folge von Naturgefahren erhalten von den Transportexperten die höchste Bewertung aller Befragten.
- Schließlich spielt der Faktor Mensch auch in der Bewertung der Transportexperten eine wichtige Rolle, die in der hohen Gewichtung der Risikokriterien fehlendes Fachpersonal, Social Engineering und mangelndes Sicherheitsbewusstsein zum Ausdruck kommt.

Bewertung der Experten des Behördensektors

- Die Behördenvertreter sind sich der eigenen Verwundbarkeit staatlicher IKT-Systeme durch Cyberrisiken sehr genau bewusst. Das zeigt sich an der Bewertung der Risikofaktoren Social Engineering, Cybercrime und Cyberspionage in Verbindung mit der Gefahr des Diebstahls bzw. der Manipulation digitaler Identitäten und Bürgerdaten. Cybercrime und Cyberspionage dürften auch deshalb so hoch eingestuft worden sein, weil die Behördenvertreter in ihrer Zuständigkeit für die gesamtstaatliche Gefahrenabwehr und die öffentliche Sicherheit für die Minimierung dieser Risiken zuständig sind.
- In der Bewertung der Behördenvertreter zeigen sich aber auch Unterschiede. Diese erklären sich zum einen aus der Grundaufgabe der Behördenvertreter und damit auch der Rolle der IKT. Zum anderen ist relevant, ob die Behörden in direktem Kontakt mit Bürgerinnen und Bürgern sowie Unternehmen stehen und dazu beispielsweise auf internetgestützte Dienste zurückgreifen. In diesem Fall ist die Betroffenheit bei Ausfall der entsprechenden Dienste entsprechend höher.
- Zusätzlich kommt in den Antworten der Behördenexperten die Sorge um die Abhängigkeiten zwischen verschiedenen Infrastruktursektoren zum Ausdruck, was sich in der Bewertung potenziell manipulierter IKT-Systeme in den Sektoren Energie, Verkehr, Kommunikation und Finanzen niederschlägt.

Handlungserfordernisse

Bewusstsein für Cyberrisiken fördern und Nutzer qualifizieren

- Erforderlich ist erstens ein Kommunikationsansatz, der Cyberrisiken auf der einen und die von den österreichischen Behörden und Unternehmen ergriffenen Schutz- und Abwehrmaßnahmen auf der anderen Seite ausgewogen zum Ausdruck bringt. Gleichzeitig sollte dieser Ansatz verstärkt betonen, dass Lösungen für die Cybersicherheit den österreichischen Unterneh-

men und wissenschaftlichen Einrichtungen auch neue Marktchancen eröffnen können.

- Zweitens geht es darum, junge Anwender für die Risiken im Cyberspace zu sensibilisieren, z.B. indem die Lehrpläne der verschiedenen Unterrichtsstufen entsprechend ergänzt werden.
- Drittens wäre es sinnvoll, sektorspezifische und sektorübergreifende Initiativen zum Umgang mit sozialen Medien bei strategisch bedeutenden Infrastrukturbetreibern zu lancieren. Einzelne Unternehmen könnten hierbei als Good-Practice-Beispiele genutzt werden und ihre Erfahrungen weitergeben.
- Viertens sollten die IKT-Sicherheitsbedürfnisse der kleinen und mittelgroßen Unternehmen (KMU) speziell beachtet werden. Österreichische Großunternehmen, Verbände und die Wirtschaftskammern könnten diese mit gezielten Initiativen unterstützen.
- Fünftens sollte auch berücksichtigt werden, dass Verbraucherinnen und Verbraucher immer stärker in die betrieblichen Abläufe der Unternehmen eingebunden werden (z.B. Online-Banking). Damit spielen sie auch eine größere Rolle, wenn es um die Sicherheit der entsprechenden Prozesse geht, und sollten dafür sensibilisiert werden.
- Sechstens sollte Sensibilisierung einhergehen mit verstärkten Anstrengungen im Bereich der Aus- und Weiterbildung für IKT-Sicherheit. Vor allem zur Vermittlung sektorübergreifender Lerninhalte könnten Expertise und Finanzmittel gebündelt und gemeinsam eingesetzt werden. Ebenso sollte der Personalaustausch zwischen Behörden und den strategisch wichtigen Infrastrukturbetreibern zur Förderung der IKT-Sicherheit verstärkt werden.

Aktuelle und künftige Cyberrisiken erkennen, verstehen und bewerten

- Erstens sollten Informationen der Behörden und der Unternehmen zur Bewertung von Cyberrisiken systematisch an einer Stelle gebündelt, aufbereitet und verteilt werden. Eine entsprechende Organisationseinheit sollte neben der Lagedarstellung auch die Warnung, die Aufklärung, die Strafverfolgung und die Ereignisauswertung unterstützen.
- Zweitens sind für die Umsetzung verschiedene Aspekte zu klären. Dazu zählen das Verhältnis zwischen Risikomanagement und Krisenmanagement, die organisatorische Eingliederung einer solchen Einheit sowie die Frage, welche Akteure als Lieferanten und Bezieher von Informationen beteiligt werden sollten. Ein Schalenmodell, das verschiedene Akteursgruppen anhand ihrer Relevanz für die nationale Sicherheitsvorsorge unterscheidet, ist hilfreich.

Zusammenarbeit im Umgang mit Cyberrisiken systematisch organisieren

- Österreichs Cybersicherheitsarchitektur sollte erstens partnerschaftlich aufgebaut sein und den staatlichen bzw. privatwirtschaftlichen Akteuren klare Rollen, Aufgaben und Verantwortlichkeiten zuweisen. Dabei ist es wichtig, die Zusammenarbeit umfassend zu definieren und die Aspekte der Risikoanalyse sowie Früherkennung genauso zu berücksichtigen wie die Strategiedefinition, die Krisenprävention, das Krisenmanagement und die Krisennachsorge sowie die Zusammenarbeit in unterstützenden Bereichen, wie z.B. Ausbildung, Forschung & Entwicklung und Kommunikation.
- Zweitens bedarf es eines geordneten institutionellen Umfeldes, das sich erst ansatzweise abzeichnet. In einem „Nationalen Cybersicherheitsrat“ könnten strategische Aspekte zwischen Staat und Wirtschaft thematisiert werden, während ein mögliches „Cyberlagezentrum“ als Arbeitsmuskel die operative Arbeit unterstützen könnte.
- Drittens ist es wichtig, Zuständigkeiten im Behördenumfeld und bei den Unternehmen zu klären und gleichzeitig auch zu straffen.
- Das geht viertens einher mit der Bezeichnung von Ansprechpartnern auf unterschiedlichen Entscheidungs- und Handlungsebenen.
- Fünftens ist es unerlässlich, den Informationsaustausch zwischen Staat und Wirtschaft zu strukturieren. Dafür zeichnen sich verschiedene inhaltliche Interessenschwerpunkte ab (z.B. Dialog mit Herstellern einzelner Komponenten, Dialog zwischen den Regulatoren, Zusammenarbeit bei konkreten Ereignissen). Wichtig ist hierfür ein verlässlicher Rechtsrahmen, der geschaffen werden muss.

Cyberrisikoprävention stärken

Österreichs Unternehmen und die Behörden haben umfangreiche Maßnahmen ergriffen, um sich vor Cyberrisiken zu schützen. Im Bereich der Risikoprävention sollten zwei Bereiche ausgebaut werden:

- Erstens sollte die nationale Cybersicherheitsstrategie bewusst auf vorhandene Initiativen des Risikomanagements Bezug nehmen und zum Aufbau eines nationalen Cyberrisikomanagements als umfassendes Managementsystem beitragen.
- Zweitens sollte die betriebliche Notfallvorsorge (Business Continuity Management, BCM) verstärkt sektorübergreifend konzipiert werden. Von besonderer Bedeutung sind dabei u.a. die Wechselwirkungen zwischen den BCM-Vorkehrungen in den einzelnen Sektoren, die Definition von BCM-Vorgaben für Prozesse und Dienste mit sektorübergreifender Bedeutung sowie das Monitoring und die Überprüfung, ob und wie BCM-Vorgaben umgesetzt werden.

Cybersicherheit mit Verhaltensanreizen fördern

Anreize dienen dazu, das Verhalten der Akteure in eine Richtung zu lenken, die es erlaubt, das Niveau der Cybersicherheit in Österreich zu verbessern. Zusätzlich zum öffentlich-privaten Informationsaustausch sind drei Aspekte wichtig:

- Erstens kann IKT-Sicherheit mit Standards gefördert werden. Diesbezüglich ist mehr Klarheit erforderlich, ob es neuer Standards oder einer besseren Umsetzung der bestehenden Standards bedarf, welche Standards für welche Schutzziele relevant sind, wie die Beachtung der Standards überprüft wird und was bei Nichtbeachtung geschieht.
- Zweitens können die Behörden mit eigenen Sicherheitsleistungen die Privatwirtschaft unterstützen. Dazu zählen beispielsweise digitale Schlüssel und Zertifikate von Behörden, sichere Cloud-Dienste oder die Bereitstellung von Übertragungskapazitäten im Krisenfall. Allerdings ist bei allen öffentlichen Sicherheitsleistungen zu fragen, in welchem Umfang eine Konkurrenzierung der Privatwirtschaft gewollt ist.
- Schließlich dienen Übungen und Planspiele dazu, die Eignung von Konzepten, Instrumenten und Strukturen im Hinblick auf verschiedene Cyberzwischenfälle zu testen. Sie sollten daher regelmäßig durchgeführt werden, um Lücken zu erkennen und vorhandene Stärken auszubauen.

CYBERRISIKOLANDSCHAFT ÖSTERREICH: ÜBERSICHT

© maxuser – iStockphoto.com

2

Cybersicherheit[2] hat sich innerhalb sehr kurzer Zeit zu einem der am intensivsten debattierten Themen entwickelt. Gerade weil verschiedene Formen der Nutzung der Informations- und Kommunikationstechnologie (IKT) aus dem Alltag der meisten Menschen nicht mehr wegzudenken sind, profitiert beinahe jede Bürgerin und jeder Bürger von damit verbundenen Möglichkeiten, ist aber auch von negativen Auswirkungen direkt betroffen. Eine im Sommer 2011 in Deutschland durchgeführte und veröffentlichte Umfrage zeigte, dass der Datenbetrug im Internet, der Missbrauch von persönlichen Daten sowie Computerviren mit deutlichem Abstand als die größten sicherheitsrelevanten Risiken betrachtet wurden.[3]

Die Verfügbarkeit und die Verbreitung der IKT sind zentrale Voraussetzungen der gesellschaftlichen und wirtschaftlichen Prosperität. Das XXIV. Regierungsprogramm (2008–2013) der österreichischen Bundesregierung unterstreicht diese Feststellung mit dem Hinweis, dass IKT für „rund ein Viertel der Zunahme des Bruttoinlandsproduktes und ca. 30–45 % des Produktivitätszuwachses in den EU-Staaten verantwortlich“ ist.[4] Die Schattenseiten wie Cyberkriminalität, Cyberangriffe oder der Missbrauch digitaler Medien für extremistische Zwecke stellen „neue Herausforderungen für alle betroffenen Akteure dar und erfordern ein breites Zusammenwirken im Rahmen eines Gesamtkonzepts“[5]. Mit Blick auf die strategisch bedeutsamen Infrastruktursektoren spricht der aktuelle österreichische Verfassungsschutzbericht gar von einem Gefahrenpotenzial, das „einen bisher nicht bekannten Reifegrad erreicht hat“[6]. Diese Einschätzungen sind mehr als nachvollziehbar, denn

- die Kosten der Cyberkriminalität belaufen sich weltweit auf gut 388 Milliarden $[7] oder etwa 296 Milliarden € – ungefähr das 4fache des aktuellen österreichischen Bundeshaushalts;
- die Störung oder Lahmlegung der IKT in strategisch bedeutenden Infrastruktursektoren wie Energie, Verkehr, Transport, Finanzen oder der öffentlichen Verwaltung beeinträchtigt die Versorgung mit lebenswichtigen Gütern und Diensten und kann damit auch die öffentliche Ordnung destabilisieren;
- die Spionage[8] mit modernen digitalen Mitteln gefährdet die nationale Wettbewerbsfähigkeit und untergräbt die nationale Souveränität;
- die gezielte Verbreitung von Falschmeldungen auf digitalem Weg und mit Hilfe sozialer Netzwerke kann die Reputation von Einzelpersonen, staatlichen Einrichtungen sowie Unternehmen nachhaltig gefährden und gleichzeitig Verwirrung sowie Unruhe im öffentlichen Raum schaffen.[9]

2 Siehe für eine ausführliche Begriffsdefinition die Ausführungen in Kapitel 9.4.
3 Von 18 zur Auswahl stehenden Risikokategorien folgten Inflation auf Rang 5, lebensbedrohliche Krankheiten auf Platz 8, Terroranschläge auf Rang 11, Arbeitslosigkeit auf Rang 12, Gewaltverbrechen auf Rang 16 und Krieg auf Rang 17. Siehe: Sicherheitsreport 2011, S. 14.
4 Regierungsprogramm 2008–2013, S. 64.
5 Österreichische Sicherheitsstrategie, S. 8.
6 Verfassungsschutzbericht 2011, S. 87.
7 2011 Norton Cybercrime Report. Davon entfallen 114 Milliarden $ auf die eigentlichen Straftaten, weitere 274 Milliarden $ fallen als Folge des Zeitverlusts für Opfer an. Die Untersuchung wurde in 24 Ländern durchgeführt.
8 In einer 2010 durchgeführten Studie wurde der volkswirtschaftliche Schaden der Wirtschafts- und Industriespionage für Österreich auf jährlich ca. 880 Millionen € geschätzt. Siehe: Gefahren durch Wirtschafts- und Industriespionage für die österreichische Wirtschaft, S. 4.
9 Sandawi, „Cyber Weapons 2.0“, S. 18–19.

Der abstrakten Gefährdung steht die konkrete Bedrohung Österreichs durch Cyberrisiken gegenüber. Die vom Sicherheitssoftwareunternehmen McAfee regelmäßig durchgeführte Studie „Mapping the Mal Web“, die die Sicherheit von Internetdomänen untersucht, führte Österreich im Jahre 2010 auf dem 76. von 106 zu vergebenden Plätzen – eine Verschlechterung um 13 Plätze gegenüber 2009.[10] Die Frage der Sicherheit oder Unsicherheit von Internetdomänen ist aber nur ein Aspekt der Cybersicherheit. Um das gesamte Spektrum dieser Thematik auszuleuchten, arbeitet das Kuratorium Sicheres Österreich (KSÖ) seit Mitte 2011 an verschiedenen Analysen und Vorschlägen zum Umgang mit erkannten Cyberrisiken. Der vorliegende Bericht fasst die wichtigsten Erkenntnisse dieser Arbeiten zusammen. Damit unterstützt das KSÖ die Bundesregierung in ihrer Bemühung, für Österreich eine nationale Cybersicherheitsstrategie zu definieren.

Das methodische Vorgehen zur cyberbezogenen Risikopotenzialanalyse, die für ausgewählte Sektoren der strategisch relevanten Infrastruktur Österreichs von Bedeutung ist, wurde in Anlehnung an die Risikomanagementnorm ISO 31000 definiert. Gestützt auf den in dieser Norm entwickelten Dreischritt der Risikoidentifizierung, -analyse und -bewertung zur Risikobeurteilung (Abbildung 1, grau schattiertes Feld) wurden ebenfalls drei Arbeitsphasen definiert.

In der ersten Phase (Juli bis September 2011) ging es darum, den grundsätzlich relevanten Risikoraum zu definieren. Zu diesem Zweck wurden Fachgespräche durchgeführt und die wissenschaftliche Literatur ausgewertet, um gestützt darauf eine Cyberrisikomatrix für Ös-

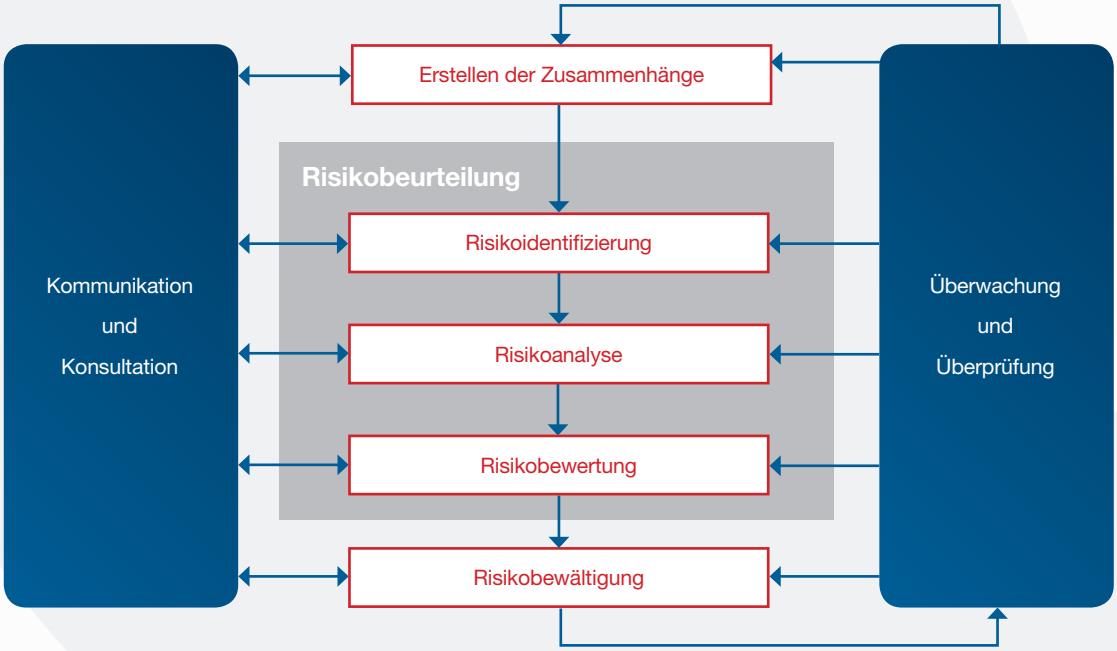


Abbildung 1: Risikomanagement nach ISO 31000
Quelle: ÖNORM ISO 31000

terreich zu entwerfen. Diese Arbeit orientierte sich an zeitgleich laufenden Bemühungen zur Darstellung der für Österreich relevanten Sicherheitsrisiken des Bundesministeriums für Landesverteidigung und Sport.[11] Zwei Gesprächsrunden mit österreichischen Experten dienten dazu, den Entwurf der Cyberrisikomatrix zu diskutieren und zu validieren. An diesen Gesprächsrunden beteiligten sich Wissensträger aus dem öffentlichen Sektor sowie aus dem privatwirtschaftlichen Bereich. Der Schwerpunkt lag dabei auf einer repräsentativen Darstellung der Sichtweise von Vertretern aus strategisch bedeutenden Infrastruktursektoren wie Energie, Finanz, Transport/Verkehr, Informations- und Kommunikationstechnologie sowie aus dem Behördensektor. Im Ergebnis entstand daraus die in Abbildung 2 dargestellte Cyberrisikomatrix,[12] die von der Bundesministerin des Inneren und dem Generalsekretär des KSÖ im Rahmen einer Konferenz im September 2011 vorgestellt wurde. Mit dieser Vorstellung wurde die Risikoidentifizierung im Sinne der grundlegenden Beschreibung möglicher Gefährdungen abgeschlossen.

Im Anschluss an einen vorbereitenden Zwischenschritt im 4. Quartal 2011 wurden im 1. Halbjahr 2012 die zweite und dritte Phase der Cyberrisikoanalyse lanciert. Phase 2 diente dazu, die mit der KSÖ-Cyberrisikomatrix allgemein dargestellte Risikolandschaft zu präzisieren. Im Vordergrund stand dabei die

10 Mapping the Mal Web, S. 13. Unter den Top 50 der schlechtesten Host- und Netzwerkanbieter findet sich gegenwärtig kein Unternehmen aus Österreich. Siehe: Top 50 Bad Hosts and Networks, S. 8.
11 Bobi, „Gefährdetes Österreich“.
12 Siehe zur Definition der jeweiligen Risiken die Ausführungen in Kapitel 9.4.

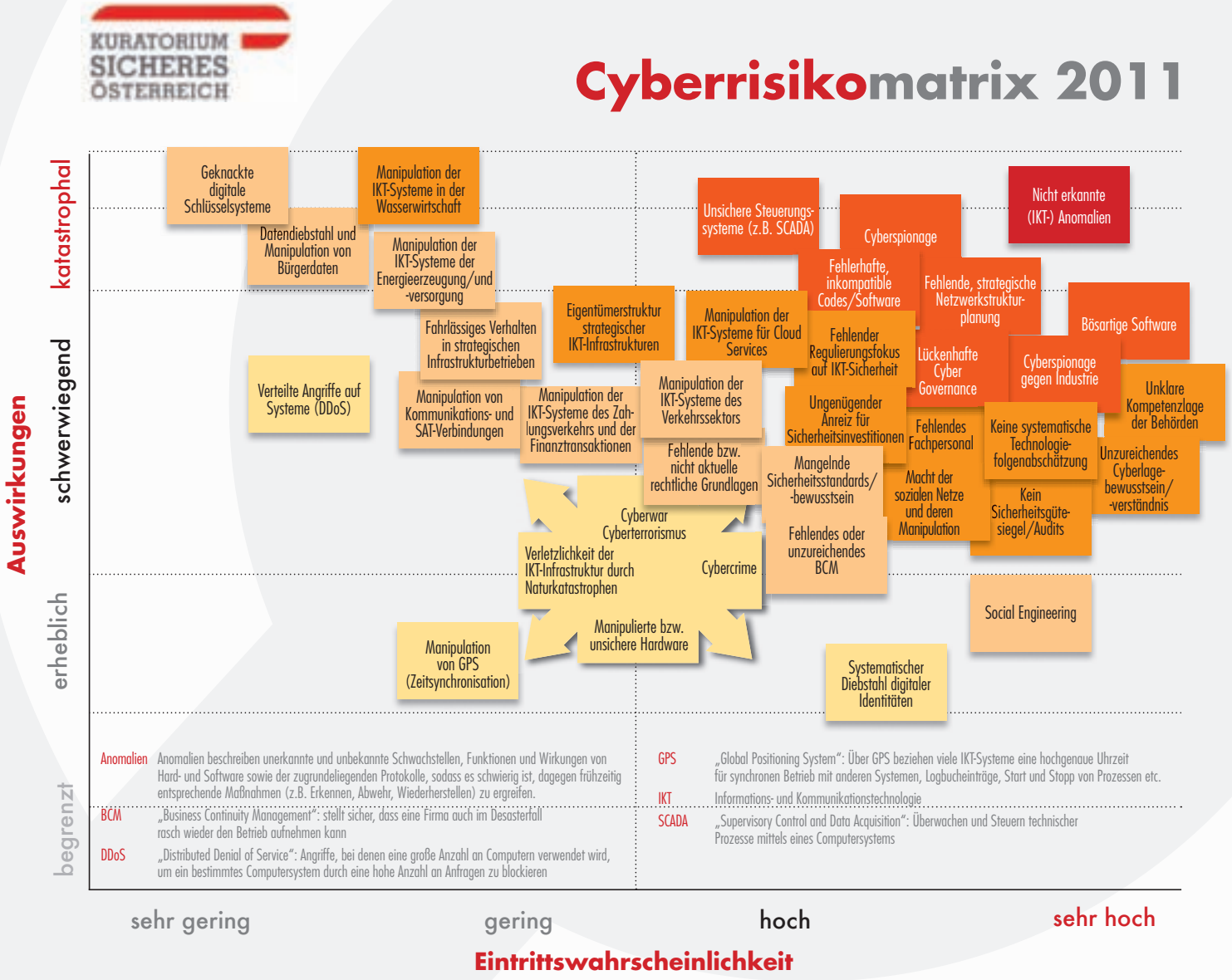
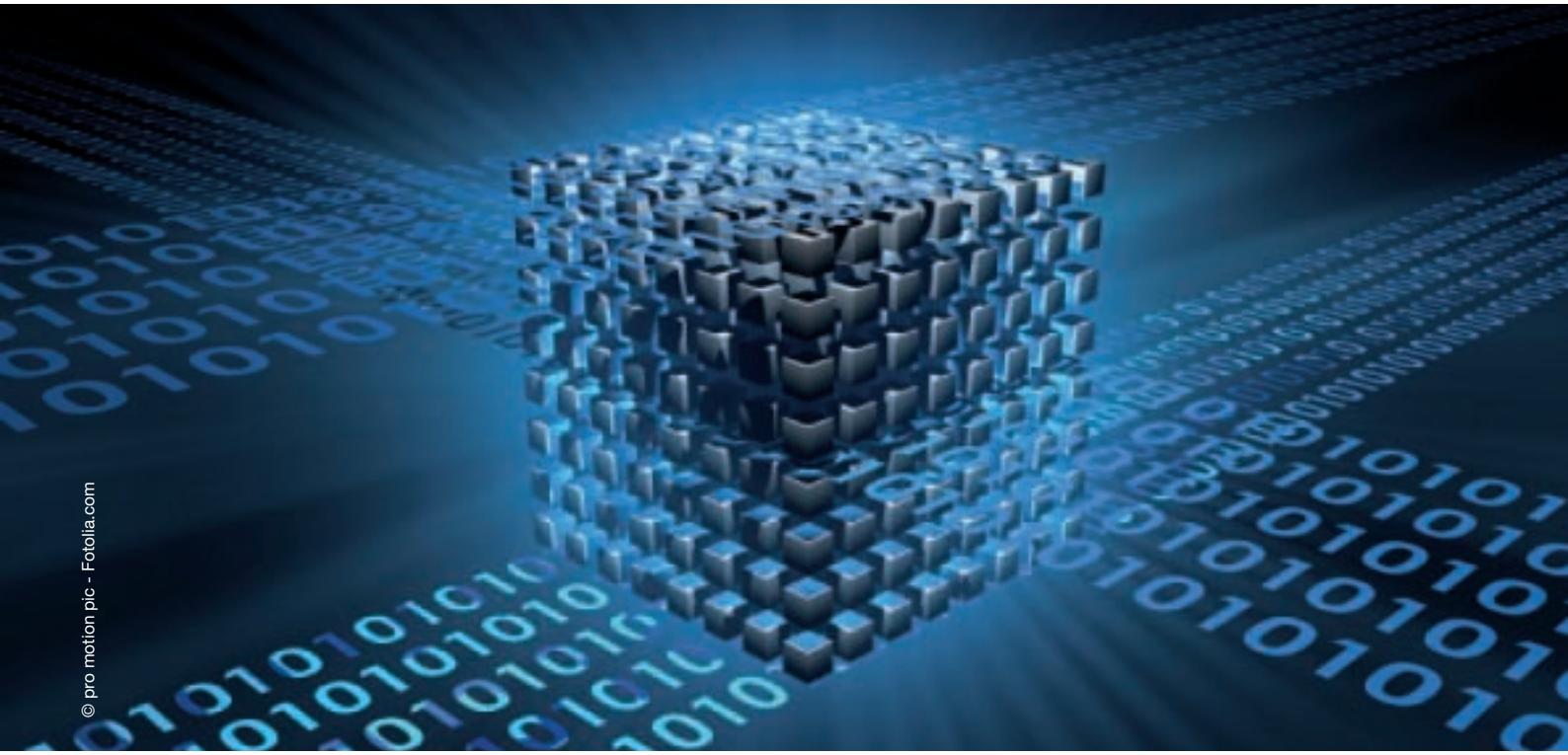


Abbildung 2: KSÖ-Cyberrisikomatrix
Quelle: KSÖ



Frage, wie relevant die einzelnen Risiken aus Sicht verschiedener strategischer Infrastruktursektoren sind. Dabei wurde das Ausmaß der möglichen Gefährdung in Kombination mit den jeweiligen Präventions- und Abwehrmaßnahmen der jeweiligen Akteure betrachtet. In dieser zweiten Phase wurden die Aspekte der Risikoanalyse und der Risikobewertung gemäß ISO 31000 zu einer Risikopotenzialanalyse kombiniert. Die dafür benötigten Informationen wurden in insgesamt 31 Einzelinterviews mit 55 Sektorexperten gewonnen (Abbildung 3).[13] Dabei handelte es sich im Kern um jene Institutionen, die sich auch bereits an der Erarbeitung der KSÖ-Cyberrisikomatrix beteiligt hatten (Kapitel 9.2).

Phase 3 widmete sich vor diesem Hintergrund der Frage, wie vorhandene Schwächen in der Erkennung, der Abwehr und der Bewältigung von Cyberrisiken in Österreich überwunden und vorhandene Stärken ausgebaut werden können. In 26 Interviews wurden 45 Sektorexperten zu den aus ihrer Sicht bestehenden Handlungserfordernissen befragt. Daraus entstand ein Fünf-Punkte-Programm, das im Sinne von Vorschlägen für die Entscheidungsträger in Politik, Wirtschaft und Verwaltung in Kapitel 8 dargestellt wird. Die Entwurfsfassung des vorliegenden Berichts wurde Anfang Mai 2012 in zwei getrennten Diskussionsrunden mit den Behördenvertretern und ausgewählten Vertretern der übrigen Infrastruktursektoren besprochen. Deren Anregungen flossen in die Überarbeitung des Berichts ein.

Ein elektronisches Konsultationsverfahren,[14] das vom 21. Mai 2012 bis 15. Juni 2012 durchgeführt wurde, gab darüber hinaus einem breiten Kreis von Expertinnen und Experten die Möglichkeit, die konkreten Vorschläge des Fünf-Punkte-Programms zu bewerten und zu kommentieren. Von den mehr als 500 eingeladenen Teilnehmerinnen und Teilnehmern beteiligten sich 155 am Konsultationsverfahren. Diese gaben knapp 4.400 Stimmen und beinahe 170 Kommentare ab. Mehr als 3.600 zustimmende Voten bringen zum Ausdruck, dass die vorgeschlagenen Maßnahmen in der Konsultation auf

13 Die Gespräche dauerten zwischen 90 und 180 Minuten und wurden schriftlich protokolliert.
14 Für die Umfrage für die cbased-Plattform genutzt, die partizipative Diskussions- und Abstimmungsprozesse unterstützt.

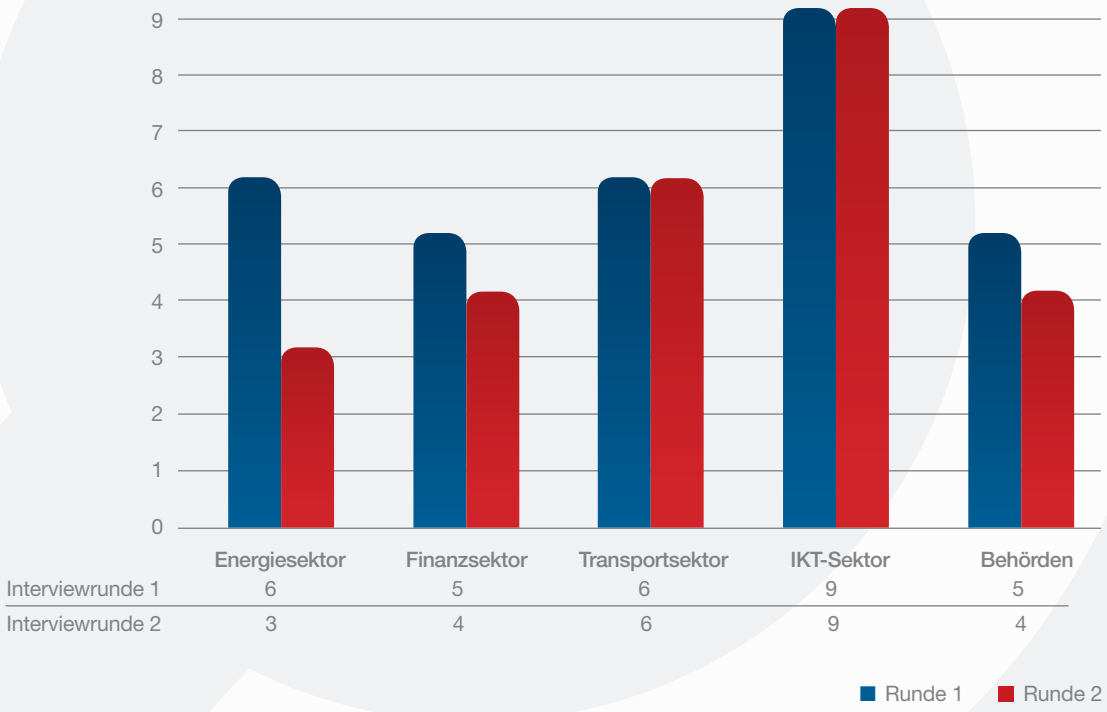


Abbildung 3: Interviewpartner nach Sektoren

Quelle: KSÖ

sehr breite Zustimmung stießen. Kritisch bewertet wurden in der Tendenz jene Vorschläge, die mit konkreten rechtlichen Vorschriften verbunden wären.

Die detaillierte Risikoanalyse und -bewertung aus Sicht der Experten der genannten fünf strategischen Infrastruktursektoren erfolgte auf Basis der KSÖ-Cyberrisikomatrix. Die Relevanz jeder Risikokategorie wurde auf einer Skala von 1 (sehr niedrig) bis 4 (sehr hoch) bewertet. Die jeweilige Einschätzung wurde während der Einzelinterviews vorgenommen und diskutiert. Die daraus resultierende Gesamtübersicht illustriert Abbildung 4.

Die Gesamtübersicht sollte vorsichtig interpretiert werden, denn die Ergebnisse stellen nicht mehr – aber auch nicht weniger – als eine Trendaussage dar. Diese Vorsicht ist erstens angebracht, weil quantitative Daten leicht überinterpretiert werden. Die Auswertung der Ergebnisse zeigte deutliche Bewertungsunterschiede innerhalb und zwischen den Sektoren, sodass sich teilweise ein sehr differenziertes, mitunter aber auch sehr heterogenes Bild ergibt. Darauf gehen die folgenden Kapitel näher ein.[15] Zweitens ist Vorsicht erforderlich, weil grundsätzlich denkbare Risikopotenziale bewertet, jedoch keine umfassenden Prozess- und Verwundbarkeitsanalysen durchgeführt wurden. Ein idealer Risikobewertungsprozess würde aus drei Schritten bestehen: Zuerst werden für jeden Infrastruktursektor die relevanten Kernprozesse und deren sektorübergreifende Verknüpfung identifiziert. Danach wird die IKT-Abhängigkeit der sektorspezifischen und sektorübergreifenden Prozesselemente bestimmt. Im Anschluss daran wird die Ver-

wundbarkeit dieser Elemente durch mögliche Cyberrisiken bestimmt. Ein solch umfassendes Vorgehen war im Rahmen des Projekts insbesondere aus zeitlichen Gründen nicht möglich, doch diese Überlegungen wurden bei den Einzelinterviews berücksichtigt.

Wird die Empfehlung zum vorsichtigen Umgang mit den Ergebnissen befolgt, können daraus mehrere Schlussfolgerungen abgeleitet werden. Zu diesem Zweck stellt Abbildung 5 in einer zusätzlichen Verdichtung die Top-15-Cyberrisiken aus Sicht der Interviewpartner dar. Folgende Aspekte fallen auf:

- Der **Faktor Mensch** erfährt in der Beurteilung der Experten die größte Beachtung.[16] Von den acht Risikofaktoren, die als besonders relevant eingestuft wurden, sind vier direkt mit dem Verhalten des Menschen in komplexen IKT-gestützten Infrastrukturen verbunden. Die Gefahr fahrlässigen Verhaltens, mangelndes Sicherheitsbewusstsein, das Risiko der Informationsabschöpfung durch Social Engineering sowie mangelndes Fachpersonal lassen keinen Zweifel daran, dass der Wert aller Bemühungen zur Förderung der Cybersicherheit mit der Expertise der Mitarbeitenden – und in weiterer Folge aller IKT-Nutzer – steht und fällt.

- Dass **sektorübergreifende Abhängigkeiten** durch den allgegenwärtigen Einsatz von IKT verstärkt werden, kommt in der Beurteilung ebenfalls deutlich zum Ausdruck. Stellvertretend dafür steht an erster Stelle das potenzielle Risiko, das mit einer Manipulation der IKT-Systeme der Energieerzeugung und -versorgung verbunden ist. Die Manipulation von Kommunikations- und Satellitenverbindungen sowie die Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen unterstreicht dieses Argument. Letzteres Risiko dürfte vermutlich auch deshalb so prominent genannt worden sein, weil technische Fortschritte (z.B. Mobile Banking, elektronische Rechnungs-/Zahlungsabwicklung) es ermöglichen, dass finanzielle Prozesse immer stärker mit den Leistungserstellungsprozessen anderer strategisch relevanter Infrastruktursektoren verknüpft werden. Im Zusammenhang mit den sektorübergreifenden Abhängigkeiten ist auch die hohe Relevanz fehlender unternehmerischer Notfallvorsorge (Business Continuity Management) zu erwähnen. Diesbezüglich sind sich die befragten Experten einig, dass BCM für einzelne Unternehmen und – wenn auch weniger stark ausgeprägt – innerhalb einzelner Sektoren bereits einen guten Stand erreicht hat. Die Herausforderung liegt künftig aber gerade bei der sektorübergreifenden Betrachtung der entsprechenden Konzepte der Notfallvorsorge.

- Es überrascht nicht, dass sich unter der Top-15-Liste fünf **technische Risikokategorien** befinden. Aufschlussreich ist, dass die Experten die hauptsächlichen Risiken in den inhärenten Schwächen und Qualitätsmängeln der eingesetzten Hard- und Software sehen. Dafür stehen Risikokategorien wie fehlerhafte bzw. inkompatible Codes und Software, geknackte digitale Schlüsselsysteme sowie nicht erkannte (IKT-)Anomalien.

- Mit **Cybercrime** und **Cyberspionage** bestätigen die befragten Experten die Bedeutung von zwei Tatbeständen, die auch aus der allgemeinen Diskussion bekannt sind. Gerade dieser Punkt verdient allerdings mit Blick auf die öffentlich-private Sicherheitszusammenarbeit besondere Beachtung. Aufgrund der Fokussierung auf die Top 15 in Abbildung 5 wird möglicherweise übersehen, dass die Phänomene des **Cyberwar** und des **Cyberterrorismus** von den Experten höchst unterschiedlich bewertet wurden. Vor allem beim Cyberwar zeigte sich ein deutlicher Unterschied zwischen der Einschätzung der privatwirtschaftlichen und der staatlichen Vertreter. Während die Relevanz dieses Risikos mit Ausnahme des Energiesektors von den privatwirtschaftlichen Experten eher als gering beurteilt wird, sieht darin vor allem

15 Hinzu kommt, dass die Stichproben in den einzelnen Sektoren unterschiedlich groß waren. Deshalb wurden für die Aufbereitung der Daten nur einfache Durchschnittswerte verwendet.
16 Hierzu weiterführend: Bowen/Stolfo/Devarajan, „Measuring the Human Factor of Cyber Security“.

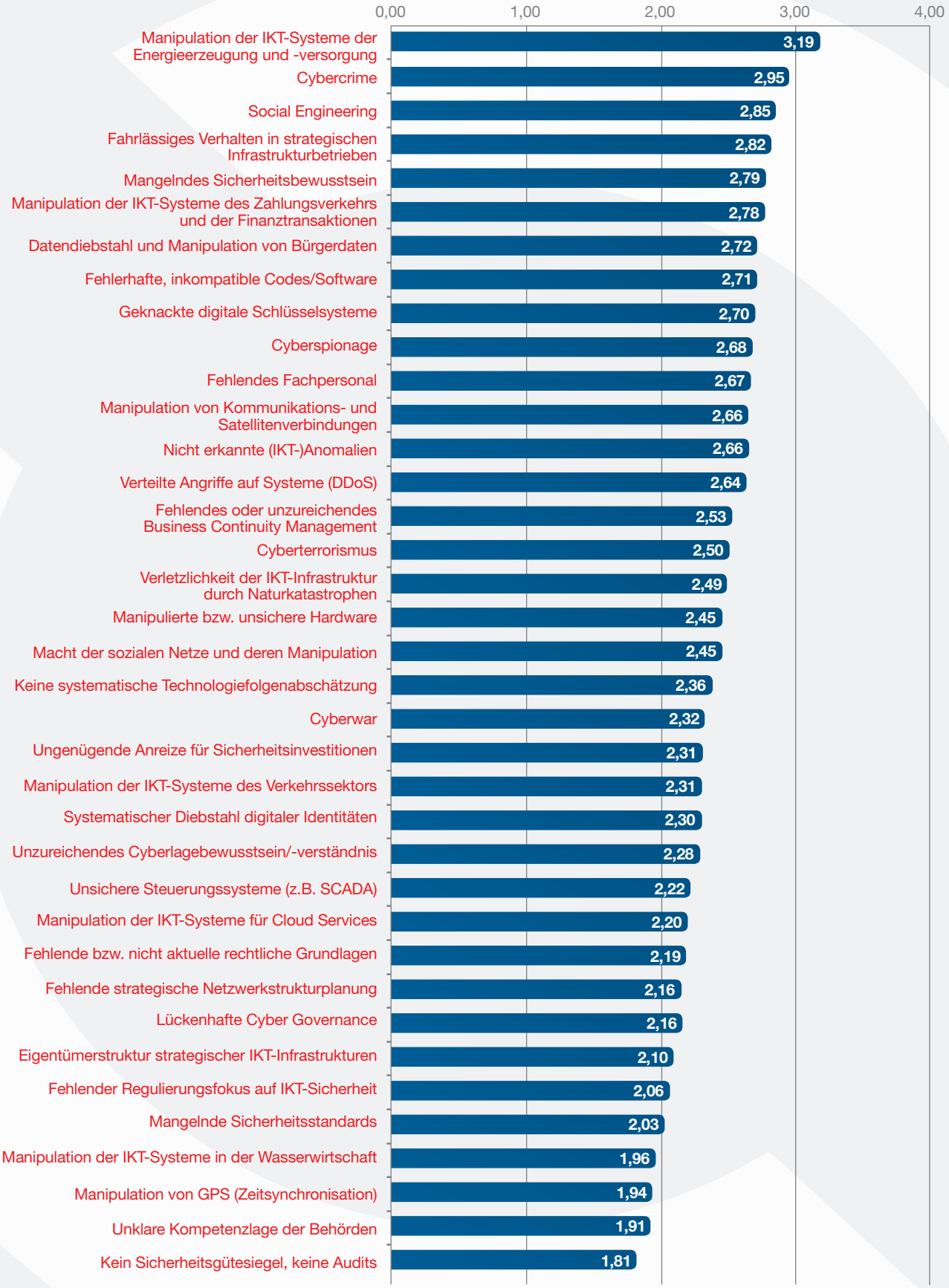


Abbildung 4: Cyberrisiken aus Sicht der Interviewpartner (Gesamtübersicht)

Quelle: KSÖ-Interviewserie

die Landesverteidigung eine zentrale Herausforderung. Dieser Unterschied deutet einen entsprechenden Diskussionsbedarf an, um zu vermeiden, dass Wahrnehmungsdifferenzen die staatliche und privatwirtschaftliche Sicherheitsvorsorge so stark beeinflussen, dass daraus eine Lücke entsteht, die möglicherweise selbst wieder ein Sicherheitsrisiko darstellen könnte.

- Zwischen der Risikoeinschätzung und dem **Stand der Sicherheitsvorsorge** in den einzelnen Sektoren bestehen deutliche Unterschiede. Das kam auch in den Interviews zum Ausdruck. Während in der ersten Interviewrunde immer wieder auf die Auswirkungen der möglichen Manipulation der IKT-Systeme der Energieerzeugung und -versorgung Bezug genommen wurde, spielte dieses Thema in der zweiten Interviewrunde kaum noch eine Rolle. Das unterstreicht, wie bedeutend die Differenzierung zwischen Fremd- und Eigenbewertung ist, macht gleichzeitig aber auch klar, wie wichtig es ist, dass über die Maßnahmen der Sicherheitsvorsorge ebenso berichtet wird wie über reelle und vermeintliche Risiken. Daraus lassen sich bereits erste Handlungserfordernisse mit Blick auf die Kommunikation und die Bewusstseinsbildung ableiten (Kapitel 8.1).

Die in der Cyberrisikomatrix dargestellten potenziellen Risiken basieren auf einem umfassenden Ansatz, der zwischen akteurs-, technik-, organisations- und umweltbezogenen Ursachen unterscheidet.[17] Dieser Ansatz ist sinnvoll, um den relevanten Risikoraum vollständig auszuleuchten. Angesichts der Vielfalt der grundsätzlich vorstellbaren Risiken, ihren unterschiedlichen Ursachen und vielfältigen Auswirkungen erscheint es sinnvoll, noch eine zusätzliche konzeptionelle Unterscheidung einzuführen. Diese dient vor allem dazu, die Merkmale der **intentionalen Cyberrisiken** zu erfassen. Dahinter steht die Überlegung, dass die Erkennung, Abwehr und Bewältigung jener Risiken, die mit dem normalen Geschäftsbetrieb der Unternehmen in strategisch bedeutenden Infrastruktursektoren zusammenhängen, auf jeden Fall durch das betriebliche Risikomanagement abgedeckt werden sollten. Das gilt auch für die Frage, wie beispielsweise technische Komplexität oder Naturereignisse den Geschäftsbetrieb beeinflussen können. Insofern bilden diese Aspekte die „Grundlast“ des betrieblichen Risikomanagements. Mit der zusätzlichen Betrachtung intentionaler, von Menschen bewusst ausgelöster Risiken kann darüber hinaus auch die „Spitzenlast“ abgedeckt und die Risikobetrachtung abgerundet werden.

Tabelle 1 illustriert die diesbezüglichen Überlegungen[18] anhand der Unterscheidung zwischen den in Frage kommenden Akteuren, dem Motiv, um ein Cyberrisiko bewusst eintreten zu lassen, den dafür bereitstehenden Mitteln und den erzielten Wirkungen. Die folgenden Kapitel werden anhand internationaler Beispiele und der Beurteilung aus Sicht der österreichischen Experten zeigen, dass alle illustrativ erwähnten Motive bereits heute zur Anwendung kommen. Zwischen der **Motivlage** und dem Verhalten einzelner **Akteure** gibt es enge Zusammenhänge:

- Im Bereich der Cyberkriminalität liegt dabei der Schwerpunkt beim Erzielen von Profit und dem Diebstahl digitaler Identitäten, denn auch damit kann Geld erwirtschaftet werden.
- Hacktivisten sind im Unterschied dazu eher darauf erpicht, die Funktionsfähigkeit von IKT-Diensten zu stören bzw. lahmzulegen, um damit die Reputation der betroffenen Gegenpartei zu schädigen und gleichzeitig den eigenen Ruf zu stärken.
- In möglicher terroristischer Absicht agierende Gruppen haben ein Interesse daran, den Cyberspace und moderne IKT zu nutzen, um eigene Handlungen zu verschleiern.
- Wenn sich Staaten der IKT bedienen, um damit sicherheitsrelevante Operationen gegen Dritte durchzuführen, dürften die Beeinträchtigung der Funktionsfähigkeit strategisch wichtiger Infrastrukturen und

17 Siehe hierzu auch: Cebula/Young, „A Taxonomy of Operational Cyber Security Risks“.
18 Siehe hierzu auch: Wilshusen, „Cybersecurity: Threats Impacting the Nation“, S. 3–5.

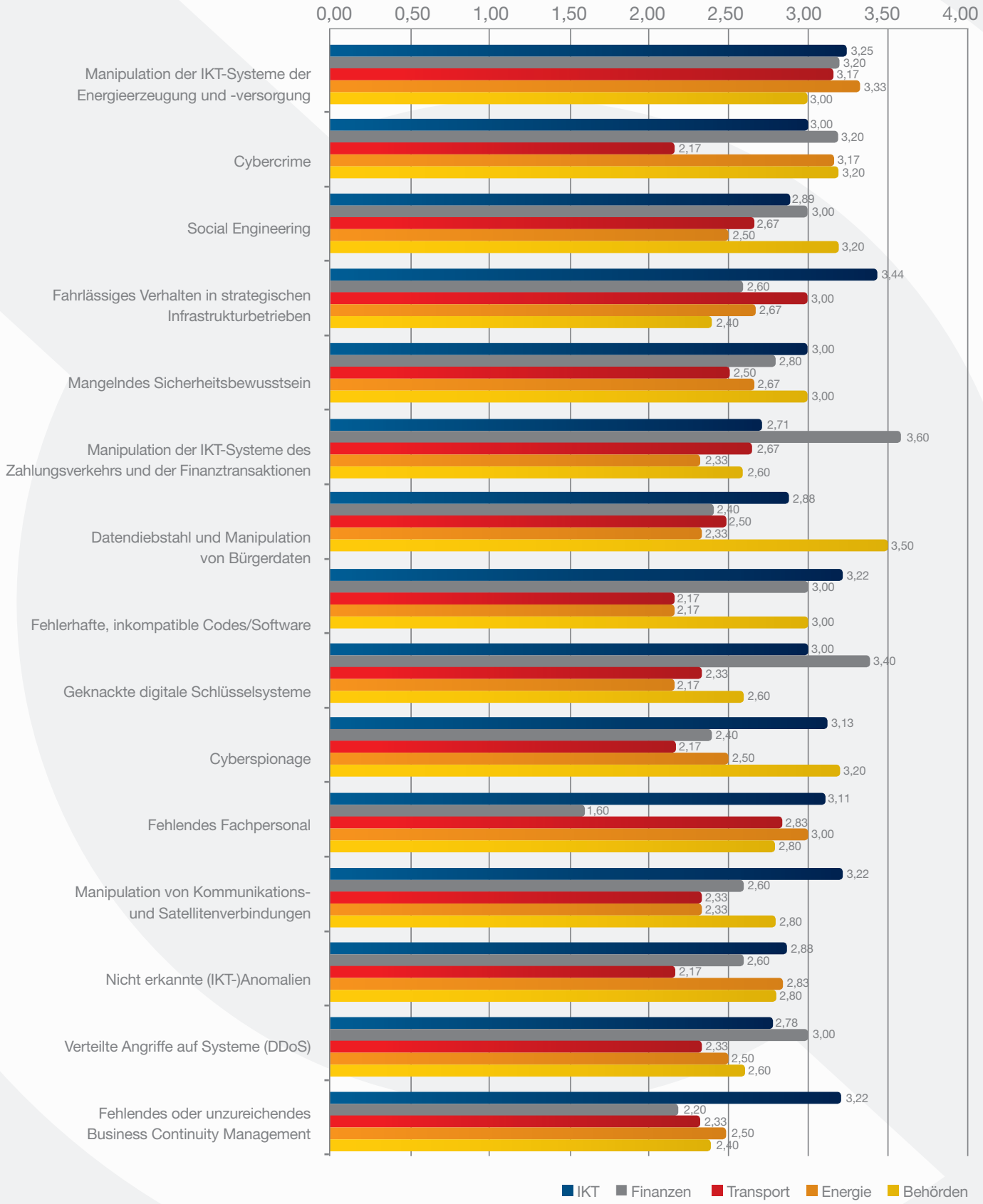


Abbildung 5: Top-15-Cyberrisiken aus Sicht der Interviewpartner (differenziert nach Sektoren)

Quelle: KSÖ-Interviewserie

© tdbiii – iStockphoto.com

„Bei der Wahl der Mittel ist die Unterscheidung zwischen Mensch, Technik und Organisation hilfreich, da damit unterschiedliche Angriffsvektoren beschrieben werden.“

ihrer Dienste, die Spionage oder auch die mögliche Destabilisierung der öffentlichen Ordnung im Vordergrund stehen.

- Wirtschaftsspionage zwischen Unternehmen ist inzwischen ein alltägliches Phänomen. Im Vordergrund steht dabei der Zugang zu geschäftsvertraulichen Informationen wie Konstruktionsplänen oder Forschungs- und Entwicklungsergebnissen, Informationen zu Vertragspartnern, Finanzdaten oder Hinweise zur künftigen strategischen Ausrichtung der Konkurrenz.
- Innentäter können verschiedene Motive verfolgen. Sie können von außen agierende Täter unterstützen, um beispielsweise Spionage zu betreiben oder sensible Informationen abzuschöpfen, oder sie wollen z.B. aus Frustration in Folge eines Arbeitsplatzverlustes den Ruf des ehemaligen Arbeitgebers schädigen.

Bei der Wahl der **Mittel** ist die Unterscheidung zwischen Mensch, Technik und Organisation hilfreich, da damit unterschiedliche Angriffsvektoren beschrieben werden. Die Bedeutung des Faktors Mensch wurde bereits angesprochen. Dieser ist relevant, weil menschliche Nachlässigkeit oder Unwissenheit als Quelle möglicher fehlerhafter Handlungen in Verbindung mit komplexen IKT-Anwendungen sehr schnell weitreichende Folgen verursachen kann. Zudem kann menschliches Verhalten auch gezielt ausgenutzt werden, um Einzelpersonen zu bestimmten Handlungen zu veranlassen oder von diesen Informationen abzuschöpfen, die in weiterer Folge für eine schädigende Handlung im Cyberspace genutzt werden können (z.B. Phishing).[19]

Beim digitalen Einsatz verschiedener technischer Mittel können grob gesprochen drei

19 Siehe zum Thema Social Engineering weiterführend: Hadnagy, „Social Engineering: The Art of Human Hacking“.

Akteure (Wer?)	Motiv (Weshalb?)	Mittel (Wie?)	Wirkung (Was?)
Kriminelle Hacktivisten Terroristen Staaten Unternehmen Innentäter	Digitale Identitäten stehlen Funktionsfähigkeit einschränken, stören, außer Kraft setzen Handlungen verschleiern Spionage betreiben Profit erzielen (inkl. Erpressung) Reputationsschaden zufügen bzw. Reputationsgewinn erzielen Verwirrung stiften sowie Unruhe und Destabilisierung erzeugen	Mensch Social Engineering (Absicht) Nachlässigkeit, Unwissenheit Technik Schadprogramme Viren Würmer Trojaner Weitere Hacking Distributed Denial of Service (DDoS) Organisation Aufbaustruktur Ablaufstruktur (Prozesse) Schnittstellen zu Dritten Verantwortlichkeiten, Zuständigkeiten und Kompetenzen	Verfügbarkeit einschränken Vertraulichkeit brechen Integrität verletzen

Tabelle 1: Merkmale intentionaler Cyberrisiken
Quelle: Eigene Darstellung

Kategorien unterschieden werden, die mit unterschiedlichen Vorgehensweisen verbunden sind:

- Bei der Verwendung von Schadprogrammen erfolgt die Schädigung oder Störung durch den Einsatz speziell dafür programmierter oder angepasster Software. Je nach Funktion kann unterschieden werden zwischen Viren, die sich an Wirtsprogramme hängen und dadurch verbreitet werden, Würmern, die wie Viren funktionieren, sich aber ohne Wirtsprogramme verbreiten, und Trojanern, die kombinierte Wirtsprogramme mit versteckter Funktion darstellen. Weitere Schadprogramme befinden sich in Umlauf.[20]
- Hacking beschreibt die bewusste Suche nach Schwachstellen in Programmen und Sicherheitssystemen, um diese auszunutzen. Um diese Schwachstellen zu erkennen, werden verschiedene Verfahren eingesetzt. Dazu gehören das Knacken von Passwörtern, das Scannen von Systemen nach bekannten Verwundbarkeiten, das Mitschneiden bzw. Abhören des Netzwerkverkehrs, die Vorspiegelung von Fakten, die so nicht existieren (Spoofing), und das aktive Eindringen in Telekommunikationskomponenten wie Telefonnetzwerke (Phreaking) und drahtlose Netzwerke (Wardriving).[21]
- Um die direkte Beeinträchtigung der Verfügbarkeit IKT-gestützter Dienste geht es schließlich bei der durch Überlastung herbeigeführten Dienstverweigerung, auch (Distributed) Denial of Service ([D]Dos) genannt. In diesen Fällen wird ein System mit Abfragen und Befehlen über seine Leistungsgrenze hinaus belastet.[22]

Zusätzlich können auch organisatorische Schwachstellen ausgenutzt werden. Besonders relevant sind im Kontext des Schutzes strategisch relevanter Infrastrukturbetriebe und ihrer Dienstleistungen die Schnittstellen zu Dritten in anderen Sektoren oder zu Leistungsanbietern, denn genau dort stellen sich komplexe Fragen rund um Verantwortlichkeiten, Zuständigkeiten und Kompetenzen.

Die **Wirkungen,** die schädigende Handlungen mit IKT-Einsatz hervorrufen können, lassen sich am besten mit den Zielen der Informationssicherheit beschreiben.[23] Drei Schutzziele stehen dabei im Vordergrund:

- Die **Verfügbarkeit** beschreibt die Anforderung, dass Daten und Systeme zur Verfügung stehen und der Zugriff darauf möglich ist. Störungen, die zu einer Unterbrechung oder vollständigen Abschaltung der Systeme führen können, sollen verhindert werden.
- Die **Vertraulichkeit** definiert, dass Daten nur berechtigten Nutzern zur Verfügung stehen. Daraus ergibt sich die Anforderung, dass Daten von unberechtigten Dritten nicht eingesehen werden dürften. Ein digitaler Datendiebstahl verletzt dieses Schutzziel genauso wie die unverschlüsselte Übermittlung von Daten über unsichere Netzwerke.
- Die **Integrität** beinhaltet die Anforderung, dass Daten richtig und integer sind. Daraus ergibt sich das Ziel, dass Daten von unberechtigten Dritten nicht verändert werden dürfen. Dieses Schutzziel kann verletzt werden, wenn Unberechtigte beispielsweise in das Informationssystem eines Logistikunternehmens eindringen, um Frachtdokumente zu fälschen, und dadurch die eigentliche Identität einer Warenlieferung verschleiern.

Ein wesentliches Unterscheidungsmerkmal der Verletzung dieser drei Schutzziele ist die Latenzzeit zwischen dem Begehen der Tat und dem Zeitpunkt des Erkennens. Eine Verletzung der Verfügbarkeit kann sofort festgestellt werden, wenn z.B. der Strom ausfällt, Banktransaktionen nicht mehr getätigt werden können oder Telekommunikationsverbindungen unterbrochen sind. Wird die Vertraulichkeit oder die Integrität verletzt, ist die entsprechende Zeitspanne in der Regel deutlich größer. Wenn im Falle des Bruchs der Vertraulichkeit der unberechtigte Dritte die gestohlenen Daten so nutzt, dass der Diebstahl dem eigentlichen Eigentümer nicht auffällt, kann eine Verletzung der Vertraulichkeit oft gar nicht oder erst bei öffentlichem Bekanntwerden einer geheimen Information festgestellt werden. Die Verletzung der Integrität wird in der Regel erst bei einer Prüfung festgestellt, d.h., zwischen der eigentlichen Verletzung des Datenschutzes und möglichen Gegenmaßnahmen kann Zeit ungenutzt verstreichen.

„Es ist wichtig, dass über Massnahmen der Cybersicherheitsvorsorge genauso berichtet wird wie über Cyberrisiken.“

20 Dazu zählen Bot-Netze, also eine Schadsoftware, die ähnlich wie ein Trojaner funktioniert und durch den Zusammenschluss verschiedener infizierter Rechner zu Bot-Netzen verbreitet wird, Backdoors, die Systemzugriffe durch versteckte Hintertüren im Quellcode ermöglichen, Rootkits, die wie eine Hintertür funktionieren, sich aber tief im Innern eines Systems verstecken, und Keylogger, die Tastatureingaben der Nutzer aufzeichnen.
21 Siehe zu diesen Verfahren weiterführend: <http://www.openwall.com/john/>; <http://www.openvas.org/>; <http://www.wireshark.org/>; <http://www.tcpdump.org/>; <http://ettercap.sourceforge.net/>; <http://www.webcrunchers.com/stories/esq-art.html>; < http://www.wardriving.ch/hpneu/index2.html> (Zugriff: 12. April 2012).
22 Siehe hierzu mit besonderer Berücksichtigung der Rechtslage in Österreich: Öhlböck/Esztegar, „Rechtliche Qualifikation von Denial of Service Attacken“, S. 126–133.
23 ISO/IEC 17799, S. 1.

CYBERRISIKEN UND ÖSTERREICHS ENERGIESEKTOR

© Sergiy Serdyuk – iStockphoto.com

3.1. Österreichs Energiesektor: Relevanz in Zahlen
3.2. Cyberrisiken im Energiesektor: Allgemeine Bewertung und Trends
3.3. Cyberrisiken im Energiesektor: Österreichische Bewertung

3

3.1. Österreichs Energiesektor: Relevanz in Zahlen

- Die gut **1.570 Unternehmen** des österreichischen Energiesektors beschäftigten 2008 ungefähr **28.300 Mitarbeitende.** Diese erzielten 2009 einen **Bruttowertschöpfungsanteil** von **5,3 Milliarden €** oder 3 % der gesamten Bruttowertschöpfung Österreichs.[24]

- Bei Österreichs **Energiemix** fällt der überdurchschnittliche Anteil erneuerbarer Energieträger auf. Nach Eurostat-Angaben lag dieser Anteil 2009 bei 73 % (EU-27: 18 %). Zweitwichtigster Energieträger war Gas mit einem Anteil von 13 % (EU-27: 19 %), gefolgt von Öl mit 9 % (EU-27: 13).[25]

- 2009 wurden insgesamt 33 Millionen Tonnen **Öl** durch Pipelines in Österreich gepumpt. Das war innerhalb der EU-27 nach Großbritannien, Frankreich und Polen der vierthöchste Wert.[26] Dabei handelt es sich im Wesentlichen um das Transportvolumen der Transalpine Pipeline, die Öl vom Hafen in Triest via Ingolstadt in den süddeutschen Raum befördert.[27] Abzweigungen führen auch zu den Raffinerien der OMV bei Wien Schwechat.

- Das österreichische **Gasnetz** umfasst ca. 2.900 km Fernleitungsnetz und 39.500 km Verteilerleitungsnetz. Hinzu kommt als weitere wichtige Infrastrukturkomponente die Gasspeicherkapazität von gut 4,7 Milliarden m^3, was etwa der Hälfte des Jahresverbrauchs an Erdgas in Österreich entspricht. Die Gasspeicher werden von der OMV AG und der RAG AG betrieben.[28] Darüber hinaus spielt Österreichs Gaspipelinenetz auch für seine Nachbarstaaten eine wichtige Rolle, denn Italien, Slowenien, Ungarn und Deutschland werden über Pipelines versorgt, die durch Österreich verlaufen.

- Das **Leitungsnetz** der Austrian Power Grid umfasst mehr als 6.700 km. In den nächsten Jahren wird die APG jährlich ungefähr 150 Millionen € investieren, um die Netzinfrastruktur auszubauen und zu modernisieren.[29]

- Das **Fernwärmenetz** Österreichs belief sich 2010 auf ungefähr 4.200 Kilometer und hat sich in seiner Länge seit 1995 verdoppelt.[30]

24 <http://www.statistik.at/web_de/services/wirtschaftsatlas_oesterreich/branchendaten_nach_wirtschaftszweigen/index.html> (Zugriff: 3. April 2012).
25 Energy, transport and environment indicators, S. 34.
26 Energy, transport and environment indicators, S. 120.
27 <http://www.tal-oil.com/> (Zugriff: 3. April 2012).
28 <http://www.e-control.at/de/industrie/gas/gasnetz>; <http://www.e-control.at/de/industrie/gas/gasmarkt/speicher>; <http://www.ovgw.at/m/gas/themen/?uid:int=355> (Zugriff: 3. April 2012)
29 <http://www.apg.at/de/netz/anlagen/leitungsnetz> (Zugriff: 3. April 2012); Netzentwicklungsplan 2011, S. 14.
30 <http://www.gaswaerme.at/bfw/themen/index_html?uid=2737> (Zugriff: 3. April 2012).

3.2. Cyberrisiken im Energiesektor: Allgemeine Bewertung und Trends

Die Energiewirtschaft ist einer jener strategisch bedeutenden Infrastruktursektoren, die seit Jahren einem äußerst anspruchsvollen Transformationsprozess unterworfen sind. Die Liberalisierung der nationalen Energiemärkte, die Integration nationaler Marktsegmente zu einem europäischen Energiemarkt für Strom und Gas, der Aufbau grenzüberschreitender Interkonnektorenkapazitäten, die Einführung des Emissionshandels und die Anforderungen, die sich aus ambitiösen nationalen und europäischen Klimazielen ergeben, sind nur einige der Stichworte, die die maßgeblichen Herausforderungen umschreiben. IKT spielt traditionell eine wichtige Rolle in allen Segmenten der Energiewirtschaft. Durch die mit den klimapolitischen Vorgaben einhergehende Einführung intelligenter Netze wird der Grad der IKT-Durchdringung des Energiesektors zusätzlich erhöht. Hinzu kommen neue Herausforderungen, die sich aus der Dezentralisierung und der Flexibilisierung von Energieerzeugung und Energieabnahme ergeben werden.

Vor diesem Hintergrund überrascht es nicht, dass mögliche Gefahren, die sich für den Energiesektor aus bewusst oder unbewusst herbeigeführten Störungen ergeben können, schon sehr früh eine prominente Rolle in der Diskussion über neue Sicherheitsgefährdungen gespielt haben. Das ist angesichts der zentralen Bedeutung des Energiesektors für alle Bereiche der Gesellschaft mehr als nachvollziehbar (Abbildung 6). Bei der näheren Betrachtung fällt auf, dass IKT in den einzelnen Segmenten des Energiesektors[31] von unterschiedlicher Bedeutung ist:[32]

- Kernprozesse des Stromsektors sind die Erzeugung, die Übertragung und die Verteilung an die Verbraucher. Diese Prozessschritte werden in der Regel ergänzt durch Elemente des Handels und Vertriebs. Innerhalb dieser Prozesskette gibt es verschiedene kritische Komponenten, wie z.B. das Netzführungssystem mit seinen Anwendungen, die Rechenzentren, die Telekommunikation sowie die Stationsleittechnik.[33] Überwachungs- und Steuerungskomponenten (SCADA: Supervisory Control and Data Acquisition) werden eingesetzt, um die Funktion und die Interaktion verschiedener Komponenten zu kontrollieren, und spielen daher eine besonders relevante Rolle. Die Verwundbarkeit dieser Elemente resultiert aus unterschiedlichen Ursachen, wie beispielsweise unsicheren Protokollen für Zugänge von außen, ungeeigneten Zugangs- und Authentifizierungsregeln oder nicht bzw. mangelhaft verschlüsselter Datenübertragung.[34]

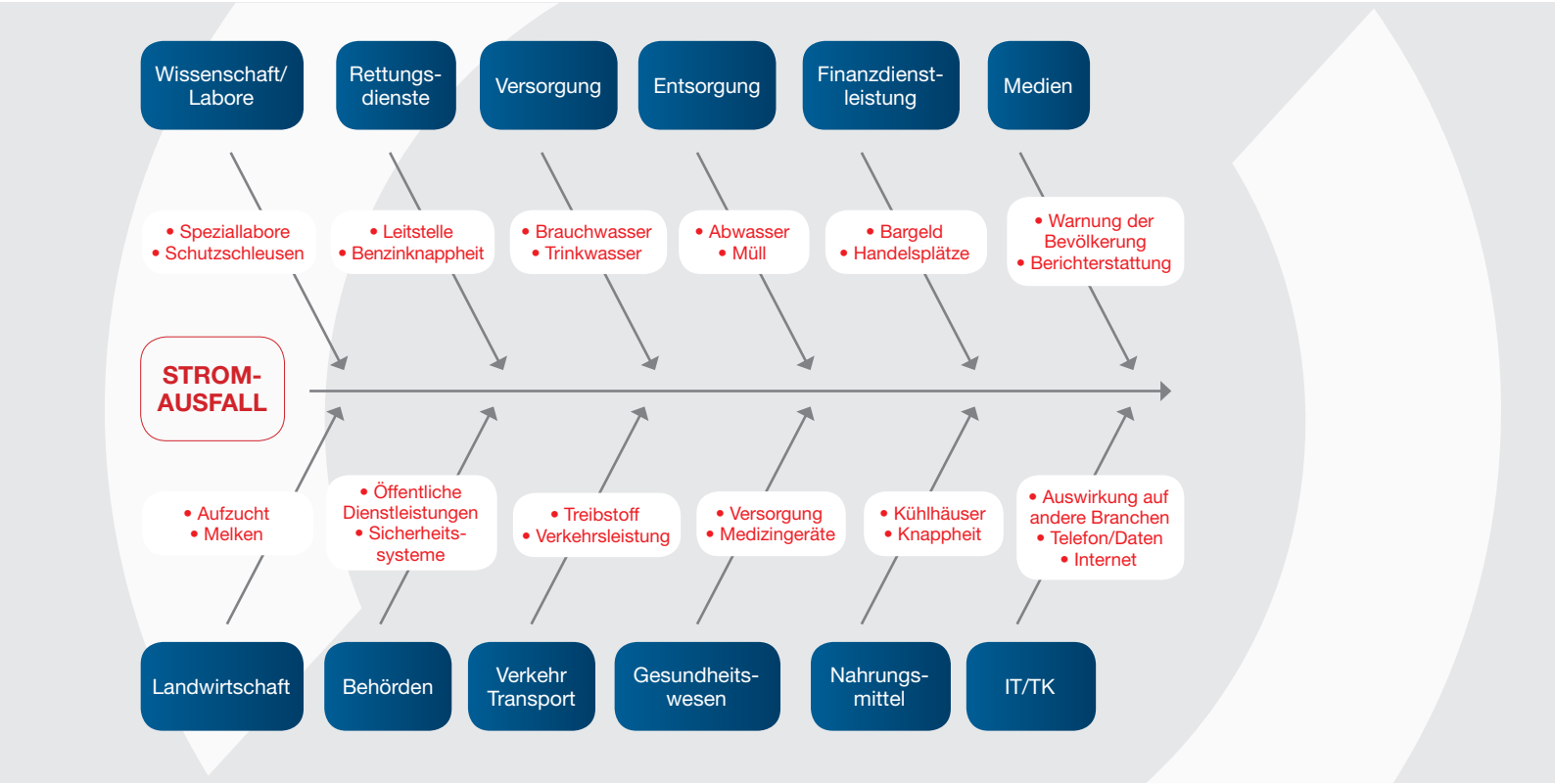


Abbildung 6: Relevanz der Stromversorgung für die Gesellschaft
Quelle: Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland, S. 22

- Der Gasbereich ist etwas anders strukturiert, verfügt aber im Kern ebenfalls über die drei zentralen Elemente der Erzeugung, Übertragung und Verteilung. Zur Verbindung der Gasförderquellen mit den Verbrauchermärkten erstreckt sich das Gasnetz, das Europa versorgt, über tausende von Kilometern. Angesichts dieser geografischen Ausdehnung kommt dem Netzwerkmanagement besondere Bedeutung zu. Neben den SCADA-Elementen spielt die IKT im Gasbereich eine zentrale Rolle, denn sie verbindet die Netze mit den Kontrollstellen, die Netze und Gasflüsse steuern.[35]

- Im Unterschied zum Gassektor ist der Ölsektor infrastrukturell weniger vernetzt. Die Versorgung erfolgt über Landungsstellen für internationale Ölschiffe, Verbindungspipelines zu Raffinerien und anderen Verbrauchsstellen sowie über Zwischenlager. Die Versorgung mittels Öltanklastwagen schafft zusätzliche Möglichkeiten der Kompensation bei Ausfällen oder Lieferunterbrechungen. Der Sektor zeichnet sich daher durch eher unabhängig voneinander betriebene IKT-Systeme aus.[36]

Auch wenn das Horrorszenario einer großflächigen und langanhaltenden Unterbre-

31 Der Nuklearsektor wird an dieser Stelle bewusst nicht betrachtet, auch wenn jüngste Beispiele wie die Verbreitung von Stuxnet nahelegen, dass dieser Bereich unter bestimmten Umständen ein ganz besonders relevantes Angriffsziel darstellen kann.
32 Hierzu weiterführend: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector; Roadmap to Achieve Energy Delivery Systems Cybersecurity.
33 ICT Continuity, S. 12.
34 Hierzu weiterführend: Common Cybersecurity Vulnerabilities in Industrial Control Systems.
35 Nerlich/Umbach, „European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat“. Siehe zum umfassenden europäischen Gasnetz auch die weiterführenden Informationen auf der Website des Dachverbands Gas Infrastructure Europe: <http://www.gie.eu.com> (Zugriff: 5. April 2012).
36 IABG, Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure, S. 53–54.

chung der Energieversorgung im Wege einer bewusst herbeigeführten IKT-Manipulation noch nicht stattgefunden hat, bedeutet dies nicht, dass es im Energiesektor keine IKT-bezogeneån Zwischenfälle gab. Dies illustrieren die folgenden Beispiele:

Spionage in Energienetzen

Unter dem Codenamen Night Dragon erfolgten nach Recherche von McAfee ab November 2009 gezielte, auf Ausspähung ausgerichtete Attacken in den IKT-Netzen weltweit führender Öl-, Gas- und petrochemischer Unternehmen. Ziel dieser Aktionen war es, geschäftsvertrauliche Informationen z.B. zu Unternehmenskennzahlen, wirtschaftlichen Kenngrößen wichtiger Projekte und Hintergrundangaben zu bevorstehenden Angeboten zu erlangen.[37]
Dass Energieunternehmen möglicherweise öfter als gedacht Opfer der Ausspähung sind, ohne dass sie dies erkennen, legen die Umfrageergebnisse einer Studie des US-amerikanischen Ponemon Institute vom April 2011 nahe. Dabei gaben 69 % der Antwortenden an, dass sie innerhalb der letzten zwölf Monate Opfer einer erfolgreich ausgenutzten Schwäche des eigenen Informationssicherheitssystems waren. 56 % sagten auch, dass bei diesen Zwischenfällen die Datenbanken der Unternehmen kompromittiert wurden, während nur 5 % auf die SCADA-Elemente verwiesen. Mit Blick auf die Frage, woher der mögliche Angriff kam, stellte die Untersuchung fest, dass es bis zu 22 Tage dauern kann, bis entdeckt wurde, dass die Manipulation durch einen eigenen Mitarbeitenden erfolgte. 35 % der Antwortenden gaben an, dass sie den Zeitraum bis zur Entdeckung der Tat gar nicht nennen konnten.[38]

Funktionsfähigkeit der Energieinfrastruktur stören und/oder ausschalten

Eng mit dem Risiko der Spionage verbunden ist der vor allem in den USA immer wieder geäußerte Verdacht, dass die eigenen Unternehmen der Elektrizitätswirtschaft Gegenstand fremder Aktivitäten sind, die das Ziel verfolgen, Codes zu hinterlassen oder die Steuerungssoftware so zu manipulieren, dass eine Unterbrechung der Stromerzeugung und -übertragung von außen möglich wird.[39] Dass durch solche Manipulationen auch die physische Infrastruktur betroffen sein kann, zeigte kürzlich der Fall Stuxnet und davor auch das vom US-Energieministerium durchgeführte Experiment Aurora, bei dem ein Generator durch Manipulation des SCADA-Elements zur Explosion gebracht wurde.[40]

Eine ganz andere Dimension der Funktionsbeeinträchtigung sprechen Bruce Averill und Eric Luiijf an, wenn sie darauf hinweisen, dass während der russisch-georgischen Auseinandersetzung im August 2008 auch die Gaspipeline zwischen Baku, Tiflis und Ceyhan (BTC) Gegenstand russischer Cyberangriffe gegen Georgien war.

Kriminelle Angriffe auf Emissionshandelssysteme

Zwischen 2009 und 2011 verübten Kriminelle mehrere Angriffe auf das Handelssystem für europäische Emissionsrechte (ETS). 2009 wurde durch den Schwindel mit der Umsatzsteuer beim Handel mit CO_2-Zertifikaten ein Schaden in dreistelliger Millionenhöhe verursacht. 2010 und 2011 wurden auf illegale Weise Emissionsrechte und Zugangsdaten der Nutzer entwendet, um auf diesem Weg die Emissionsrechte illegal weiterzuverkaufen. 2010 waren 17 nationale ETS-Handelsregister davon betroffen. 2011 wurden alleine in der Tschechischen Republik Emissionsrechte in Höhe von 6,7 Millionen € entwendet. Als Reaktion auf diese Vorfälle führte die Europäische Kommission im Frühjahr 2011 neue Sicherheitsstandards ein.[41]

Öffentliche Unruhe verursachen

Im Mai 2008 gelang es russischen Hackern, in das System einer Kernkraftanlage in St. Petersburg einzudringen. Für mehrere Stunden war die Website des Kernkraftwerks offline, während gleichzeitig Gerüchte in Umlauf gebracht wurden, dass radioaktive Strahlung ausgetreten sei. Zeitgleich war die Kommunikation zwischen der Anlage und dem staatlichen Nuklearkonzern Rosatom während Stunden unterbrochen. Das Eindringen wirkte sich nicht auf den Betrieb der Kernkraftanlage aus, hat aber Unruhe in der Bevölkerung verursacht.[42]

37 Global Energy Cyberattacks: Night Dragon.
38 State of IT Security. Study of Utilities & Energy Companies, S. 4–5. Bei den Antwortenden handelt es sich mehrheitlich um Vertreter privater und öffentlicher Elektrizitätsunternehmen sowie Öl- und Gasproduzenten bzw. -pipelinebetreiber.
39 Gorman, „Electricity Grid in U.S. Penetrated by Spies“. Hierzu weiterführend auch mit Berücksichtigung anderer Angriffsmodalitäten: High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, S. 26-46.
40 „Sources: Staged cyber attack reveals vulnerability in power grid“.
41 Gassmann, „Angriff auf den Emissionshandel“, S. 1; „Diebstahl bei Emissionshändlern“; „EU-Emissionshandel nach Hacker-Angriff gestoppt“; „Neue Sicherheitsstandards für den Emissionshandel“, S. 10.
42 Averill/Luiijf, „Canvassing the Cyber Security Landscape“, S. 1.

3.3. Cyberrisiken im Energiesektor: Österreichische Bewertung

Abbildung 7 illustriert, welche Cyberrisiken die befragten Energieexperten als besonders relevant bewerten. Mit potenziell unsicheren Steuerungssystemen und der Gefahr manipulierter IKT-Systeme rücken die Gesprächspartner des Energiesektors zwei Top-Cyberrisiken in den Mittelpunkt ihrer Risikobetrachtung, die auch mit Blick auf die Abhängigkeit anderer strategischer Infrastruktursektoren von der Energieversorgung eine große Rolle spielen. Aufschlussreich ist zudem, dass die Energievertreter die Phänomene Cyberwar und Cyberterrorismus als besonders relevant bewerten. Dies ist Ausdruck der Betroffenheit des Sektors, wenn z.B. das Internet bei einem kriegerischen oder terroristischen Angriff flächendeckend lahmgelegt würde. Auffällig ist zudem, dass die Gesprächspartner mögliche Lücken in der präventiven Sicherheit als sehr relevant erachten, was in der verhältnismäßig starken Gewichtung der sieben mit dem Durchschnittswert 2,67 bewerteten Risikofaktoren zum Ausdruck kommt.

Im Einzelnen haben die Energieexperten die Top-15-Cyberrisiken wie folgt bewertet:[43]

Unsichere Steuerungssysteme (z.B. SCADA) und Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

Bei den Antworten zu diesen beiden Punkten fallen zwei Aspekte auf. Zum einen sind sich

Abbildung 7: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Energiesektors

Quelle: KSÖ-Interviewserie

43 Alle Angaben stützten sich auf Interviews, die am 2., 13. und 22. Februar 2012 sowie am 2. und 6. März 2012 durchgeführt wurden.

die Gesprächspartner der Risiken in diesen zentralen Technologiebereichen bewusst und bereiten sich auch auf den Umgang mit den damit verbundenen Gefährdungen vor. Zum anderen wird die Frage, wie relevant diese Risiken für den einzelnen Energieversorger sind, unmittelbar durch seine Unternehmens- und Risikokultur bestimmt. Mehrere Gesprächspartner wiesen auf das risikoaverse Verhalten ihres jeweiligen Unternehmens hin, das dazu beiträgt, dass technische Innovationen erst mit einer gewissen Verzögerung übernommen werden. Diese Verzögerung eröffnet aus Sicht der Gesprächspartner die Möglichkeit, dass mit zunehmendem Reifegrad der Technologien auch entsprechende Risiken vermieden werden können. So zeigen sich denn auch die meisten Gesprächspartner zurückhaltend, wenn es z.B. um die Anwendung von Cloud Services im Energiesektor geht, auch weil aus deren Sicht die Chancen und Risiken dieser Anwendungen noch nicht umfassend bewertet werden können. Gerade im Bereich der Steuerungssysteme wird allerdings auch darauf hingewiesen, dass ein verstärkter Dialog mit den entsprechenden Herstellern begrüßenswert wäre, um Risiken frühzeitig zu erkennen und damit umzugehen.

Cybercrime

Kriminelle Taten, die in Profitabsicht erfolgen, sind für die Unternehmen des Energiesektors relevant, weil davon beispielsweise Kundendaten betroffen sein können. Neben dem Diebstahl dieser Daten geht es auch um die mögliche Manipulation von Verbrauchsdaten bzw. Mehrwertsteuerabrechnungen, aus denen Dritte einen Nutzen ziehen können. Dem Cybercrime können des Weiteren der Stromhandel und der Handel mit Emissionshandelszertifikaten zum Opfer fallen. Beide Bereiche sind für die Energiewirtschaft von vitaler Bedeutung, denn im ersten Fall geht es um die Handelbarkeit des Stroms, im zweiten um den klimapolitischen Beitrag der Energiewirtschaft.

Cyberwar und Cyberterrorismus

Unterschiedliche Ansichten vertraten die Gesprächspartner des Energiesektors lediglich bei der Frage, ob die Energiewirtschaft im Rahmen kriegerischer oder terroristischer Hand-

© ra2 studio – Fotolia.com

© pagadesign – iStockphoto.com

lungen ein attraktives Ziel darstelle oder nicht. Während einige Betreiber diese Frage bejahten, sahen andere Betreiber und Vertreter aus dem staatlichen Umfeld die Energiewirtschaft nicht als prioritäres Angriffsziel. Einigkeit bestand dagegen bei allen Interviewpartnern in der Beurteilung der Folgen: Würde ein Akt des Cyberwar oder ein terroristischer Anschlag zu einer Lahmlegung des Internet führen, hätte dies signifikante Auswirkungen insbesondere für die Stromwirtschaft.

Dessen ungeachtet zeigte sich in der Diskussion, dass die Unternehmen der Energiewirtschaft in hohem Ausmaß auf eigene IKT-Infrastrukturen zurückgreifen, um die für ihren Betrieb erforderlichen Prozesse abzuwickeln. Diese Unabhängigkeit von allgemeinen IKT-Infrastrukturen schuf bislang zusätzliche Sicherheit. Ob sich diese Autonomie der IKT-Netze allerdings im Zuge der Einführung intelligenter Stromnetze, die für Energie-Anbieter/-Nachfrager unterschiedlichster Provenienz offen sein müssen, verändern wird, bleibt abzuwarten.

Fehlendes Fachpersonal

Fehlendes Fachpersonal wird von allen Gesprächspartnern als sicherheitsrelevantes Risiko mit hoher Relevanz eingestuft. Dabei wurde auch zum Ausdruck gebracht, dass verstärkt in die Aus- und Weiterbildung investiert werden sollte, wobei die Vermittlung von Kenntnissen der IT-Sicherheit aus Sicht der Befragten eine besondere Rolle spielt.

Fehlender Regulierungsfokus auf IKT-Sicherheit

In diesem Punkt fällt die Beurteilung differenziert aus. Zum einen wird argumentiert, dass es nicht an Regulierung zur IKT-Sicherheit im Energiesektor mangelt. Vielmehr liege das Problem bei der Umsetzung der entsprechenden Vorschriften und damit verbunden auch bei der Überprüfung. Zum anderen sehen insbesondere die Betreiber einen Bedarf darin, neue Technologieentwicklungen regulatorisch adäquat abzubilden, um auf damit möglicherweise verbundene Risiken reagieren zu können. Die Diskussion um die Sicherheit der Smart Meter gilt dabei als Beispiel, das den Bedarf nach einem intensiveren Austausch zwischen der staatlichen Seite und den Betreibern sowie den Herstellern illustriert.

Nicht erkannte (IKT-)Anomalien

Die Bedeutung dieser Risikokategorie wird von allen Gesprächspartnern anerkannt, doch zeigt sich in den Antworten auch ein

gewisses Unbehagen angesichts der Unbestimmtheit des Begriffs. Deutlich wird zudem, dass die meisten Energieunternehmen nicht in ausreichendem Ausmaß über Ressourcen verfügen, um selbst nach möglichen Anomalien zu suchen. Sie verlassen sich in dieser Hinsicht teilweise auf die Unterstützung durch staatliche Akteure wie CERT.

Fahrlässiges Verhalten in strategischen Infrastrukturbetrieben

Fahrlässigkeit wird als Risiko hoch bewertet, doch bemühen sich alle Akteure des Energiesektors nach eigener Einschätzung darum, durch Schulung und Bewusstseinsbildung die möglichen negativen Auswirkungen einzudämmen. Der Rückgriff auf weitgehend autonom betriebene Netze (siehe Cyberwar/Cyberterrorismus) trägt ebenfalls dazu bei, dieses Risiko zu minimieren.
Auf einer anderen Ebene angesiedelt, aber für die Energiewirtschaft unmittelbar relevant sind politische Vorgänge. Die Gesprächspartner wiesen darauf hin, dass politisch begründete Interventionen in die Abläufe der Energiewirtschaft ein sehr komplexes System aus dem Gleichgewicht bringen können – dabei ist der Aufwand zur nachträglichen Stabilisierung insbesondere in finanzieller Hinsicht sehr hoch. Das unterstrichen die Gesprächspartner mit Hinweisen auf die jüngst in Deutschland geführte Diskussion über den Ausstieg aus der Kernenergie und die damit verbundenen Folgen für das Stromnetz.

Fehlende bzw. nicht aktuelle rechtliche Grundlagen

Die Energieexperten beurteilen die Qualität des bestehenden energiewirtschaftlichen Rechtsrahmens sehr differenziert. Grundsätzlich sehen sie die Gefahr der Überregulierung. Sie sind aber auch der Ansicht, dass der fehlende Regulierungsfokus auf IKT-Sicherheit zu Problemen führen kann. Wichtigste regulatorische Herausforderung ist aus Sicht der Unternehmen der Energiewirtschaft der Umgang mit dem Risikopotenzial neu eingeführter Technologien.

© Kerstin Waurick – iStockphoto.com

Keine systematische Technologiefolgenabschätzung

In den bereits wiedergegebenen Antworten zur Regulierung spiegelt sich auch die Meinung der Befragten zur systematischen Technologiefolgenabschätzung. Hier sehen insbesondere die Betreiber Handlungsbedarf, weil die rechtlichen Vorgaben und die Einführung neuer Technologien bzw. die Technologieentwicklung aus ihrer Sicht nicht aufeinander abgestimmt sind. Neben dem Stichwort Smart Meter fiel in den Interviews auch der Hinweis, dass die mobile Kommunikation für die Energiewirtschaft an Bedeutung gewinnen wird. Dies vor allem durch Applikationen der Energiesteuerung für den privaten Endverbraucher. Mobile Kommunikationsendgeräte werden damit Teil des Netzes der Energiewirtschaft, was von dieser entsprechend berücksichtigt werden muss.

Lückenhafte Cyber Governance

Diesen Aspekt beurteilen die staatlichen und die privatwirtschaftlichen Energieexperten unterschiedlich. Auf staatlicher Seite wird eher die Ansicht vertreten, dass Ansprechpartner und Austauschprozesse benannt sind. Bei den Unternehmen der Energiewirtschaft herrscht dagegen die Ansicht vor, dass es zu viele Initiativen bzw. Plattformen gibt und die Angebote und Maßnahmen staatlicherseits zu wenig aufeinander abgestimmt werden. Gerade der Umstand, dass Prozesse nicht durchgängig definiert sind, könnte sich in der Wahrnehmung der Betreiber des Energiesektors im Krisenfall nachteilig auswirken. Angesprochen wurde darüber hinaus auch die sektorübergreifende Abstimmung, beispielsweise mit Blick auf die Frage, welche Aufgabe die Provider von Internetdiensten zur Abwehr von Cyberrisiken übernehmen und wie dabei die Koordination erfolgt.

Macht der sozialen Netze und deren Manipulation

Die verhältnismäßig hohe Bewertung dieses Risikos ist überraschend, zumal aus den Gesprächen keine eindeutigen Argumente für die starke Gewichtung der möglichen Manipulation sozialer Netze und der Auswirkungen für die Energiewirtschaft erwähnt wurden. Angesprochen wurde das Risiko, dass in sozialen Netzen Stimmung gegen Energieunternehmen gemacht werden kann, beispielsweise im Hinblick auf deren Preispolitik, den Kundenservice oder die Energieträger, die von den Unternehmen genutzt werden. Das müsse im Sinne des Umfeldmonitoring beobachtet werden. Darüber hinaus kam die Anwendung sozialer Medien durch Mitarbeitende der Unternehmen zur Sprache. Hierfür haben einzelne Energieversorger bereits Schulungsmaßnahmen ergriffen.

Mangelndes Sicherheitsbewusstsein

Das mangelnde Sicherheitsbewusstsein ist ein potenzielles Risiko, doch bei den Gesprächspartnern überwiegt die Ansicht, dass viel getan wird, um die Mitarbeitenden für Sicherheitsfragen fit zu machen. Offen blieb in den Diskussionen die Frage, ob sich die Förderung des Sicherheitsbewusstseins künftig auch auf neue Akteure erstrecken muss, wenn zusätzliche Erzeuger und Abnehmer durch intelligente Energienetze Teil der Energiewirtschaft werden. Wenn das Elektroauto zum intelligenten Energiespeicher wird, wer kümmert sich dann um die relevanten Aspekte der Cybersicherheit: die Energiewirtschaft, die Automobilbranche, der Telekommunikationsanbieter oder der Verbraucher?

Unzureichendes Cyberlagebewusstsein und -verständnis

Die Gesprächspartner, die ein unzureichendes Cyberlagebewusstsein und -verständnis als hohes Risiko einstuften, verweisen insbesondere darauf, dass sich nicht alle Verantwortlichen der Risiken bewusst sind und dies angesichts der unterschiedlichen Definitionen und Argumentationsketten auch nicht einfach ist. Ohne einheitliches Begriffsverständnis, so das Argument, sei es aber auch schwierig, die Notwendigkeit von Maßnahmen zu beurteilen. Das wirkt sich dann auch wieder auf die Cyber Governance im Sinne des institutionellen Rahmens zur Kooperation zwischen verschiedenen Akteuren aus.

CYBERRISIKEN UND ÖSTERREICHS FINANZSEKTOR

MR.LIGHTMAN – Fotolia.com

4.1. Österreichs Finanzsektor: Relevanz in Zahlen
4.2. Cyberrisiken im Finanzsektor: Allgemeine Bewertung und Trends
4.3. Cyberrisiken im Finanzsektor: Österreichische Bewertung

4

Österreichs Finanzsektor: Relevanz in Zahlen

4.1.

- Die **Bruttowertschöpfung** der österreichischen Finanz- und Versicherungsdienstleistungen lag 2009 bei gut 18 Milliarden € oder 11 % der gesamten Bruttowertschöpfung. Mit 13 Milliarden € oder 8 % entfiel der Löwenanteil auf die Finanzdienstleistungen.[44]
- Der gesamte Finanzsektor beschäftigte Ende 2010 ca. 118.000 **Mitarbeitende** oder 3,5 % aller Erwerbstätigen in Österreich.[45] Ende 2009 zählte der österreichische Finanzsektor knapp 6.800 Unternehmen.[46]
- Ende 2011 verfügten Österreichs **Kreditinstitute** über 824 Hauptanstalten und 4.441 Zweiganstalten.[47]
- Mit einer Bank für 10.000 Einwohner weist Österreich innerhalb der EU eine der größten **Bankendichten** auf.[48]
- Österreich verfügt im internationalen Vergleich über eines der **dichtesten Netze an Geldausgabeautomaten.** Ende 2009 kam ein Geldausgabeautomat auf 1.035 Einwohner.[49]
- 2010 befanden sich in Österreich etwas über acht Millionen Maestro-**Bankomatkarten** in Umlauf. Damit wurde im gleichen Jahr ein Zahlungsvolumen von 15,9 Milliarden € umgesetzt. 2011 lag der Umsatz der 2,5 Millionen **Kreditkarten,** die in Österreich ausgegeben wurden, bei gut 8,6 Milliarden €.[50]

44 <http://www.statistik.at/web_de/services/wirtschaftsatlas_oesterreich/branchendaten_nach_wirtschaftszweigen/index.html> (Zugriff: 3. April 2012).
45 Statistik Austria, Jahrbuch 2012, S. 197. Das Total umfasst 80.374 Mitarbeitende für die Erbringung von Finanzdienstleistungen, 27.281 für Versicherungen, Rückversicherungen und Pensionskassen ohne Sozialversicherung sowie 10.293 Mitarbeitende für Tätigkeiten, die mit Finanz- und Versicherungsdiensten verbunden sind.
46 <http://www.statistik.at/web_de/services/wirtschaftsatlas_oesterreich/branchendaten_nach_wirtschaftszweigen/index.html> (Zugriff: 3. April 2012).
47 <http://www.oenb.at/isaweb/report.do?lang=DE&report=3.1.2> (Zugriff: 2. April 2012).
48 <http://www.regiodata.eu/de/bankenparadies-oesterreich> (Zugriff: 2. April 2012).
49 Streissler, Bedeutung der Banken für die österreichische Wirtschaft, S. 22–23.
50 <http://www.paylife.at/web/content/de/Home/Ueber_Europay/Facts_Figures/Transaktionenx_Umsatz/index.html>; <http://www.oenb.at/isaweb/report.do?lang=DE&report=5.4.2> (Zugriff: 2. April 2012).

4.2. Cyberrisiken im Finanzsektor: Allgemeine Bewertung und Trends

Der Finanzsektor zählt aus Sicht der Akteure, die den Cyberspace und moderne IKT für Straftaten aller Art nutzen, traditionell zu den beliebtesten Angriffsobjekten. Das erklärt sich weniger aus der Unsicherheit der dort eingesetzten Anwendungen als vielmehr aus der hohen Technologieaffinität des Finanzsektors, die zu einer starken IKT-Durchdringung führt und damit möglichen Cybertätern unterschiedliche Angriffsflächen bietet. So überrascht es nicht, dass der Finanzsektor im 2012 Data Breach Investigations Report von Verizon mit einem Anteil von 40 % die Liste der Sektoren anführt, die von Verletzungen der Datensicherheit betroffen sind. Ein ähnliches Bild ergibt sich auch aus dem Symantec Internet Security Threat Report und den Prognosen des Kaspersky Lab.[51] Je stärker die Abwicklung elektronischer Zahlungsvorgänge auch in anderen Wirtschaftszweigen und anderen strategisch bedeutenden Infrastruktursektoren Einzug hält – man denke hier an Themen wie E-Mobility oder elektronische Rechnungen –, desto relevanter werden die entsprechenden Verwundbarkeiten auch für diese anderen Sektoren.

Die Cyberrisiken im Finanzsektor sind vielfältig. Objekte möglicher Angriffe oder Manipulation sind in der Regel die eigentlichen Finanzdaten bzw. die Daten der Nutzer von Finanzdiensten und -systemen, die Wege der Datenübermittlung sowie die Systeme und Verfahren zur Abwicklung von Finanzdiensten. Wie die folgenden Beispiele verdeutlichen, sind dabei verschiedene Cyberrisikoarten zu unterscheiden:

Skimming von Geldautomaten

Das Ausspähen von Daten, die auf Magnetstreifen von Bankomat- und Kreditkarten gespeichert sind, gehört zu den „Klassikern“ im Bereich der Cyberkriminalität. Finanzdienstleister sind davon in vielfältiger Weise direkt betroffen. Aus Sicht der Strafverfolgungsbehörden besonders problematisch ist der Umstand, dass die Techniken des Skimming mit den entsprechenden Abwehr- und Gegenmaßnahmen scheinbar mühelos Schritt halten können.[52]

Übernahme digitaler Konten und Kontoinformationen

Einbrüche in digitale Systeme von Finanzdienstleistern wie Banken und Kreditkartenunternehmen, aber auch Dienstleistern, die im Auftrag ihrer Kunden abrechnen, erfolgen mit dem Ziel, Nutzerdaten zu erlangen und illegal auf digitale Konten zuzugreifen. In den USA verfolgte das Federal Bureau of Investigation (FBI) bis Ende September 2011 400 Fälle registrierter illegaler Kontoübernahmen mit einem Schadensvolumen von 225 Millionen $.[53] Am 30. März 2012 alarmierten Visa und Mastercard die Banken in den USA über eine massive Verletzung der Datensicherheit, die bis zu 10 Millionen Kreditkartennummern betreffen könnte.[54] Auffällig ist die Zunahme ausgeklügelter technischer Lösungen, um die Verwundbarkeit der Systeme im Finanzsektor auszunutzen. Dabei werden immer öfter nicht nur die Finanzdienstleister, sondern deren Kunden angegriffen.

Ein besonders raffiniertes Beispiel hierfür ist Qakbot. Diese Schadanwendung ist darauf ausgerichtet, Online-Informationen über Bankkonten zu stehlen. Dazu werden u.a. Informationen ausgespäht, die ein Nutzer aktiv während seiner Online-Vorgänge z.B. auf einer Banken-Website eingibt, um damit auch andere Online-Vorgänge zu kompromittieren.[55] Dem gleichen Zweck dient der seit 2006 in Umlauf befindliche Trojaner ZeuS, der sich auf Rechnern einnistet und wartet, bis die Nutzer eine vorgesehene Website eines Finanzdienstleisters aufrufen, um dann die entsprechenden Informationen abzugreifen und an einen Zentralrechner weiterzuleiten.[56] Problematisch bei diesen und anderen Fällen ist, dass sich der elektronische Diebstahl nicht nur auf direkt finanzrelevante Informationen bezieht, sondern zum umfassenderen Diebstahl digitaler Identitäten beitragen kann, wenn weitergehende persönliche Daten entwendet werden.

Finanzdienstleister können von den hier angesprochenen Problemen auch indirekt betroffen sein. Das zeigten die jüngsten Angriffe auf die Online-Spiele-Plattform von Sony oder den privaten US-Nachrichtendienst Strafor. In beiden Fällen wurde eine große Zahl von Kreditkartennummern erbeutet. Ebenso relevant sind für Fi-

© mbbirdy – iStockphoto.com

nanzdienstleister Angriffe auf die Anbieter digitaler Schlüssel und Zertifikate, wie beispielsweise DigiNotar,[57] die zur Authentifizierung von Online-Vorgängen eingesetzt werden (Kapitel 5.2).

Cyberspionage

Das Ausspionieren digitaler Informationen bei Finanzdienstleistern kann sich zum einen auf Kundendaten beziehen. Zum anderen stieg jüngst die Zahl der Meldungen, dass sich Cyberspionage möglicherweise auch auf vertrauliche Unternehmensbewertungen beziehen könnte.[58] Kopfzerbrechen bereitet den Banken und den Strafverfolgungsbehörden offenbar auch die Tatsache, dass elektronische Börsen- und Handelssysteme zum Opfer von Cyberspionage wurden, ohne dass allerdings klar ist, welches Ziel die Täter beispielsweise beim jüngsten Eindringen in die Systeme von US-Börsen verfolgt haben.[59]

Manipulation von Handelssystemen

Elektronische Handelssysteme können manipuliert werden, um dadurch illegal Finanzmittel abzuschöpfen. In den USA kam es zu Fällen, bei denen parallel zur Manipulation der Handelssysteme auch die Telefonverbindungen zwischen Kunden und Finanzdienstleistern lahmgelegt wurden, um zu verhindern, dass die Rechtmäßigkeit der jeweiligen Handlungen verifiziert werden konnte.[60]

Weitaus problematischer sind neuere Fälle der bewussten Manipulation von Algorithmen, die z.B. beim sogenannten Hochfrequenzhandel genutzt werden. Dabei geht es darum, selbst von kleinsten Kursschwankungen im Millisekundenbereich zu profitieren. Da der Hochfrequenzhandel die Volatilität der Kurse zusätzlich verstärken kann, sind Manipulationen in diesem Bereich von gesamtwirtschaftlicher Bedeutung. Banken wie Goldman Sachs und Société Générale haben in der Vergangenheit bereits Klagen wegen des Diebstahls solcher Algorithmen eingereicht.[61]

Eine neue Dimension hätte diese Gefahr erreicht, wenn sich die Gerüchte bestätigen sollten, die sich um den Kursabsturz der Handelsplattform BATS (Better Alternative Trading System) ranken. Der Börsengang von BATS erfolgte am 23. März 2012 und wurde innerhalb von 900 Millisekunden mit dem Totalabsturz der Aktien von 15 $ ins Bodenlose abgebrochen. Es wird vermutet, dass der Absturz von Konkurrenten der Handelsplattform durch einen Algorithmus ausgelöst wurde, der den BATS-Kurs gezielt gegen null bringen sollte. Auch wenn der Fehler innerhalb von zwei

51 2012 Data Breach Investigations Report, S. 12; Tillett, „Cybersecurity: Threats to the Financial Sector“, S. 4; Gostev, „Kaspersky Security Bulletin 2011/2012“, S. 6.
52 Snow, „Cybersecurity: Threats to the Financial Sector“, S. 4.
53 Snow, „Cybersecurity: Threats to the Financial Sector“, S. 1.
54 „MasterCard, VISA Warn of Processor Breach“.
55 Falliere, W32.Quakbot in Detail.
56 Banking Trojans.
57 „DigiNotar-Hack: Kritische Infrastruktur war unzureichend geschützt“.
58 „Cyber-Attacken: US-Großbanken schmieden Allianz gegen Hacker“.
59 Barrett, „Hackers Penetrate Nasdaq Computers“, Snow, „Cybersecurity: Threats to the Financial Sector“, S. 3.
60 Snow, „Cybersecurity: Threats to the Financial Sector“, S. 3.
61 „Hackers’ trial behind closed door“.

Stunden behoben werden konnte, war das Vertrauen möglicher Investoren in die Aktie offenbar verloren.[62]

Verletzen und Stören der IKT-Infrastruktur und der IKT-Supply Chain

Angesichts der hohen Abhängigkeit des Finanzsektors von funktionsfähiger IKT-Infrastruktur stellt die bewusst herbeigeführte Verletzung und Störung derselben ein entsprechendes Risiko dar. Dieses erstreckt sich von der physischen Infrastruktur bis hin zu mobilen Bankanwendungen:

- So kam es in der Vergangenheit vor, dass Schadsoftware bereits auf Geldautomaten und auf Kartenterminals vorinstalliert war.[63]
- Die Kollokation besonders leistungsfähiger Rechnersysteme kann sinnvoll sein, um die Leistungsfähigkeit von Handelssystemen zu verbessern, schafft aber auch zusätzliche Risiken durch die Konzentration ebendieser Infrastruktur in räumlicher Nähe.
- Darüber hinaus fällt in jüngster Zeit die Zunahme von Angriffen gegen Anwendungen im Bereich des Mobile Banking auf. Schon heute gibt es „Schad-Tweeds“, über die Schadsoftware auf Mobiltelefone heruntergeladen wird.[64] Mit dem unaufhaltsamen Voranschreiten elektronischer Applikationen, die auch für Bankgeschäfte genutzt werden, dürfte dieses Risiko nach Einschätzung von Beobachtern künftig deutlich zunehmen. Allerdings hängt die Ausprägung dieser Gefahr auch stark davon ab, wie schnell sich diese Anwendungen bei den Nutzern etablieren.[65]

Insiderstraftaten

Alle aufgeführten Risiken können ihren Ursprung bei Handlungen von Innen- und Außentätern, ehemaligen und aktiven Mitarbeitenden des Finanzsektors sowie bei Vertragspartnern haben. Auf die Bedeutung der Innentäter verwies kürzlich Gregory E. Shannon, Chief Scientist des US-amerikanischen CERT, bei einer Kongressanhörung. Dabei stellte er fest, dass in den letzten sieben Jahren rund die Hälfte aller Finanzinstitutionen in den USA von Insiderstraftaten betroffen war. Ebenfalls in gut der Hälfte aller untersuchten Fälle arbeiteten die Innentäter mit Komplizen außerhalb der Finanzinstitutionen zusammen. Dabei ging es nicht nur um Betrug, sondern auch um den Diebstahl geistigen Eigentums, wie z.B. Algorithmen für Handelssysteme und die Sabotage von IKT-Systemen.[66]

Digitale Verschleierung eigener Handlungen

Die Digitalisierung der Finanzwelt eröffnet darüber hinaus auch die Möglichkeit, eigene Handlungen zu verschleiern und die Arbeit der Strafverfolgungsbehörden zu erschweren. Digitales Geld bzw. die Möglichkeit, Überweisungen in kaum noch auffindbare Teilüberweisungen zu unterteilen und diese digital zu übermitteln, stellt eine Möglichkeit dar. Eine weitere Option ist die schwierig zu kontrollierende mobile Geldüberweisung per Smartphone. So gibt es z.B. in einigen Schwellenländern inzwischen deutlich mehr Smartphone-Nutzer als Bankkontoinhaber. Währungen, die in virtuellen Welten wie Second Life oder World of Warcraft geschaffen werden, stellen eine weitere Möglichkeit dar. So gibt es inzwischen offenbar Hinweise, dass es Hacker in China geschafft haben, in Online-Spielen auf illegale Weise eine Vielzahl von Spielpunkten zu erreichen, die danach in Geld umgewandelt wurden, das seinen Weg unter Umgehung internationaler Sanktionen nach Nordkorea fand.[67]

62 Durden, „SkyNet Wars: How a Nasdaq Algo Destroyed BATS“; Henkel, „Computerfehler steckt hinter blamablem Bats-Debut“.
63 Snow, „Cybersecurity: Threats to the Financial Sector“, S. 5; „Visa: Regelmäßiges Wiegen der Kartenterminals schützt vor Manipulationen“.
64 Snow, „Cybersecurity: Threats to the Financial Sector“, S. 4.
65 Tillitt, „Cybersecurity: Threats to the Financial Sector“, S. 4; Informationssicherung: Lage in der Schweiz und international. Halbjahresbericht 2011/1, S. 11.
66 Snow, „Cybersecurity: Threats to the Financial Sector“.
67 Bronk/Monk/Villasenor, „The Dark Side of Cyber Finance“, S. 129–142.
68 Alle Angaben stützten sich auf Interviews, die am 6. und 13. Februar 2012 sowie am 4. April 2012 durchgeführt wurden.

Cyberrisiken im Finanzsektor: Österreichische Bewertung

4.3.

Abbildung 8 illustriert die 15 relevantesten Cyberrisiken aus Sicht der Gesprächspartner des Finanzsektors in Österreich. Auffällig ist dabei die relativ große Homogenität in der Bewertung. Die ersten fünf genannten Risikokategorien wurden von vier der fünf Gesprächspartner als sehr hoch bzw. hochrelevant eingestuft und auch bei den darauffolgenden sechs Risikokategorien fiel die Bewertung durch drei Gesprächspartner immer noch in die Kategorien hoch bis sehr hoch. Ähnlich wie im Energiesektor steht die Sorge um die Gefährdung der eigenen Geschäftsprozesse der Finanz- und Versicherungsdienstleister an der Spitze, was in der Top-Reihung der potenziellen Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen sowie der geknackten digitalen Schlüsselsysteme zum Ausdruck kommt. In dieses Bild passt auch der hohe Stellenwert, den der Finanzsektor der systematischen Technologiefolgenabschätzung schenkt, weil das eigene Geschäftsmodell unmittelbar von der Sicherheit und Funktionsfähigkeit neuer Technologien abhängt (Stichworte: E-Banking, Mobile Banking). Die hohe Relevanz der Cyberkriminalität ist ein Spiegel der aktuellen Gefährdungslage.

Im Einzelnen können die Bewertungen der Finanz- und Versicherungsexperten zu den 15 Top-Cyberrisiken wie folgt zusammengefasst werden:[68]

Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen

Eine große Zahl der potenziell relevanten Cyberrisiken kann dazu führen, dass dadurch die im Finanzsektor eingesetzten IKT-Systeme tangiert bzw. manipuliert werden. Inso-

Abbildung 8: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Finanzsektors
Quelle: KSÖ-Interviewserie

weit als dadurch die Kernprozesse des Finanzsektors betroffen sind, ist dieses Risiko für den Sektor sehr relevant. Neben dem Reputationsverlust, der mit dem Ausfall möglicher Kern-IKT-Systeme verbunden ist, sprechen alle Interviewpartner auch die damit verbundenen finanziellen Schäden an. Wie beim Risiko geknackter digitaler Schlüsselsysteme wird auch in diesem Fall unterstrichen, dass gewisse Systeme sektorweit von zentraler Bedeutung sind. Das gilt beispielsweise für Systemkomponenten der Oesterreichischen Nationalbank.

Geknackte digitale Schlüsselsysteme

Die hohe Bewertung dieses Risikos ergibt sich aus der generellen Bedeutung digitaler Schlüsselsysteme im modernen Bankgeschäft. Diese Bewertung deckt sich auch mit internationalen Untersuchungsergebnissen (Kapitel 4.2). Die Antwortenden differenzieren in ihrer Bewertung allerdings danach, wie wichtig die einzelnen Zertifikate für die verschiedenen Geschäftsprozesse sind. Ebenso fällt auf, dass die Auswirkung geknackter digitaler Schlüsselsysteme unterschiedlich beurteilt wird, je nachdem, innerhalb welchen Segments des Finanzsektors die Antwortenden tätig sind. So kann die Kompromittierung digitaler Schlüsselsysteme nicht nur Änderungen in der Software, sondern auch in der verwendeten Hardware nach sich ziehen, wenn z.B. Bankomaten ausgetauscht werden müssen.

Cybercrime

Für die im kommerziellen Geschäft tätigen Banken ist Cybercrime inzwischen zu einem alltäglichen Problem geworden, das sich negativ auf das Vertrauen und die Reputation der Banken auswirkt und wirtschaftliche Schäden verursacht. Einzelne Akteure ausgewählter Teilsegmente des Finanzsektors behelfen sich, indem sie Aufgaben der IT-Sicherheit an hoheitliche Aufgabenträger übergeben und damit im Bereich Cybercrime weniger verwundbar sind. Die Entwicklung in den nächsten Jahren dürfte jedoch dazu führen, dass die Bedeutung des Risikos auch in diesem Segment zunimmt.

Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

Die hohe Relevanz dieses Risikos unterstreicht, wie wichtig die Analyse sektorübergreifender Abhängigkeiten ist. Gerade weil die Abhängigkeit von Strom im Finanzsektor hoch ist, bereiten sich die Akteure entsprechend darauf vor. Lösungen zur Notstromversorgung und zur Absicherung mit redundanten Ausfallrechenzentren an verschiedenen Orten wurden von den Gesprächspartnern als wichtige Maßnahmen der Krisenvorsorge erwähnt. Dabei wurde allerdings auch konzediert, dass die zeitliche Wirkung eigener Notfallmaßnahmen beschränkt ist. So könnten Stromunterbrechungen bis zu einer Woche noch kompensiert werden; länger andauernde Stromunterbrechungen hätten weitreichende Konsequenzen für die Verfügbarkeit der Leistungen des Finanzsektors.

Fehlerhafte, inkompatible Codes/Software

Für dieses Cyberrisiko sehen sich die Banken nach Auskunft der Gesprächspartner gut gewappnet, insbesondere durch eigene Testteams, Audits und Prüfverfahren, bevor mögliche neue Software Releases eingesetzt werden. Als besonders kritisch erweist sich diese Risikokategorie vor allem für den zeitgesteuerten Zahlungsverkehr sowie für den Bargeldverkehr. Einzelne Gesprächspartner räumten auch ein, dass Tests zwar unerlässlich, aber auch tückisch sind, weil sie zu Störungen des laufenden Betriebs führen können.

Social Engineering

Alle Gesprächspartner des Finanzsektors sind sich dieses Risikos bewusst, bewerten dessen Bedeutung aber unterschiedlich.[69] Aufschlussreich ist, dass es Finanzakteure gibt, die nicht nur mit Schulungsmaßnahmen zur Aus- und Weiterbildung ihrer Mitarbeitenden beitragen, sondern die Sensibilisierung ihrer Mitarbeitenden für Sicherheitsfragen teilweise mit Unterstützung staatlicher Sicherheitsbehörden überprüfen.

69 In zwei Fällen wurde das Risiko als sehr hoch, in den beiden anderen Fällen als niedrig bewertet.

Verteilte Angriffe auf Systeme (DDoS)

Die Beurteilung dieses Risikos variiert mit dem Grad der Abhängigkeit der jeweiligen Unternehmen von Leistungen, die des Internets bedürfen. Vor allem kommerziell tätige Bankinstitute sind von DDoS-Attacken direkt betroffen, beispielsweise wenn sich diese gegen das Online-Banking oder auch die Geldautomaten richten. Zusätzlicher Personaleinsatz kann aus Sicht der Gesprächspartner teilweise helfen, die möglichen Systemausfälle zu kompensieren.

Manipulierte bzw. unsichere Hardware

Die meisten Gesprächspartner beschreiben und bewerten dieses Risiko gleich wie die Gefahr fehlerhafter bzw. inkompatibler Codes und Software. Explizit erwähnt wurde die Gefahr manipulierter Hardware, wie z.B. Geldautomaten oder Automaten, die am Verkaufsort eingesetzt werden, ohne dass es sich dabei jedoch um Vorfälle handelte, die bei entsprechenden Unternehmen in Österreich auftraten. Abnahmetests und Zertifizierungen sind wichtige Maßnahmen, um mit diesem Risiko umzugehen.

Mangelndes Sicherheitsbewusstsein

Nach Einschätzung der Befragten ist das Sicherheitsbewusstsein im Finanzsektor generell hoch. Gleichwohl gibt es Übereinstimmung darin, dass die Anstrengungen künftig verstärkt werden müssen, sei es durch Zertifizierung anhand sicherheitsrelevanter Standards oder Aus- und Weiterbildung. Gerade in diesem Zusammenhang wird aber auch auf das Spannungsverhältnis zwischen Sicherheit und Kosten hingewiesen und die Rolle des Staates bei der Förderung der Sicherheit von strategischen Infrastrukturbetreibern angesprochen (Kapitel 8.5).

Fahrlässiges Verhalten in strategischen Infrastrukturbetrieben

Die Gesprächspartner unterscheiden in diesem Punkt zwischen dem Verhalten innerhalb des Finanzsektors und anderen strategisch relevanten Infrastruktursektoren. Fahrlässigkeit in anderen Sektoren ist in den Auswirkungen mit anderen Risiken zu vergleichen, wie z.B. dem Stromausfall, wenn diesem entsprechende Nachlässigkeit bei Energieversorgern vorausgehen würde. Gegen die negativen Folgen fahrlässigen Verhaltens im Finanzsektor bzw. in einzelnen Finanzinstituten setzen diese auf die technische Segmentierung ihrer Netze, mit

deren Hilfe Kaskadeneffekte verhindert bzw. die damit verbundenen Auswirkungen eingedämmt werden sollen. Auch hier gilt es allerdings zu unterscheiden, welche Prozesse betroffen sind.

Keine systematische Technologiefolgenabschätzung

Die Bedeutung dieses Themas variiert erneut mit dem Marktsegment, in dem die jeweiligen Unternehmen tätig sind. Aus Sicht der Gesprächspartner einer Geschäftsbank und eines Betreibers wichtiger Infrastrukturen des Finanzsektors gehört die Technologiefolgenabschätzung zu den strategisch wichtigen Fragen. Das gilt vor allem für das Zusammenspiel von Technologie, Komfort und Einfachheit der Bedienung sowie Sicherheit der Datenübermittlung, wie das Beispiel Near Field Communication für bargeldloses Zahlen mit Mobiltelefonen oder speziellen Cash-Karten verdeutlicht.

Macht der sozialen Netze und deren Manipulation

Vor allem die kommerziellen Banken sehen in sozialen Netzen ein Medium, das gezielt genutzt werden kann, um den Ruf von Unternehmen zu schädigen. Darüber hinaus wird auch die Gefahr gesehen, dass soziale Netze genutzt werden, um interne Sicherheitsstandards zu umgehen und möglicherweise Daten aus den Unternehmen zu schmuggeln. Mitarbeiterschulung und der professionelle Umgang mit diesen Medien auch durch die internen Kommunikationsabteilungen sind Maßnahmen, die als Antwort auf die mögliche Gefährdung ergriffen werden.

Manipulation von Kommunikations- und Satellitenverbindungen

Kommunikationsverbindungen stellen neben der Energieversorgung die zweite Schnittstelle des Finanzsektors zu einem anderen strategisch relevanten Infrastruktursektor dar. Das Risiko der Manipulation von Kommunikationsverbindungen wird generell als hoch eingeschätzt. Besondere Abhängigkeiten von Kommunikationstechnologie, wie sie im Bereich des Hochfrequenzhandels gegenwärtig festzustellen sind (Kapitel 4.2), wurden dabei allerdings nicht explizit erwähnt. Im Bargeldtransport spielt darüber hinaus auch die Abhängigkeit von Satellitenverbindungen eine Rolle, um Werttransporte zu lokalisieren.

Nicht erkannte (IKT-)Anomalien

Die Bewertung dieses Risikos fällt unterschiedlich aus. Allgemein wird auf verschiedene technische und nicht-technische Lösungen hingewiesen, um Auffälligkeiten zu erkennen.

Verletzlichkeit der IKT-Infrastruktur durch Naturkatastrophen

Das Geschäftsmodell der Unternehmen und auch die Verteilung ihrer Standorte wirken sich auf die Antworten zu dieser Risikokategorie aus. Alle Gesprächspartner nennen die Behinderung des Geschäftsbetriebs als unmittelbare Konsequenz der möglichen Folgen von Naturkatastrophen. Die Absicherung dagegen kann mit hohen Kosten verbunden sein, wenn Finanzinstitute in mehrere alternative Standorte für ihre Rechenzentren investieren.

CYBERRISIKEN UND ÖSTERREICHS IKT-SEKTOR

© Guido Vrola – Fotolia.com

5.1. Österreichs IKT-Sektor: Relevanz in Zahlen
5.2. Cyberrisiken im IKT-Sektor: Allgemeine Bewertung und Trends
5.3. Cyberrisiken im IKT-Sektor: Österreichische Bewertung

5

5.1. Österreichs IKT-Sektor: Relevanz in Zahlen

- Der **Bruttowertschöpfungsanteil** des IKT-Sektors in Österreich lag 2009 bei ungefähr 30 Milliarden € oder gut 18 % der gesamtwirtschaftlichen Bruttowertschöpfung. Auf die Herstellung von Datenverarbeitungsgeräten und elektrischer Ausrüstung entfielen dabei etwa 15,5 Milliarden €, der Rest auf Telekommunikation, IT-Dienstleistungen sowie Informationsdienstleistungen.[70]

- Die knapp 13.300 Unternehmen des österreichischen IKT-Sektors beschäftigten 2009 ungefähr 135.000 **Mitarbeitende.**[71] 2008 stellten die IKT-Unternehmen in Österreich Produkte, Systeme, Komponenten und Dienstleistungen im Wert von 18,5 Milliarden € her.[72]

- Auf 100 in Österreich lebende Personen entfielen 2009 ca. 137 **Mobilfunkanschlüsse,** was deutlich über dem OECD-Durchschnitt von 102 Anschlüssen lag. Innerhalb der OECD zählte Österreich damit zur Spitzengruppe. Bei den **Breitbandanschlüssen** entfielen im gleichen Jahr etwa 23 Anschlüsse auf 100 Einwohner, womit Österreich im OECD-Vergleich den 19. Rang belegte. Auf Platz eins lag Dänemark (37,34 Anschlüsse) gefolgt von den Niederlanden (37,09).[73]

- 72 % der Privathaushalte in Österreich verfügten 2011 über einen **Breitbandzugang** zum Internet (EU-27: 67 %). Bei den Unternehmen Österreichs lag der Anteil mit Breitbandzugang zum Internet im gleichen Jahr bei 82 % (EU-27: 87 %).[74]

- 44 % der in Österreich lebenden **Personen** nutzten 2011 das **Internet,** um Waren oder Dienstleistungen zu bestellen, was in etwa dem Durchschnitt der EU-27 von 43 % entspricht. Bei den **Unternehmen** lag der Anteil mit 41 % deutlich über dem EU-Durchschnitt von 19 %. Damit zählten Österreichs Unternehmen gemeinsam mit Irland und Schweden zur EU-Spitzengruppe.[75]

- 2010 lagen die **IKT-Ausgaben** in Österreich bei 2 % des BIP, leicht unter dem Durchschnitt der EU-27 von 2,5 %. Führend waren in diesem Bereich Großbritannien (3,8 %) und Finnland (3,3 %).[76]

70 Siehe zur Bruttowertschöpfung die Daten von Statistik Austria <http://www.statistik.at/web_de/services/wirtschaftsatlas_oesterreich/branchendaten_nach_wirtschaftszweigen/index.html> (Zugriff: 3. April 2012).
71 Ebd. Der Löwenanteil entfiel dabei auf die Herstellung von elektrischen Ausrüstungen (43.673 Mitarbeitende) und IT-Dienstleistungen (35.986 Mitarbeitende).
72 IKT Made in Austria, S. 4.
73 OECD Communications Outlook 2011, S. 160, S. 164.
74 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00089&plugin=1>; <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00090&plugin=1> (Zugriff: 3. April 2012)
75 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00096&plugin=1> (Zugriff: 3. April 2012).
76 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tsiir090&plugin=1> (Zugriff: 3. April 2012).

- Der Anteil des **elektronischen Geschäftsverkehrs am Gesamtumsatz** der Unternehmen lag in Österreich 2011 bei 14 %, was genau dem EU-Durchschnitt entsprach. Führend war die Tschechische Republik (25 %), gefolgt von Finnland (20 %).[77]
- Der Anteil der Unternehmen, deren **Geschäftsprozesse automatisch** mit denen ihrer Zulieferer und/oder Kunden verbunden sind, lag in Österreich 2010 bei 14 %, womit Österreich unter dem Durchschnitt der EU-27 von 18 % lag. Führend waren Kroatien (53 %) und Portugal (40 %).[78]

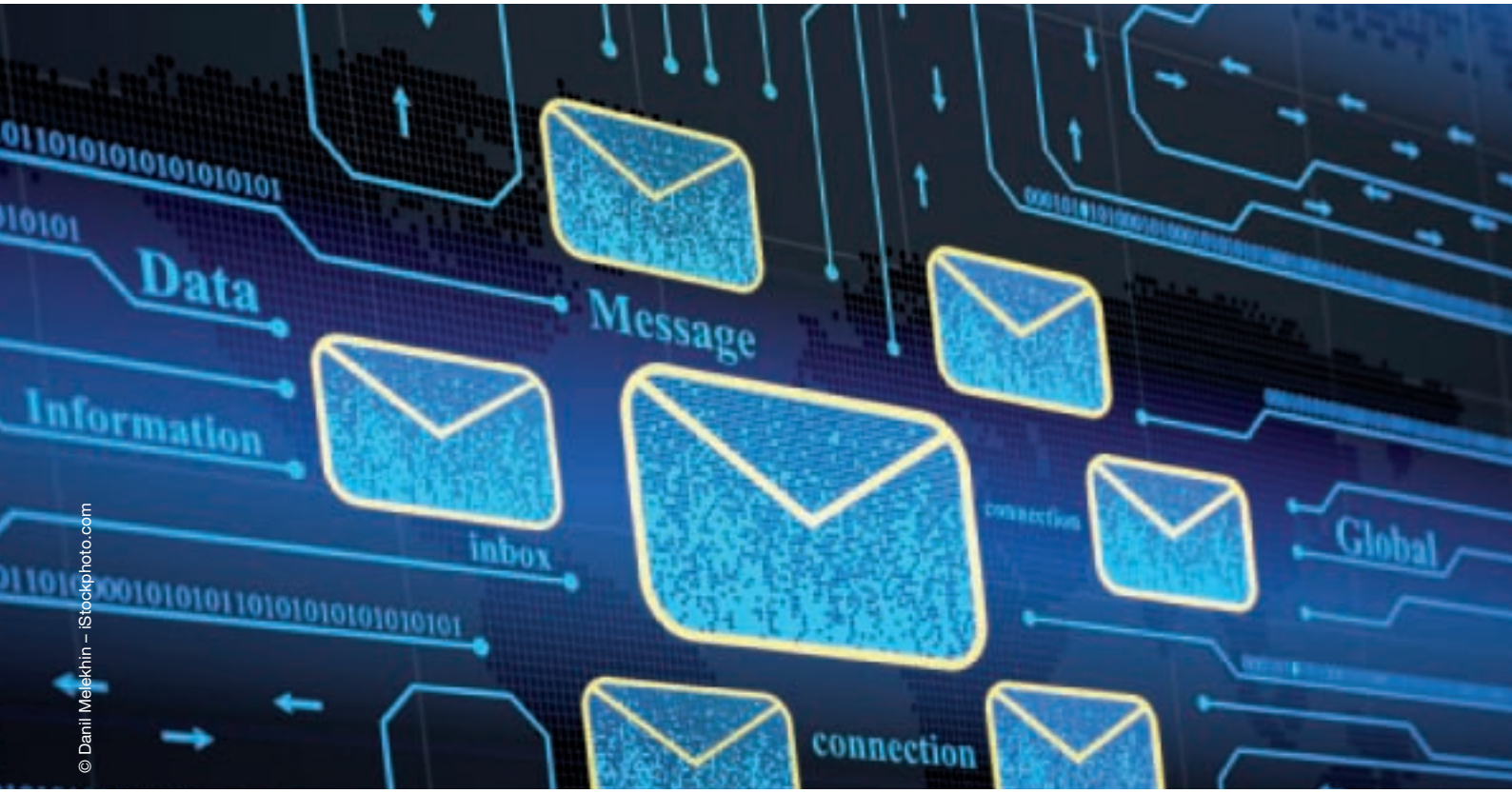
5.2. Cyberrisiken im IKT-Sektor: Allgemeine Bewertung und Trends

Wie der Verkehrssektor erbringt der IKT-Sektor eine grundsätzliche Transportdienstleistung, nur in diesem Fall im digitalen Umfeld. Der IKT-Sektor ermöglicht es den Nutzern, Daten zu erfassen, zu be- und verarbeiten, zu speichern und zu übertragen. Konnektivität und Erreichbarkeit sind deshalb die zentralen Beiträge des IKT-Sektors in einem globalisierten Wirtschaftsumfeld. Ein Blick auf erkennbare Entwicklungstrends deutet an, dass die Nachfrage nach Konnektivität künftig deutlich steigen wird – und damit eine Verschmelzung der Dienste bewirkt, die in den bislang strukturell voneinander getrennt organisierten Infrastruktursektoren angeboten werden:

- Das Volumen des weltweiten, auf Internetprotokollen basierenden Datenaufkommens dürfte bis 2015 auf monatlich 80 Exabytes steigen.[79]
- Die Zahl von gut sechs Milliarden Telefonen, die weltweit genutzt werden, erscheint schon immens. Sie verblasst aber vor dem Hintergrund der Schätzung, dass bis 2020 gut 50 Milliarden Geräte miteinander kommunizieren werden.[80]
- Im Online-Geschäft für digitale Dienste knackten Apple-Nutzer im Frühjahr 2012 die Marke von 25 Milliarden heruntergeladenen Diensten; bis 2014 könnten weltweit mehr als 70 Milliarden digitale Dienste für verschiedene Plattformen heruntergeladen werden.[81]

Die Liste der Beispiele lässt sich beliebig weiterführen. Für die nationale Bewertung von Cyberrisiken ist die Botschaft klar: die Angriffs- und Verwundbarkeitsfläche nimmt dramatisch zu – und zwar in allen Dimensionen des staatlichen, wirtschaftlichen und privaten Handelns.

Diese Betrachtung ist maßgebend, wenn es darum geht, die Quellen der Verwundbarkeit im IKT-Sektor zu identifizieren, um darauf in geeigneter Weise zu reagieren. Abbildung 9 illustriert hierzu in allgemeiner Form die verschiedenen Elemente der IKT-Wertschöpfungskette. Sehr stark vereinfacht kann bei der Telekommunikation zwischen verschiedenen Formen der Übertragung im Fest- und Mobilnetz, auf Basis von internetbasierten Protokollen (IP) oder per Funk bzw. Satellit unterschieden werden. Informationstechnologie ist fester Bestandteil der Komponenten, die in der Telekommunikation zur Anwendung kommen. Dieser hohe Grad der Verknüpfung stellt für die Risikoanalyse eine besondere Herausforderung dar: Die Hardware mit ihren unterschiedlichen Komponenten und Endgeräten wird ergänzt durch eine unüberschaubare Anzahl von Softwareanwendungen im Bereich der Betriebssysteme, der Datenbanken, der Sicherheit (Schlüssel, Zertifikate, Virenschutz) sowie weiterer Kategorien. Angebote wie Cloud-Dienste lassen die Grenze zwischen Hard- und Software



© Danil Melekhin – iStockphoto.com

sowie zwischen Netzwerken zusehends verschwimmen. Hinzu kommt ein deutlicher Trend zur Software als Dienstleistung, der den Bezug von Software erleichtert, gleichzeitig aber auch neue Sicherheitsfragen nach Betrieb, Pflege und Bereitstellung der Softwaredienstleistung hervorruft. Alle diese Komponenten dienen im Wesentlichen einem Zweck, nämlich der Erstellung und dem Umgang mit Daten. Dabei handelt es sich um frei verfügbare Daten und um besonders schützenswerte Daten wie personenbezogene und klassifizierte Informationen. Diesen Daten gilt das Interesse möglicher Täter. Dass die Daten dabei selbst Ziel illegaler Handlungen sind und zusätzlich über die Hard- und Softwarekomponenten der dafür benötigten Infrastruktur angegriffen werden können, macht den Datenschutz zu einer entsprechend anspruchsvollen Aufgabe.

Die Komplexität des Datenschutzes und des Schutzes verschiedener Elemente der IKT-Wertschöpfungskette vor verschiedenen Risiken illustrieren die folgenden Beispiele:

Angriffe gegen Anbieter von Telekommunikations- und Internetdiensten

Hinter Angriffen gegen Telekommunikations- und Internetdienstleister können neben dem Ziel des illegalen Zugangs zu Daten auch politische Motive stehen. Prominentestes Beispiel dafür sind die Probleme des Internetriesen Google mit Google Mail in China. Nachdem das Unternehmen der chinesischen Regierung im März 2011 vorwarf, den E-Mail-Dienst des Unternehmens zu blockieren, kam es im Juni

77 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00110&plugin=1> (Zugriff: 3. April 2012).
78 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00115&plugin=1> (Zugriff: 3. April 2012).
79 Cisco Visual Networking Index, S. 6, 9. Dabei entspricht ein Exabyte einer Trillion Bytes.
80 OECD Communications Outlook 2011, S. 5; Emmerson, „M2M: the Internet of 50 billion devices“, S. 19–22.
81 „Das Smartphone als Verkaufsplattform“, S. 35.

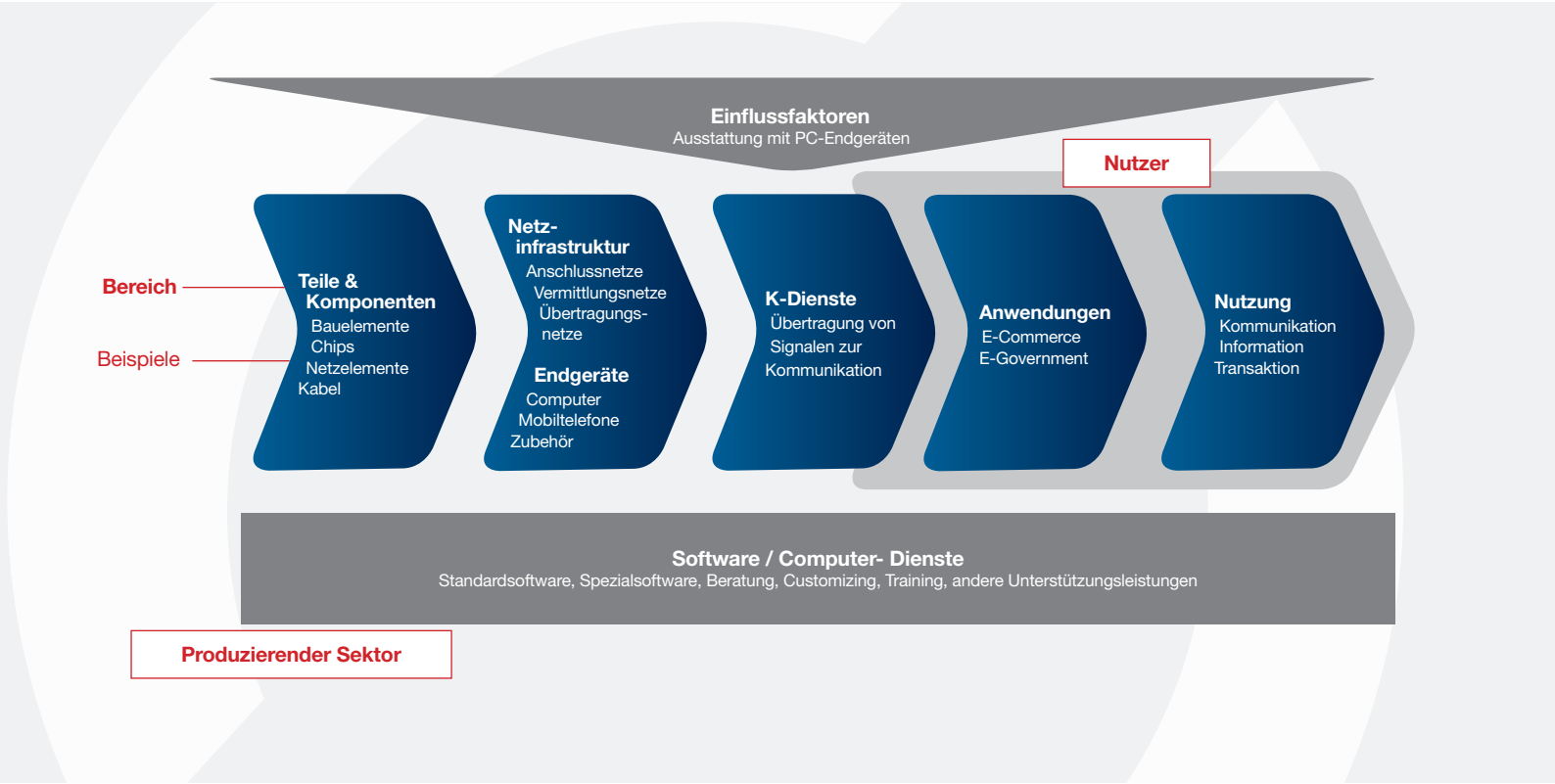


Abbildung 9: IKT-Wertschöpfungskette
Quelle: Reichardt/Serentschy, „Der IKT-Masterplan", S. 17

des gleichen Jahres zu versuchten Angriffen auf Konten von Google Mail, die Regierungsvertreter, Journalisten und Aktivisten genutzt hatten.[82] Eindeutig kriminelle Motive lagen wohl dem Vorgehen jener Telefon-Hacker zugrunde, die Mitte 2011 in Systeme der Deutschen Telekom eindrangen, um durch Manipulation der PIN-Nummer den Rufverkehr auf teurere ausländische Nummern umzuleiten.[83] Gegen solche und andere Vorfälle setzen sich Telekommunikationsbetreiber aktiv zur Wehr. So hat die Deutsche Telekom jüngst Maßnahmen ergriffen, die es ermöglichen, Angriffe gegen Smartphones in Echtzeit zu registrieren und zu beobachten. Dabei werden Server eingesetzt, die vorgeben, ein Smartphone zu sein, um dadurch Hacker anzulocken.[84]

Angriffe gegen Anbieter von IKT-Sicherheitslösungen

Die hohe Verbreitung spezifischer Produkte zur Verbesserung des Schutzes gegen Cyberrisiken macht deren Anbieter zu besonders attraktiven Zielen für mögliche Täter. Im März 2011 wurde das US-amerikanische Unternehmen RSA, ein Anbieter von Lösungen für sichere digitale Identitäten, Opfer eines Angriffs. Die Entwendung von Daten aus dem Unternehmen wurde möglich über Schadsoftware, die im Anhang eines Dokumentes enthalten war, das verschiedene Mitarbeiter des Unternehmens per E-Mail erhalten und vereinzelt auch geöffnet hatten.[85] Nur wenige Monate später wurden die Zertifikate für die SSL-Verschlüsselung des Unternehmens DigiNotar geknackt. In der Folge stellten Betrüger falsche Zertifikate aus. Dieser Vorgang blieb nicht ohne Folgen, denn die niederländischen Behörden entzogen daraufhin dem Unternehmen ihr Vertrauen und kündigten diesen Schritt in einer Pressekonferenz an.[86] Einen ähnlichen Vorfall gab es 2006 auch bei Symantec, einem Hersteller von Antivirensoftware. Nach Presseberichten wurde der Quellcode für verschiedene Softwareprodukte entwendet und im Januar 2012 im Internet veröffentlicht. Nach Unternehmensangaben besteht für die Nutzer aktueller Softwareversionen keine Gefahr.[87]

Angriffe gegen Anbieter sozialer Medien

Anbieter sozialer Medien und blog-basierte Medienunternehmen sind ebenfalls beliebte Ziele. Oftmals geht es den Angreifern um den Zugriff und meist auch die Veröffentlichung der Nutzerdaten. Beim Eindringen in die Datenbank von Gawker Media wurden 2010 über 1,3 Millionen Nutzerdaten entwendet.[88] Die in die Rechner von Twitter eingedrungenen Hacker knackten verschiedene Nutzerkonten, darunter auch dasjenige des damaligen US-Präsidentschaftskandidaten Barack Obama sowie Twitter-Mitteilungen des Nachrichtensenders Fox News.[89] Dieses Beispiel ist mit Blick auf die Manipulation sozialer Medien und die damit verbundenen Auswirkungen für die Kommunikation von Behörden und Unternehmen von Relevanz.

Cyberspionage gegen Ausrüster

Anfang 2012 wurde bekannt, dass sich Unberechtigte Zugang zu den Datensystemen des ehemaligen US-Telekommunikationsausrüsters Nortel verschafft und das Unternehmen offenbar jahrelang ausspioniert hatten. Nach Presseberichten hatten die Täter Zugriff auf alle relevanten Unternehmensdaten. Das Eindringen sei erst 2004 entdeckt worden. Offenbar äußerten sich Unternehmensverantwortliche in der Vergangenheit nicht darüber, ob und in welcher Form Produkte des Unternehmens durch diesen Angriff möglicherweise kompromittiert wurden.[90]

Manipulation der Transportinfrastruktur

Die Manipulation der digitalen Transportinfrastruktur dient dazu, den Datenverkehr umzuleiten, und dürfte in der Regel mit der Absicht erfolgen, die Daten dabei auszulesen. Durch die bewusste Veränderung des Border Gateway Protocol (BGP), das die Verbindung zwischen Netzwerken herstellt, ist eine Umleitung des Datenverkehrs möglich. Das geschah im November 2010, als gut 15 % des weltweiten Internetverkehrs für knapp 18 Minuten auf chinesische Server umgeleitet wurden. Über einen ähnlichen Vorfall berichtete die Presse 2008, als der Datenverkehr für die Online-Videoplattform YouTube aufgrund der Maßnahmen eines Internetdienstleisters aus Pakistan während zwei Stunden umgeleitet wurde. Eine andere Form der Manipulation besteht darin, das System zur Bezeichnung von Internetdomänen (Domain Name System, DNS) zu verändern. Einer DNS-Manipulation fielen 2009 die Kunden einer brasilianischen Bank zum Opfer. Sie landeten auf einer gefälschten Website, die dazu diente, Benutzernamen und Kennwörter abzugreifen.[91]

Eingeschränkte Verfügbarkeit von Cloud-Diensten

Mit der zunehmenden Popularität von Cloud-Diensten wächst auch die Abhängigkeit von deren Betreibern. Im April 2011 kam es im Zuge der Softwareaktualisierung bei Amazon Web Services zu einem Fehler, der in einer Kettenreaktion zur Nichtverfügbarkeit der Cloud-Dienste für zwei Tage führte. Die Unterbrechung beim Marktführer hatte Konsequenzen für zahlreiche seiner Nutzer und andere Web-Dienste, wie z.B. die Online-Nachrichten-Plattform Reddit und das soziale Netzwerk Foursquare.[92] Mit ähnlichen Folgen traf es im Oktober 2011 auch die Nutzer von Blackberry-Diensten, die nach dem Ausfall eines Elementes der unternehmenseigenen IT-Landschaft, die monatlich ein Datenvolumen von 25 Petabytes verarbeitet, nicht mehr verfügbar

82 „Google wirft China die Störung von Google Mail vor"; „Angriffe auf E-Mailkonten chinesischer Aktivisten".
83 „Telefonanlagen gehackt: Mehrere tausend Euro Schaden".
84 „Telekom lockt Hacker zu Life-Angriffen auf Smartphone".
85 Richmond, „The RSA Hack: How They Did It".
86 Arthur, „DigiNotar SSL certificate hack amounts to cyberwar, says expert".
87 Finkle, „Symanteck Hack: Company Admits Hackers Stole Norton Source Code in 2006".
88 Sreenivasan, „Gawker Data Breach Could Lead to Attacks on Government Agencies".
89 „Micro-Blog Twitter gehackt".
90 „Nortel hit by suspected Chinese cyberattacks for a decade".
91 Barnett, „Cybersecurity: Threats to Communications Networks and Public-Sector Responses", S. 5–6.
92 Tibken/Russolillo, „Amazon Glitch Hobbles Websites"; „Summary of the Amazon EC2 and Amazon RDS Service Interruption".

waren.[93] Cloud-Dienste sind wie andere Datendienste nicht nur anfällig für Ausfälle, die sich aus der technischen Komplexität ergeben, sondern weisen auch Lücken auf, die ausgenutzt werden können. Das demonstrierten nach eigenen Angaben Forscher der Ruhr-Universität Bochum, die Schwächen im Sicherheitssystem von Amazon Web Services nachwiesen. Diese seien nach Bekanntwerden sofort geschlossen worden, teilten die Forscher in einer Presseerklärung mit.[94]

Gefahr gefälschter Bauteile

Produktfälschung ist für Unternehmen ein großes Risiko, weil damit Reputationsverluste und die Schädigung des Markenwerts verbunden sind. Wenn Produktfälschungen gezielt erfolgen, um beispielsweise die Funktionalitäten einer Anwendung von außen zu steuern, erreicht das Problem eine Schwelle, die auch für die nationale Sicherheitsvorsorge relevant ist. Vor allem dann, wenn die entsprechenden Bauteile von Infrastrukturbetreibern in strategisch bedeutsamen Sektoren eingesetzt werden. Anstelle vieler Beispiele aus dem IKT-Sektor sei auf das Problem gefälschter Bauteile des US-Netzwerkherstellers Cisco hingewiesen. Unter den Bezeichnungen „Operation Cisco Raider“ und „Operation Network Raider“ führten mehrere US-Behörden in den letzten Jahren Strafverfolgungsmaßnahmen gegen kriminelle Gruppen durch, die gefälschte Cisco-Bauteile in den USA einführten. Dabei wurden mehr als 94.000 Komponenten mit einem Verkaufswert von 86 Millionen $ beschlagnahmt. Einige der Lieferungen gingen auch an die US-Streitkräfte sowie an das FBI.[95]

93 Reißmann/Lischka, „Blackberry-Ausfall: Die Cloud-Katastrophe; Totzke, „Cybersecurity: The Pivotal Role of Communications Networks“, S. 4.
94 „Cloud Computing: ‚Wolke’ mit Lücken“.
95 „Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware“.
96 Die Ausführungen basieren auf Interviews vom 24. Januar 2012, 7.– 9., 13., 15., 22. und 23. Februar 2012 sowie 20. April 2012.

Österreichs IKT-Sektor: Österreichische Bewertung

5.3.

Wie vor dem Hintergrund der oben beschriebenen allgemeinen Gefährdung die spezifische Bewertung der befragten IKT-Experten in Österreich ausfällt, illustriert Abbildung 10. Auf den ersten Blick möglicherweise überraschend ist der Umstand, dass auch die IKT-Experten die Rolle des Menschen im Umgang mit IKT als besonders wichtig erachten. Das kommt in der hohen Bewertung jener Risiken zum Austruck, die mit fehlendem Fachpersonal, mangelndem Sicherheitsbewusstsein und der Gefahr der Manipulation durch Social Media einhergehen können.

Ebenfalls deutlich stärker als die übrigen Experten betonen die IKT-Fachleute die sektorübergreifenden Abhängigkeiten. Das Risiko fahrlässigen Handelns erhält mit deutlichem Abstand den höchsten Wert in der gesamten Bewertung der Cyberrisiken. Auch die Relevanz fehlender bzw. unzureichender unternehmerischer Notfallvorsorge (BCM) betonen die Gesprächspartner des IKT-Sektors stärker als die anderen Interviewpartner. Das mag mit der besonderen Sensibilität für die unternehmensweiten und sektorübergreifenden Folgen der IKT-Störung bzw. des IKT-Ausfalls zusammenhängen.

Ausdruck der Gefährdung der eigenen Geschäftsprozesse sind die mit hohen Relevanzwerten eingestuften Risiken fehlerhafter bzw. inkompatibler Codes/Software, manipulierter Kommunikations- und Satellitenverbindungen, geknackter digitaler Schlüsselsysteme und unsicherer Steuerungsinstrumente. Dass die IKT-Unternehmen schließlich auch attraktive Ziele für Cyberspionage und Cyberkriminelle darstellen, verdeutlicht die entsprechende Bewertung dieser beiden Risiken. Auffällig ist dabei, dass das Risiko der Cyberspionage von den IKT-Experten deutlich höher bewertet wird als von den anderen privatwirtschaftlichen Gesprächspartnern.

Im Einzelnen beschrieben die IKT-Experten die 15 wichtigsten Cyberrisiken wie folgt:[96]

Fahrlässiges Verhalten in strategischen Infrastrukturbetrieben

Diese Risikokategorie erhielt die höchste Bewertungsnote. In die Antworten flossen auch Aspekte ein, die Verbindungen zu anderen Risikokategorien aufzeigen. So wurde angesprochen, dass der vorherrschende Kostenfokus zu einem weitgehenden Abbau von redundanzfördernden Maßnahmen führt, was gerade in strategisch bedeutenden Infrastrukturbetrieben problematisch sei. Wichtig war den Gesprächspartnern auch der Hinweis auf die Rolle der Mitarbeitenden in Unternehmen, die national von strategischer Bedeutung sind. Seitens der IKT-Anbieter wurde insbesondere betont, dass verschärfte Sicherheitsregeln gelten, wenn die eigenen Mitarbeitenden auf der Kundeninfrastruktur dieser Unternehmen arbeiten. Hierfür und auch für andere Aspekte der eigenen Tätigkeit sehen die Unternehmen mehrerer Gesprächspartner regelmäßige Audits vor, damit das Eigenrisiko und das mögliche Risiko der Kunden eingeschränkt werden kann.

Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

Auch wenn das Risiko generell als hoch bewertet wurde, gingen die Meinungen be-

züglich seiner Bedeutung doch auseinander. Dabei zeigte sich, dass die von den Unternehmen verfolgten Geschäftszwecke einen Einfluss auf die Bewertung haben. Vor allem die Vertreter der Unternehmen mit einem Versorgungsauftrag und mit Verantwortung für den Betrieb von IKT-Infrastrukturen bewerten das Risiko deutlich höher als beispielsweise klassische Softwarehersteller.

Fehlendes oder unzureichendes BCM

In der hohen Bewertung dieser Risikokategorie kommen die Eigensicht der IKT-Experten und vor allem deren Einblicke in den Stand der Krisenvorsorge anderer Unternehmen zum Ausdruck. Geht es um das eigene Geschäftsrisiko, sagen die IKT-Vertreter, dass ihre Unternehmen über umfassende BCM-Ansätze verfügen. Deren Notwendigkeit ergibt sich teilweise auch aus den branchenspezifischen Risikomanagement- und Sicherheitsstandards, deren Einhaltung durch die IKT-Betreiber von den Kunden erwartet werde. Bei der Bewertung der Sicherheitsvorsorge anderer Unternehmen gehen die Urteile leicht auseinander. Während ein Gesprächspartner argumentierte, BCM sei für seine Kunden kein „heißes“ Thema, weil es vermutlich bereits ausreichend berücksichtigt werde, sprachen mehrere andere IKT-Experten davon, dass das Fehlen ausreichender BCM-Policies und -Prozesse in anderen Sektoren ein Risiko darstelle.

Fehlerhafte und inkompatible Codes/Software

Nur ein einziger Gesprächspartner bewertete dieses Risiko als weniger relevant, während es in der Prioritätenliste der anderen oben bzw. ganz oben stand. Vor allem die Gesprächspartner, deren Unternehmen Dienste anbieten und IKT-Infrastrukturen betreiben, betonten die weitreichenden Folgen, die sich aus fehlerhafter und inkompatibler Software bzw. Codes ergeben können. Die Bedeutung des Risikos wird aus Sicht einzelner Experten sogar noch zunehmen, weil die Komplexität durch die IKT-basierte Verknüpfung verschiedener Abläufe in einzelnen Infrastruktursektoren deutlich zunehmen wird. Neben entsprechender Sorgfalt bei der Programmierung, umfangreichen Tests vor der Einführung, der Beratung von Kunden im Zusammenhang mit der Einführung neuer Softwarereleases sprach ein Experte auch die Beschaffungspolitik (Single-Vendor- vs. Multi-Vendor-Ansatz) als Instrument der Risikovermeidung an.

Manipulation von Kommunikations- und Satellitenverbindungen

Vor allem die Betreiber von Kommunikationsinfrastrukturen erachten die Gefahr der Manipulation ihrer Verbindungsinfrastruktur als sehr relevant. Das gilt ganz besonders im Satellitenbereich, wo weniger Redundanzen vorhanden sind. Eine direkte Verbindung zwischen der Manipulation von Kommunikations- und Satellitenverbindungen sowie dem Risiko manipulierter bzw. unsicherer Hardware (Supply Chain Risk Management) stellten die Gesprächspartner nicht her.

Cyberspionage

Vertreter forschungs- und entwicklungsintensiver IKT-Unternehmen betonen die Relevanz der Cyberspionage. Im Umfeld der Infrastrukturbetreiber fiel die Bewertung dagegen eher tiefer aus. Aufschlussreich ist allerdings, dass es gerade der Vertreter eines IKT-Infrastrukturbetreibers war, der darauf hinwies, dass sein Konzern ein eigenes Spionageabwehrprogramm lanciert habe. Der Vertreter eines IKT-Komponentenherstellers ergänzte, dass der Umgang mit dem Spionagerisiko Teil des konzernweiten Supply Chain Risk Managements sei.

Fehlendes Fachpersonal

In der Sorge um die negativen Folgen fehlenden Fachpersonals mischt sich auch die

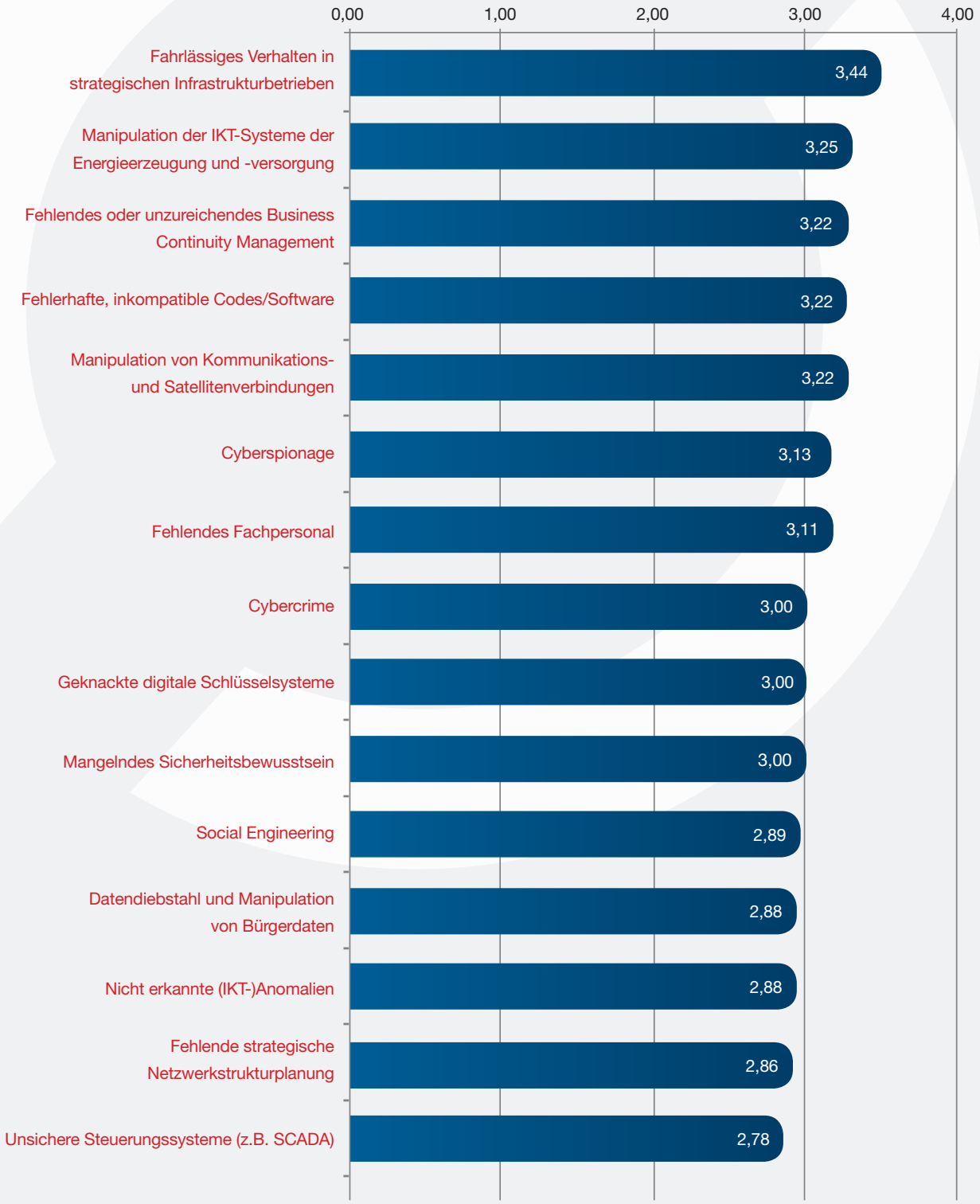


Abbildung 10: Top-15-Cyberrisiken aus Sicht der Interviewpartner des IKT-Sektors
Quelle: KSÖ-Interviewserie

Kenntnis der IKT-Experten, dass die künftigen Anwendungen und damit auch das Umfeld, in dem die Mitarbeitenden tätig sind, aufgrund des Zusammenwachsens von Diensten und Infrastrukturen noch anspruchsvoller werden. Insgesamt überwog bei den Gesprächspartnern die Ansicht, dass zwar nach wie vor in Techniker investiert werde, dass aber die Sicherheitsausbildung insgesamt zu kurz komme. Das gilt auch mit Blick auf den immer bedeutender werdenden Aspekt der Auslagerung von Tätigkeiten und von Personal. Unter Hinweis auf Empfehlungen aus dem IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) erwähnte ein Gesprächspartner das Risiko des Verlusts von eigener Expertise durch Auslagerung, das sich in der Risikobewertung der Unternehmen niederschlagen müsse.[97]

Cybercrime

Die Unternehmen verschiedener IKT-Gesprächspartner waren selbst Opfer der Cyberkriminalität, meist in Form des Diebstahls von Kundendaten. Dementsprechend ausgeprägt ist das Bewusstsein für Maßnahmen, die dazu beitragen, die eigenen Systeme und die Kunden zu schützen. Die jüngste Novelle des Telekommunikationsgesetzes (§ 16a) hat die diesbezügliche Verpflichtung der Betreiber von Kommunikationsinfrastrukturen verstärkt.

Geknackte digitale Schlüsselsysteme

Zusammen mit der Bewertung der Risiken einer lückenhaften Cyber Governance war dies der einzige Punkt, bei dem die Bewertungen der Gesprächspartner die gesamte Bewertungsskala von 1–4 abdeckten.[98] Gerade vor dem Hintergrund der in Kapitel 5.2 beschriebenen Beispiele wurde die Relevanz des Risikos geknackter digitaler Schlüsselsysteme aber insgesamt als hoch eingestuft. Ein Experte erwähnte, dass von seinem Unternehmen ein Auditverfahren zur Überprüfung von Zertifikaten entwickelt wurde.

Mangelndes Sicherheitsbewusstsein

Dieser Risikofaktor wurde aus einer ganz allgemeinen Betrachtung als hoch bewertet, ohne dass die Gesprächspartner besondere Punkte explizit hervorhoben. Vereinzelt wurde, allerdings ohne vertiefende Hinweise, der Mangel an sicherheitsrelevanter Präventionsarbeit beklagt.

Social Engineering

In der Bewertung dieses Risikos fielen die Antworten wiederum sehr differenziert aus. Allerdings wurde der bei anderen Antworten erkennbare Bewertungsunterschied zwischen Betreibern von IKT-Diensten/-Infrastrukturen sowie Entwicklern und Anbietern von IKT-Produkten in diesem Fall durchbrochen. Dort, wo das Risiko als hoch bewertet wurde, verwiesen die Gesprächspartner auch auf spezielle interne Sicherheitsmaßnahmen, um dem Risiko zu begegnen. Diese reichen von Mitarbeiterschulung über die gesonderte Absicherung des Zugangs zu spezifischen Räumlichkeiten bis zur Überwachung des Zugriffs auf besonders sensible Daten.

Datendiebstahl und Manipulation von Bürgerdaten

Mehrfach haben die IKT-Experten darauf hingewiesen, dass der Datendiebstahl in Zukunft eines der Hauptrisiken sein werde. Die regelmäßige Überprüfung der möglichen Schwachstellen der eigenen Systeme ist eine Maßnahme, die wiederholt als Mittel genannt wurde, um Machenschaften der Cyberkriminellen abzuwehren. Gleichwohl sind mehrere Experten der Ansicht, dass Unternehmen generell zu wenig gegen das Risiko des Datendiebstahls geschützt sind.

Nicht erkannte (IKT-)Anomalien

Die IKT-Experten bestätigen zwar das generelle Risiko nicht erkannter IKT-Anomalien. Bei

„Das Risiko der Cyberspionage wurde von den IKT-Experten deutlich höher bewertet als von den andern privatwirtschaftlichen Gesprächspartnern.“

© Eugeny Sverdlov – iStockphoto.com

der Frage, wie prioritär Maßnahmen sind, die helfen, das Problem zu bekämpfen, gehen die Meinungen aber auseinander. Vereinzelt nutzen die Unternehmen der Gesprächspartner Systeme, die dem Monitoring von Anomalien dienen.

Fehlende strategische Netzwerkstrukturplanung

Das Risikopotenzial einer fehlenden strategischen Netzwerkstrukturplanung war eines der wenigen Themen, bei denen das Spannungsfeld zwischen Sicherheit und Wettbewerb deutlich wurde. Einige Gesprächspartner betonten, dass das Problem durch vertraglich festgelegte Leistungsanforderungen (Service Level Agreement) gelöst werden könne. Andere argumentierten dagegen, dass die unterschiedliche Interessenlage zwischen den IKT-Betreibern gerade in diesem Punkt den Informationsaustausch eher erschwere, weil die Netzwerkstrukturplanung auch Auskunft über die Wachstumsstrategie einzelner Unternehmen gibt. Eine dritte Gruppe von Experten bemängelte die Zersplitterung der Zuständigkeiten und Aufgaben bei der generellen Planung und Entwicklung von Infrastrukturmaßnahmen in Österreich, wodurch die sektorübergreifende Koordination entsprechend erschwert wird.

Unsichere Steuerungssysteme (z.B. SCADA)

Für die Hersteller von IKT-Produkten, die mit Steuerungskomponenten zusammenwirken bzw. die Steuerungskomponenten schützen, hat das Risiko selbstredend eine sehr hohe Relevanz. Im Umfeld anderer befragter IKT-Experten werden SCADA-Elemente nicht eingesetzt, sodass die Relevanz nicht gegeben ist. Explizite Hinweise auf die Notwendigkeit eines stärkeren Dialogs mit den Herstellern von SCADA-Elementen, wie sie von den Gesprächspartnern anderer Sektoren geäußert wurden, machten die IKT-Experten nicht. ▮

97 Siehe hierzu den Maßnahmenkatalog M 2.250 Festlegung einer Outsourcing-Strategie des BSI unter: <https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02250.html> (Zugriff: 12. April 2012).
98 Die Bewertung mit dem Faktor 1 erklärt sich in diesem Fall mit dem Hinweis der entsprechenden Gesprächspartner, dass in ihrem Unternehmen keine digitalen Schlüssel eingesetzt werden.

CYBERRISIKEN UND ÖSTERREICHS TRANSPORTSEKTOR

© Henrik Jonsson – iStockphoto.com

6.1. Österreichs Transportsektor: Relevanz in Zahlen
6.2. Cyberrisiken im Transportsektor: Allgemeine Bewertung und Trends
6.3. Cyberrisiken im Transportsektor: Österreichische Bewertung

6

Österreichs Transportsektor: Relevanz in Zahlen

6.1.

- Der gesamte Transportsektor Österreichs beschäftigte 2010 gut 184.000 **Mitarbeitende** in beinahe 13.800 Unternehmen. Deren Anteil an der **Bruttowertschöpfung** lag 2009 bei ungefähr 8 %.[99]
- 2009 spielte der Schienenverkehr in Österreich verglichen mit den EU-27-Mitgliedern eine verhältnismäßig hohe Bedeutung, denn darauf entfielen 36 % des **Frachttransports** (EU-27: 17 %). Den Löwenanteil machte der Straßenverkehr mit 60 % aus (EU-27: 78 %). Volumenmäßig entsprach dies im Schienenverkehr 99 Millionen Tonnen, beim Straßenverkehr 337 Millionen Tonnen.[100]
- Mit 522 Personenkraftwagen bzw. 46 Lastkraftwagen pro 1.000 Einwohner wies Österreich 2009 eine höhere **Fahrzeugdichte** auf als Deutschland.[101]
- Volumenmäßig war der Schienenverkehr 2010 das wichtigste Transportmedium zur Abwicklung des **grenzüberschreitenden Güterverkehrs,** gefolgt vom Straßenverkehr und der Schifffahrt.[102]
- Das **Bundesstraßennetz** der Autobahnen und Schnellstraßen Österreichs erstreckt sich über eine Länge von gut 2,2 Millionen km. Seit 2000 wuchs dieses Netz um etwa 250.000 km. Auf ungefähr 340 km führt dieses Straßennetz durch Tunnel und überquert insgesamt mehr als 5.000 Brücken.[103]
- Das österreichische **Schienennetz** erstreckt sich auf eine Betriebslänge von 5.828 km. Davon waren Ende 2010 insgesamt 3.781 km ein- und 2.046 km zweigleisig befahrbar. Rund zwei Drittel der Betriebslänge waren elektrifiziert. Auf diesem Netz verkehren 645 Triebwagen, mehr als 2.500 Personen- sowie über 21.000 Güterwagen.[104]
- Österreichs **Flughäfen** wickelten 2010 den An- und Abflug von je ca. 12 Millionen Passagieren ab und bewältigten ein Frachtvolumen von 145.000 Tonnen im Anflug bzw. 79.300 Tonnen im Abflug. [105]

99 Statistik Austria, Jahrbuch 2012, S. 197. Der Löwenanteil entfiel auf den Landverkehr und den Transport in Rohrfernleitungen mit 101.311 Mitarbeitenden. Die Schifffahrt beschäftigte 422 Mitarbeitende. In der Luftfahrt waren es 7.856 Mitarbeitende, in der Lagerei sowie der Erbringung sonstiger Dienstleistungen für den Verkehr 47.317 und bei Post-, Kurier- und Expressdiensten 26.453 Mitarbeitende. Siehe zur Bruttowertschöpfung die Daten von Statistik Austria <http://www.statistik.at/web_de/services/wirtschaftsatlas_oesterreich/branchendaten_nach_wirtschaftszweigen/index.html> (Zugriff: 3. April 2012).
100 Energy, transport and environment indicators, S. 108, 110, 112.
101 Energy, transport and environment indicators, S. 90, S. 96.
102 Statistik Austria, Jahrbuch 2012, S. 434. Die wichtigste Kategorie war 2010 die Beförderung sonstiger Waren, die 42 % des Schienen- und 38 % des Straßenverkehrstransportvolumens ausmachte.
103 Statistik Straße & Verkehr, S. 9, 25, 27, 28.
104 <http://www.statistik.at/web_de/statistiken/verkehr/schiene/schienenfahrzeuge_bestand/index.html> (Zugriff: 3. April 2012).
105 Statistik Austria, Jahrbuch 2012, S. 442.

6.2. Cyberrisiken im Transportsektor: Allgemeine Bewertung und Trends

Mobilität ist ein Kernmerkmal der Globalisierung. Um Waren an unterschiedlichen Versorgungspunkten verfügbar zu machen und Menschen zu verschiedenen Destinationen zu befördern, sind Transport und Logistik unerlässlich. Im Hinblick auf die möglichst zeitverzugslose Belieferung der Nutzer und die damit verbundene Notwendigkeit hocheffizienter Abläufe spielt der Einsatz von IKT im Transport- und Logistiksektor eine zentrale Rolle. Dabei ist zu beachten, dass der Transport- und Logistiksektor einen sehr heterogenen Charakter aufweist, der aus einer Vielzahl verschiedener Akteure innerhalb der einzelnen Teilsektoren (Straße, Schiene, Luft, Wasser) resultiert. Daraus entstand im Laufe der Jahre eine Konföderation unterschiedlichster IKT-Systeme, die miteinander verknüpft wurden.[106] Das macht bereits deutlich, dass es Ansätze für den gesamten Verkehrssektor kaum gibt, sondern sich diese immer auf einzelne Segmente beziehen. Das gilt in der Regel auch für die Sicherheitsüberlegungen. Hinzu kommt, dass der Transport- und Logistiksektor weltweit unter hohem Kostendruck agiert.

Im Rahmen multimodaler Verkehrs- und Logistikkonzepte geht es darum, den Beitrag der einzelnen Verkehrsträger möglichst passgenau auf die Partnerorganisationen abzustimmen, um die logistische Wertschöpfungskette zu optimieren. Zu diesem Zweck werden IT-Syste-

me, drahtlose Kommunikationsanwendungen, Systeme der Navigation und der Steuerung von Plattformen, Wetterdienste sowie viele andere Komponenten miteinander zu Verkehrsnetzen verbunden. Allerdings handelt es sich dabei um einzelne Komponenten, die kaum für den Einsatz in einem dermaßen anspruchsvollen und vernetzten Umfeld entwickelt wurden. Daher besteht das Risiko, dass selbst kleine Störungen große negative Auswirkungen nach sich ziehen können.[107] Dies erklärt die grundsätzliche Relevanz von Cyberrisiken für den Transport- und Logistiksektor.

Mit Blick auf die Cyberrisikoanalyse im Transportsektor ist es sinnvoll, neben den verschiedenen Verkehrsträgern Straße, Schiene, Luft und Wasser[108] auch verschiedene Elemente zu unterscheiden. Zusätzlich zu den physischen Verkehrswegen[109] geht es dabei auch um die unterschiedlichen Plattformen (Fahrzeuge, Schiffe, Lokomotiven, Wagons, Flugzeuge), die Systeme des Verkehrsmanagements (inkl. Navigation) und die Logistiksysteme. Beispiele aus der Praxis machen deutlich, dass bei jedem dieser Elemente unterschiedliche Cyberrisiken möglich sind:

Störung der Funktionsfähigkeit der Plattformen

Personen- und Lastkraftwagen sind heute mit modernster Elektronik ausgestattet. Treiber der „Elektronisierung" der Fahrzeuge des Straßenverkehrs sind die Komfort- und Unterhaltungsbedürfnisse der Fahrer und Passagiere. Immer stärker werden einzelne Fahrzeuge zudem mit anderen Fahrzeugen und intelligenten Systemen zur Steuerung des Verkehrsflusses verknüpft (z.B. automatische Geschwindigkeitskontrollen, automatische Abstandsmelder). Verschiedene Untersuchungen legen nahe, dass die Automobilelektronik Sicherheitslücken aufweist. Elektronische Steuerungssysteme (Electronic Control Units), die zur Überwachung von bis zu 50 verschiedenen Komponenten[110] wie Motor, Klimaanlage, Licht, Radio, Türschlösser, Bremssystem oder Reifendruck eingesetzt werden, können durch Angriffe verletzt werden. In Labortests wurde beispielsweise dargestellt, wie Fahrzeuge abrupt zum Stehen gebracht werden können oder wie die Tachometernadel eines Fahrzeugs die Höchstgeschwindigkeit anzeigt, obwohl das Fahrzeug eigentlich stillsteht. Das US-amerikanische Transportation Research Board hat als Reaktion darauf verschiedene Empfehlungen zur Verbesserung der Cybersicherheit von Fahrzeugen veröffentlicht.[111]
Vergleichbare Risiken gibt es im Luftverkehr aufgrund der elektronischen Komponenten, die in Flugzeugen eingesetzt werden. Im Vorfeld der Lancierung der neuen Boeing 787 machten Gerüchte die Runde, wonach es möglich sei, sich über die WiFi-Netze, die an Bord für die Benutzung durch die Passagiere eingerichtet werden, in das Elektroniknetz des Flugzeugs zu hacken und dessen Funktionstüchtigkeit zu stören. Die US-amerikanische Flugaufsichtsbehörde (FAA) erließ in diesem Zusammenhang sogar eigene Weisungen. Der Flugzeughersteller Boeing bestritt dagegen Probleme mit der Sicherheit der IT-Systeme des Flugzeugs.[112] Dessen ungeachtet lancierte das John A. Volpe National Transportation Systems Center des US-Transportministeriums im Frühjahr 2010 ein umfassendes Projekt, um verschiedene Aspekte der Sicherheit von IT-Systemen in Flugzeugen zu simulieren. Am sogenannten Airborne Network Security Simulator beteiligen sich elf Flugzeughersteller und -zulieferer, fünf Fluglinien, sieben Regierungseinrichtungen aus den USA und Großbritannien (darunter auch das UK Center for the Protection of National Infrastructure) sowie zwei US-amerikanische Universitäten.[113]

106 Cybersecurity of Freight Information Systems.
107 Telefonisches Hintergrundgespräch mit europäischem Experten für kritische Infrastrukturen und IKT-Sicherheit, 3. April 2012.
108 Der Schifffahrtsverkehr wird an dieser Stelle nicht näher betrachtet. Eine Übersicht der möglichen Cyberrisiken in diesem Umfeld findet sich in: Analysis of Cyber Security Aspects in the Maritime Sector.
109 Es gibt einen klaren Trend, physische Verkehrswege, wie z.B. Straßen, durch den IKT-Einsatz ebenfalls „intelligenter" zu gestalten, beispielsweise durch die Integration von Signalisationsanlagen in den Boden oder den Einbau von Sensoren, die die Fahrzeuge und die Fahrer über veränderte Straßeneigenschaften (z.B. Glätte in Folge Gefrierens oder Regens) informieren. Da es sich dabei in der Regel um Anwendungen handelt, die dem Ziel eines verbesserten Verkehrsmanagements dienen, werden intelligente physische Verkehrswege an dieser Stelle nicht gesondert betrachtet.
110 The Safety Promise and Challenge of Automotive Electronics, S. 30.
111 Koscher et. al., „Experimental Security Analysis of a Modern Automobile"; The Safety Promise and Challenge of Automotive Electronics.
112 Kuhl, „How to Hack Into a Boeing 787".
113 Dinning, „Introduction to Cyber Security Issues for Transportation", S. 20.

Störung der Funktionsfähigkeit der Systeme des Verkehrsmanagements

Im Frühjahr 2009 sorgte ein Untersuchungsbericht der Innenrevision des US-Transportministeriums zur Luftfahrtbehörde FAA für Aufsehen. Die Innenrevision untersuchte mehr als 70 webbasierte Anwendungen und stellte 763 Verwundbarkeiten im Hochrisikobereich fest. Würden diese Verwundbarkeiten ausgenützt, so der Bericht weiter, hätten unberechtigte Dritte nicht nur Zugriff auf Personendaten in den Systemen der FAA, sondern könnten auch auf die Systeme des Flugverkehrsmanagements (Air Traffic Control) zugreifen. Die FAA selbst bestritt dieses Risiko.[114] Eine weitere potenzielle Verwundbarkeit sehen Forscher eines Instituts der US-Luftwaffe in der Anwendung der sogenannten Automatic Dependent Surveillance-Broadcast-Technologie (ADS-B). Dabei geht es um die Positionsbestimmung von Flugzeugen im Anflug, die bislang mittels Radar erfolgt, künftig aber GPS-basiert durchgeführt werden kann. Die Forscher kritisieren, dass die ADS-B-Signale weitgehend unverschlüsselt ausgestrahlt werden, sodass sie von außen gestört werden könnten.[115] Zusätzlich warnt die Innenrevision des US-Transportministeriums davor, dass die Flugaufsichtsbehörde beim Übergang zu einem ADS-B-System der nächsten Generation erstmals nicht mehr selbst Systembetreiberin sei, sondern diese Funktion einem Vertragsnehmer übertragen habe. Daher habe sie nur noch indirekten Einfluss auf die Systemsicherheit.[116]

Inwieweit die Verkehrsmanagementsysteme im Schienenverkehr bereits gezielt von Cyberangreifern ins Fadenkreuz genommen wurden, ist anhand der öffentlich zugänglichen Quellen schwieriger zu beurteilen. Im Januar 2012 meldeten US-Medien unter Bezug auf ein Memo des US-Transportministeriums, dass Züge der Pacific Northwest Railway Lines im Dezember 2011 Ziel eines Cyberangriffs aus dem Ausland geworden seien. Außer leichten zeitlichen Verzögerungen im Zugverkehr entstanden dabei keine weiteren Schäden. Nur wenige Tage später zweifelten jedoch Experten des US-Heimatschutzministeriums daran, dass es sich wirklich um einen gezielten Angriff gehandelt habe.[117] Eine grundsätzliche Verwundbarkeit der Zugleittechnik in Europa sprach im Dezember 2011 Prof. Stefan Katzenbeisser von der Technischen Universität Darmstadt bei einem öffentlichen Vortrag mit dem Titel „Can trains be hacked?“ an. Er sieht nach Medienberichten in der Funkkommunikation für kritische Informationsübermittlung ein Risiko. Als neuralgisch betrachtete er auch die automatische Zwangsbremsung von Zügen, wenn Haltevorsignale nicht beachtet würden.[118]

Eine wichtige Rolle innerhalb des Verkehrsmanagements spielen Systeme zur Positionsbestimmung und Navigation wie das Global Positioning System (GPS). Auch diese Systeme können von außen attackiert werden, beispielsweise um die eigene Position zu verschleiern oder die Positionsbestimmung eines anderen Nutzers zu erschweren.[119]

Störung der Funktionsfähigkeit der Logistiksysteme

Dass IT-gestützte Logistiksysteme von Dritten bewusst gestört werden, scheint gegenwärtig eher die Ausnahme zu sein. 80 Experten, die vom Beratungsunternehmen PricewaterhouseCoopers in Zusammenarbeit mit dem Supply Chain Management Institute nach künftigen Herausforderungen für die Sicherheit des Supply Chain Managements befragt wurden, sahen darin auch für die nahe Zukunft kein wachsendes Problem. Das gilt auch für die Gefahr, dass IT-Systeme der Logistik zum Zwecke der Spionage infiltriert werden.[120] Aktuelle Forschungsvorhaben zur IT-basierten Logistik zeigen allerdings indirekt auf, dass die Bedrohung zunehmen kann. So wurde z.B. am Hamburger Institut für Seeverkehrswirtschaft und Logistik im Rahmen des Projekts Amatrak ein Multiagentensystem zur Planung und Disposition in der Beschaffungs- und Distributionslogistik entwickelt.[121] Softwaregestützte Dispositionsagenten sollen dabei den menschlichen Disponenten die besten Angebote für die Zuteilung von Aufträgen zu Fahrzeugen unterbreiten – das lässt erkennen, welche Angriffsvektoren in diesem Bereich entstehen könnten.

Diese möglichen Gefahren sind allerdings nicht nur für die privatwirtschaftlichen Akteure von Bedeutung. Auch spezifische IT-Systeme der Behörden, die für die Logistik von Bedeutung sind, können davon betroffen sein. Das gilt beispielsweise für Systeme, die in der Zollab-

fertigung eingesetzt werden und eine wichtige Rolle bei der reibungslosen Abwicklung der Ein- und Ausfuhren spielen.[122]

Verletzung der Daten-/ Informationssicherheit

Beispiele von Verstößen gegen die Datensicherheit mit eindeutig kriminellen Motiven finden sich auch im Transportsektor. Im Februar 2003 wurde in Los Angeles ein ehemaliger Mitarbeiter eines Luftfahrtdienstleisters verhaftet, nachdem er zuvor in das System seines früheren Arbeitgebers eingebrochen war und geschäftsvertrauliche Daten gelöscht sowie Zugangsberechtigungen verändert hatte.[123] Im April 2011 wurde eine Gruppe von drei Kriminellen in China verhaftet, nachdem sie in das Online-Buchungssystem der China Eastern Airlines eingebrochen waren. Die Kriminellen erwarben Flugtickets zu vergünstigten Preisen und richteten damit einen Schaden in Höhe von 317.000 $ an.[124] Dass auch bargeldlose Zahlungssysteme des öffentlichen Personennahverkehrs geknackt werden können, demonstrierte eine Gruppe niederländischer Forscher Mitte 2008 am Beispiel der sogenannten Oyster-Karte, die in London eingesetzt wird.[125] Der Verletzung der Datensicherheit von Transportunternehmen können auch politische und andere Motive zugrunde liegen. Wohl eindeutig politischer Absicht war der Angriff einer Hackertruppe der pakistanischen Streitkräfte auf die indischen Eisenbahnbetriebe im April 2011, u.a. mit dem Ziel des Zugangs zu den Nutzerdaten.[126] Politische Motive dürften auch die Täter verfolgt haben, die im April 2012 die Facebook-Seite von Gulf Air aus Bahrain gehackt haben. Anstelle des Unternehmenslogos stellten sie das Bild eines inhaftierten Aktivisten auf die Seite, der sich seit zwei Monaten im Hungerstreik befand.[127] Der Veröffentlichung sensibler Personendaten diente der Angriff einer Hackergruppe, die in das Datensystem eines lokalen Transportunternehmens in San Francisco (Bay Area Rapid Transit, BART) eindrang. Dabei wurden die Datensätze von mehr als 100 Bahnpolizisten mit Angaben zu deren Privatanschrift entwendet und danach online gestellt. Der Vorgang stand im Zusammenhang mit einer Aktion der BART-Polizei, bei der ein Obdachloser den Tod fand.[128]

114 Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems, S. 3; Gorman, „FAA's Air-Traffic Networks Breached By Hackers".
115 Marks, „Air traffic system vulnerable to cyber attack".
116 Top Management Challenges for Fiscal Year 2012, S. 31.
117 Sternstein, „Hackers manipulated railway computers, TSA memo says"; Zetter, „Hackers Breached Railway Network, Disrupted Service".
118 „28C3: Hacker nehmen Eisenbahnsicherungen unter die Lupe".
119 Palmer, „Sat-nav systems under growing threat from ‚jammers'".
120 Transport & Logistics 2030: Securing the Supply Chain, S. 23.
121 <http://www.isl.org/projects/1370amatrak/index.php?lang=de> (Zugriff: 10. April 2012).
122 Cybersecurity of Freight Information Systems, S. 3; Interview, 18. April 2012.
123 „Ex-employee of Airport Transportation Company Arrested for Allegedly Hacking Into Computer, Destroying Data".
124 „Group jailed after hacking online systems".
125 Schneier, „Why being open about security makes us all safer in the long run".
126 „India's Railway Email System hacked by Pakistan Cyber Army".
127 „Bahrain's Gulf Air Facebook page ‚hacked'".
128 Vijayan, „Anonymous claims release of BART police officers' data".

6.3. Cyberrisiken im Transportsektor: Österreichische Bewertung

Die Gruppe der Gesprächspartner des Transportsektors war heterogener zusammengesetzt als jene der anderen Sektoren. Sie umfasste neben einem reinen Infrastrukturbetreiber aus dem Bereich des Straßenverkehrs auch Betreiber von Infrastruktur und Transportdiensten aus dem Straßen-, Schienen- und Luftverkehr, Logistikunternehmen und Betreiber zentraler Verkehrsmanagementdienstleistungen im Luftverkehr.

Trotz dieser unterschiedlichen Ausgangspositionen zeigt ein Blick auf die Top 15 der Cyberrisiken in Abbildung 11, dass auch die Transportexperten der sektorübergreifenden Abhängigkeit hohe Bedeutung beimessen. Dementsprechend wird das Risikopotenzial einer möglichen Manipulation der IKT-Systeme der Energieerzeugung und -versorgung (Durchschnittswert 3,17) sogar noch höher bewertet als die eigene Abhängigkeit von IKT-Systemen (Durchschnittswert: 3). Damit einher geht auch die hohe Relevanz der Gefahr fahrlässigen Verhaltens in strategischen Infrastrukturbetrieben, deren Bedeutung als Sicherheitsrisiko nur im IKT-Sektor noch höher bewertet wird. Aufgrund des physischen Umfeldes, das den Transportsektor prägt, haben die Experten in diesem Bereich auch ein besonderes Bewusstsein für Naturgefahren entwickelt, die die Funktionsfä-

higkeit der IKT- und der Transportinfrastruktur gefährden können. Mit einem Durchschnittswert von 2,83 erhält dieser Faktor von den Transportexperten die höchste Bewertung aller Befragten. Schließlich spielt der Faktor Mensch auch im Urteil der Transportexperten eine wichtige Rolle, die in der hohen Gewichtung der Risikokriterien fehlendes Fachpersonal, Social Engineering und mangelndes Sicherheitsbewusstsein zum Ausdruck kommt.

Im Einzelnen wird die Bewertung der verschiedenen Risikokategorien durch die Gesprächspartner des Transportsektors wie folgt begründet:[129]

Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

Eine mögliche Manipulation der IKT-Systeme der Energieerzeugung und -versorgung stellt für die Transportexperten das Top-Cyberrisiko dar, das von vier Gesprächspartnern mit dem Faktor 4 bewertet wurde.[130] Dabei ist allerdings zu beachten, dass die Energieversorgung innerhalb des Transportsektors eine unterschiedliche Rolle spielt. Jene Verkehrsträger und Anbieter verkehrsrelevanter Dienste, die von der Stromerzeugung abhängen, weisen ein anderes Risikoprofil auf als jene, die auf die Versorgung mit fossiler Energie angewiesen sind. Hinzu kommt, dass eine Institution nicht nur als Transporteur, sondern auch als Lebensmittelversorger von der Energieerzeugung und -versorgung abhängig ist. Die meisten Gesprächspartner wiesen darauf hin, dass Unterbrechungen der Energieversorgung nur für eine beschränkte Zeit überbrückt werden können, weil Notenergieversorgung möglich ist oder der Betrieb auf Kernprozesse reduziert werden kann.

Fahrlässiges Verhalten in strategischen Infrastrukturbetrieben

Die wechselseitige Abhängigkeit der verschiedenen Verkehrsträger spiegelte sich in den Antworten der Gesprächspartner zu dieser Risikokategorie, da oftmals auf die gegenseitigen Verflechtungen hingewiesen wurde. Das gilt vor allem für jene Akteure des Transportsektors, die eine kritische Drehscheibenfunktion ausüben. In den Antworten kam allerdings auch zum Ausdruck, dass die Akteure versuchen, das Risiko mit verschiedenen Maßnahmen zu minimieren. So wies ein Gesprächspartner auf die umfassende Prozessorientierung und die Risikomanagementzertifizierung seiner Institution hin, die einen Beitrag zur Risikobewältigung leisten soll.

Manipulation der IKT-Systeme des Verkehrssektors

Betont wurde bei dieser Risikokategorie zum einen der Kaskadeneffekt innerhalb des Verkehrssektors, der im schlimmsten Fall eine verkehrsträgerübergreifende Koordination zur Überbrückung logistischer Lücken unmöglich machen könnte. Das hätte wiederum weitreichende Folgen für alle von der logistischen Versorgung abhängigen Verbraucher. Zum anderen betonte ein Gesprächspartner, dass die Verfügbarkeit eigener Kommunikationsnetze zumindest eine gewisse Redundanz ermöglicht. Aufgrund der technischen Entwicklungen, die zu immer höheren Reisegeschwindigkeiten in diesem Segment des Verkehrssektors führen, stellt sich allerdings die Frage, ob und inwieweit die Abhängigkeit von zuverlässig funktionierender IKT möglicherweise die Sicherheit durch unabhängige eigene Netze überwiegen könnte.

Unsichere Steuerungssysteme (z.B. SCADA)

Steuerungssysteme spielen auch im Transportsektor eine zentrale Rolle. Sie werden zur Kontrolle der einzelnen Verkehrsträger, für beförderungsunterstützende Dienstleistungen sowie für Betriebsleistungen zur Bewirtschaftung der Transportinfrastruktur eingesetzt. Ein direkter Angriff gegen diese Systeme oder deren inhärente Unsicherheit wird daher als hochrelevan-

129 Die Ausführungen stützen sich auf Interviews vom 31. Januar, 1., 8.–10. und 21. Februar 2012.
130 Je ein Gesprächspartner bewertete das Risiko mit dem Faktor 2 (niedrig) bzw. sogar 1 (sehr niedrig).

Abbildung 11: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Transportsektors

Quelle: KSÖ-Interviewserie

tes Risiko erachtet. Hinzu kommt, dass die Sicherheitsmerkmale der Steuerungssysteme in einzelnen Transportteilsektoren offenbar über einen bestimmten Zeitraum nicht verändert werden können, was mit Blick auf die Kompatibilität zwischen den verschiedenen IKT-Komponenten zusätzlich problemverschärfend wirken kann.

Fehlendes Fachpersonal

Dass fehlendes Fachpersonal mit Bezug auf die anspruchsvollen Aufgaben im Bereich der Cybersicherheit ein Problem darstellt, wurde von den Gesprächspartnern des Transportsektors nicht bestritten. Allerdings gibt es Unterschiede in der Bewertung der damit verbundenen Konsequenzen. Überwiegend wurde ein Mangel an qualifizierten Kräften am Markt beklagt, der durch die innerbetriebliche Aus- und Weiterbildung nur ansatzweise kompensiert werden könne. Ein Gesprächspartner wies explizit darauf hin, dass die Rahmenbedingungen für die Qualifizierung der Mitarbeitenden im staatlichen Umfeld sehr schlecht seien, während der Vertreter eines anderen öffentlichen Unternehmens feststellte, dass es in seinem Umfeld ausreichend qualifiziertes Fachpersonal gebe.

Verletzlichkeit der IKT-Infrastruktur durch Naturkatastrophen

Die Relevanz dieses Risikos bemisst sich immer auch danach, wie relevant die IKT-Infrastruktur innerhalb der einzelnen Teilsektoren des Transportgewerbes ist. Mehrfach wurde betont, dass die Verletzlichkeit durch Redundanzen wie die Unterbringung kritischer IKT-Elemente an unterschiedlichen Standorten teilweise reduziert werden könne. Ein Gesprächspartner ging mit Blick auf Naturgefahren auch auf das erhöhte Risiko ein, das von der physischen Nähe von Transport-, Energie- und IKT-Infrastrukturen ausgehen kann.

Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen

Die Relevanz finanzwirtschaftlicher IKT-Systeme für den Verkehrssektor ergibt sich aus der Abwicklung von Zahlungen als Gegenleistung für die Beförderungsdienste, die die Verkehrsträger anbieten. In ausgewählten Bereichen wie der Lebensmittelversorgung betrifft der Ausfall der IKT-Systeme des Zahlungsverkehrs zudem auch die Kernprozesse der jeweiligen Unternehmen. Das gilt verstärkt ebenso für jene Verkehrsträger, die ihre Infrastrukturen auch für Dienstleistungen zur Verfügung stellen, die mit dem eigentlichen Verkehr nichts mehr zu tun haben. So gibt es beispielsweise inzwischen Flughäfen, die mit Geschäften, Restaurants und anderen angebotenen Dienstleistungen einen größeren Umsatz erzielen als mit der Abfertigung von Flugzeugen.[131]

Social Engineering

Social Engineering spielt als Risiko auch im Transportsektor eine Rolle, doch wird dessen Relevanz im Vergleich zu den anderen Sektoren verhältnismäßig niedrig bewertet.[132] Gerade dort, wo jedoch zur Verbesserung der Sicherheit stark auf technische Maßnahmen vertraut wird, gewinnt der Mensch als Risikofaktor an Bedeutung, so ein Gesprächspartner aus dem Bereich des Luftverkehrs. Um diesem Risiko zu begegnen, setzt der Betrieb eines anderen Gesprächspartners aus dem Bereich des Straßenverkehrs konsequent auf Ethik- und Integritätsschulung und hat ein eigenes Antikorruptionssystem aufgebaut. Hinzu kommen ergänzende Maßnahmen zur Förderung des Sicherheitsbewusstseins.

131 Lahrtz, „Rasantes Wachstum des Flughafens München“, S. B1.
132 Die Durchschnittsbewertung der Gesprächspartner aller Sektoren liegt bei 2,85, während die Transportexperten das Risiko des Social Engineering mit 2,67 bewertet haben.

© Artur Marciniec – iStockphoto.com

Datendiebstahl und Manipulation von Bürgerdaten

Die Gesprächspartner differenzierten bei diesem Punkt: Handelt es sich um Kundendaten, wird das Risiko des verletzten Informationsschutzes als hoch bewertet, auch weil damit entsprechende Reputationsverluste verbunden sein können. Noch relevanter ist aus der Sicht eines Gesprächspartners das Risiko, dass sich der Datendiebstahl auch auf Personendaten der eigenen Mitarbeitenden beziehen könnte. Ein unbefugter Dritter könnte sich dadurch Zugang zu physischen Einrichtungen und IKT-Systemen verschaffen. Je nach Absicht des Täters könnte dieser Identitätsdiebstahl schwerwiegende Konsequenzen nach sich ziehen.

Macht der sozialen Netze und deren Manipulation

Das Spektrum möglicher Risiken, das die Vertreter des Transportsektors in der Manipulation sozialer Netze sehen, ist breit. Erwähnt wurden Kampagnen, die den Ruf des jeweiligen Betriebs schädigen können, die Gefahr des Informationsabflusses durch unerlaubtes Eindringen in Daten unter Einsatz sozialer Medien, unbewusste Informationsweitergabe sowie die Möglichkeit eines gezielten Angriffs auf die eigenen Systeme ebenfalls unter Nutzung sozialer Medien. Ein Betrieb, der die Relevanz des Risikos zwar als sehr niedrig erachtet, hat gleichwohl bereits eine Übung durchgeführt, um seine Mitarbeitenden im Umgang mit einem Angriff auf die Unternehmensreputation über eine in den sozialen Netzen gesteuerte Kampagne vorzubereiten.

Mangelndes Sicherheitsbewusstsein

Für alle Partner des Verkehrssektors ist Sicherheit Teil der Grundaufgabe, denn die Verlässlichkeit der eigenen Dienstleistung hängt direkt davon ab. Gleichwohl können sicherheitsrelevante Zwischenfälle auch in Folge mangelnden Sicherheitsbewusstseins nicht ausgeschlossen werden. Die Unternehmen treffen Vorsorge in Form spezifischer Schulungsmaßnahmen und führen vereinzelt auch externe Prüfungen durch, um den Stand der Vorbereitung in diesem Bereich zu evaluieren.

Fehlendes oder unzureichendes Business Continuity Management

Die ausgeprägte Abhängigkeit der Verkehrsträger untereinander kommt in dieser Risikokategorie nochmals deutlich zum Ausdruck, denn mehrere Gesprächspartner verwiesen auf die Wechselwirkungen zwischen den Verkehrspartnern entlang der logistischen Wertschöpfungsketten. In dem Maße, wie einzelne Verkehrs- und Logistikpartner IKT-Systeme betreiben, die intensiv auch von Dritten genutzt werden, wird diese Abhängigkeit zusätzlich verstärkt. Ausfallpläne, Planspiele, Übungen und der Test kritischer Systemelemente zählen zum Repertoire der Krisenvorbereitung, das erwähnt wurde. Einzelne Gesprächspartner verwiesen auch darauf, dass Partnerunternehmen eigenen Audits unterzogen werden.

Geknackte digitale Schlüsselsysteme

Die Abhängigkeit von Dritten als Lieferanten digitaler Schlüssel und Zertifikate scheint im Transportsektor unterschiedlich ausgeprägt zu sein. Immerhin zwei Gesprächspartner gaben an, digitale Schlüssel und Zertifikate selbst herzustellen. In anderen Teilsektoren wird digitalen Schlüsselsystemen nur beschränkt vertraut, sodass teilweise auf den physischen Austausch zurückgegriffen wird. Der Gesprächspartner aus der Lebensmittellogistik verwies darauf, dass es länderspezifische Unterschiede gibt, die auch zu beachten seien. So müsse die Rechnungsprüfung je nach Land verschlüsselt und signiert werden. Verletzungen in diesem Bereich hätten für das Unternehmen nur beschränkte Auswirkungen.

Manipulation der IKT-Systeme für Cloud Services

Beim Einsatz Cloud-basierter Dienste zeigten sich die Vertreter des Transportsektors sehr zurückhaltend. Zwei Gesprächspartner gaben an, dass deren Einsatz entweder verboten sei oder in internen IT-Regeln ausgeschlossen werde. Ein weiterer Gesprächspartner deutete an, dass der Einsatz gerade auch vor dem Hintergrund der aktuellen Datenschutzdiskussion in seinem Umfeld sehr restriktiv gehandhabt werde. Geheime Daten oder ganze Services würden auf keinen Fall in einer Datenwolke abgelegt.

Manipulation der IKT-Systeme in der Wasserwirtschaft

Auch in diesem Punkt kommen die verschiedenen Geschäftsmodelle der Transport- und Logistikbetreiber zum Ausdruck. Einige Gesprächspartner erachten das Risiko als hoch, weil es sich auf die Mitarbeitenden und deren Anwesenheit im Unternehmen auswirken kann. Ein anderer Interviewpartner betonte die möglichen Auswirkungen auf die Versorgung mit Löschwasser und damit die Notfallvorsorge des eigenen Betriebs. Der Vertreter des Lebensmittelversorgers erklärte die Bedeutung der Wasserversorgung aus der Tatsache, dass es sich hierbei um den größten fleischverarbeitenden Betrieb Österreichs handelt. Ein Ausfall der Wasserversorgung wäre in diesem Fall aber nicht unternehmensgefährdend.

CYBERRISIKEN UND ÖSTERREICHS BEHÖRDENSEKTOR

© Petrovich9 – iStockphoto.com

7.1. Österreichs Behördensektor Relevanz in Zahlen
7.2. Cyberrisiken im Behördensektor Allgemeine Bewertung und Trends
7.3. Cyberrisiken im Behördensektor: Österreichische Bewertung

7

Österreichs Behördensektor: Relevanz in Zahlen

7.1.

- Nach Schätzungen des Bundesfinanzministeriums belaufen sich die **Ausgaben** des Bundeshaushalts 2012 auf gut 73,5 Milliarden € bei **Einnahmen** in Höhe von ungefähr 64,4 Milliarden €. Der daraus resultierende Verlust von etwa 9,1 Milliarden € entspricht einem Defizit von 3 % des Bruttoinlandsprodukts (BIP).[133]
- Die **größten Ausgabenposten** im Bundesvoranschlag 2012 sind Finanzen (21 Milliarden €), Arbeit, Soziales und Konsumentenschutz (19,4 Milliarden €) sowie Unterricht, Kunst und Kultur (8 Milliarden €). Für die Bereiche Inneres, Äußeres, Justiz und Landesverteidigung sowie Sport sind gesamthaft 6,3 Milliarden € vorgesehen.[134]
- 2012 will die österreichische Regierung rund 2,4 Milliarden € für **Forschung und Entwicklung** ausgeben, wobei der Löwenanteil mit 1,7 Milliarden € auf das Bundesministerium für Wissenschaft und Forschung entfällt. Knapp 4,5 Milliarden € sind als Investitionen in die **Infrastruktur** vorgesehen, wobei davon 3,7 Milliarden € als Beiträge an ausgegliederte Gesellschaften erfolgen.[135]
- Die öffentliche Verwaltung in Österreich wies Ende 2010 einen **Personalbestand** von gut 350.000 Mitarbeitenden auf (Bund: 132.804, Länder: 142.798, Gemeinden: 74.922). Mit einem Anteil öffentlich Bediensteter von 12,8 % an der Gesamtbeschäftigung (2009) lag Österreich 2009 deutlich unter dem EU-Durchschnitt von 16,3 %.[136]
- Bei verschiedenen öffentlichen Diensten,[137] die elektronisch angeboten werden **(E-Government),** erreichte Österreich 2010 als einer von nur vier EU-Mitgliedstaaten eine 100-prozentige Abdeckung. Knapp 80 % der Unternehmen greifen auf diese Dienste zurück, womit sich Österreich im Durchschnitt der EU-27 bewegt, während die Zurückhaltung bei den Bürgerinnen und Bürgern mit einem Nachfragewert von unter 40 % deutlicher ausfällt.[138] 2010 nutzten zudem 15 % der Unternehmen das Internet, um Angebote bei elektronischen öffentlichen Ausschreibungen zu unterbreiten, womit Österreich leicht über dem Durchschnitt der EU-27 von 13 % lag.[139]

133 <https://www.bmf.gv.at/Budget/Budgetsimberblick/Sonstiges/Budgetsimberblick/Budgetentwurf2012/TabellenDownload/eckwerte_tabellen_2012.xlsx> (Zugriff: 3. April 2012).
134 <https://www.bmf.gv.at/Budget/Budgetsimberblick/Sonstiges/Budgetsimberblick/Budgetentwurf2012/TabellenDownload/budgetsichten_tabellen_2012.xlsx> (Zugriff: 3. April 2012).
135 <https://www.bmf.gv.at/Budget/Budgetsimberblick/Sonstiges/Budgetsimberblick/Budgetentwurf2012/TabellenDownload/fue-beilage_tabellen_2012.xlsx>; <https://www.bmf.gv.at/Budget/Budgetsimberblick/Sonstiges/Budgetsimberblick/Budgetentwurf2012/TabellenDownload/infrastruktur_tabellen_2012.xlsx> (Zugriff: 3. April 2012).
136 Das Personal des Bundes 2011, S. 11, 14. Die Zahlen zum Personalbestand beziehen sich auf Vollbeschäftigtenäquivalente.
137 Darunter fallen z.B. Dienste der Steuer- und Sozialversicherungsbehörden, die Möglichkeit, einen Wohnortwechsel elektronisch anzeigen zu können, oder öffentliche Auftragsvergabe.
138 Europe's Digital Competitiveness Report, S. 86–88.
139 <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tin00109&plugin=1> (Zugriff: 3. April 2012).

7.2. Cyberrisiken im Behördensektor: Allgemeine Bewertung und Trends

Cybergefahren gehören inzwischen auch im Behördenumfeld zum allgemeinen Risikobild. Die Allgegenwärtigkeit dieser Gefahr verdeutlichte im letzten Jahr General Keith Alexander, Leiter des United States Cyber Command, mit der Feststellung, dass jede Stunde ca. 250.000 Angriffe gegen Informationssysteme des US-Verteidigungsministeriums lanciert werden.[140] Auch wenn die USA aufgrund ihrer exponierten internationalen Position ein besonderes Ziel für Cyberangriffe darstellen, trifft die Feststellung, dass staatliche Informationssysteme von fremden Nachrichtendiensten, Cyberkriminellen und Hacktivists ins Fadenkreuz genommen werden, auch für viele andere Staaten zu. So stellte beispielsweise das deutsche Innenministerium fest, dass die Zahl elektronischer Angriffe mit nachrichtendienstlichem Hintergrund gegen Rechner von Bundesbehörden von 2009 (1.511 Angriffe) bis 2010 (2.108 Angriffe) um gut 30 % zugenommen hat.[141] Dass die Größe eines Landes oder seine außenpolitische Grundhaltung keinen Schutz vor elektronischen Angriffen bietet, zeigten in der Vergangenheit die Angriffe gegen Rechnersysteme der Außenministerien in der Schweiz und in Österreich.[142]

Aufgrund der Vorfälle der jüngsten Vergangenheit können verschiedene Kategorien möglicher Ziele von Cyberattacken im staatlichen Umfeld unterschieden werden:

- Ministerien, Behörden und internationale Organisationen bilden aufgrund ihrer Visi-

bilität und der medialen Aufmerksamkeit, die Angriffe gegen diese Einrichtungen erzeugen, offenbar ein besonders attraktives Ziel für Cyberstraftaten unterschiedlichster Art.

- Einsatzkräfte und ihre Führungs-, Informations- und missionskritischen Einsatzsysteme stellen eine zweite Zielgruppe dar, denn Angriffe gegen diese technischen Einrichtungen wirken sich unmittelbar auf die Leistungsfähigkeit der Streit- und Sicherheitskräfte aus.
- In einer dritten Kategorie können jene staatlichen Einrichtungen zusammengefasst werden, die besonders sensible Daten verwalten. Dazu gehören beispielsweise Rechenzentren, mit deren Hilfe andere staatliche Systeme gesteuert werden oder die zur Abwicklung des staatlichen Finanzverkehrs genutzt werden. Eine vergleichbare Rolle spielen auch öffentliche Register, die Personendaten von Bürgerinnen und Bürgern speichern, verwalten und mit anderen staatlichen und nicht-staatlichen Institutionen austauschen. Ebenfalls zu dieser Kategorie zählen staatliche Forschungseinrichtungen, die aufgrund der vorhandenen Forschungsergebnisse (Stichwort: geistiges Eigentum) ein attraktives Ziel darstellen.

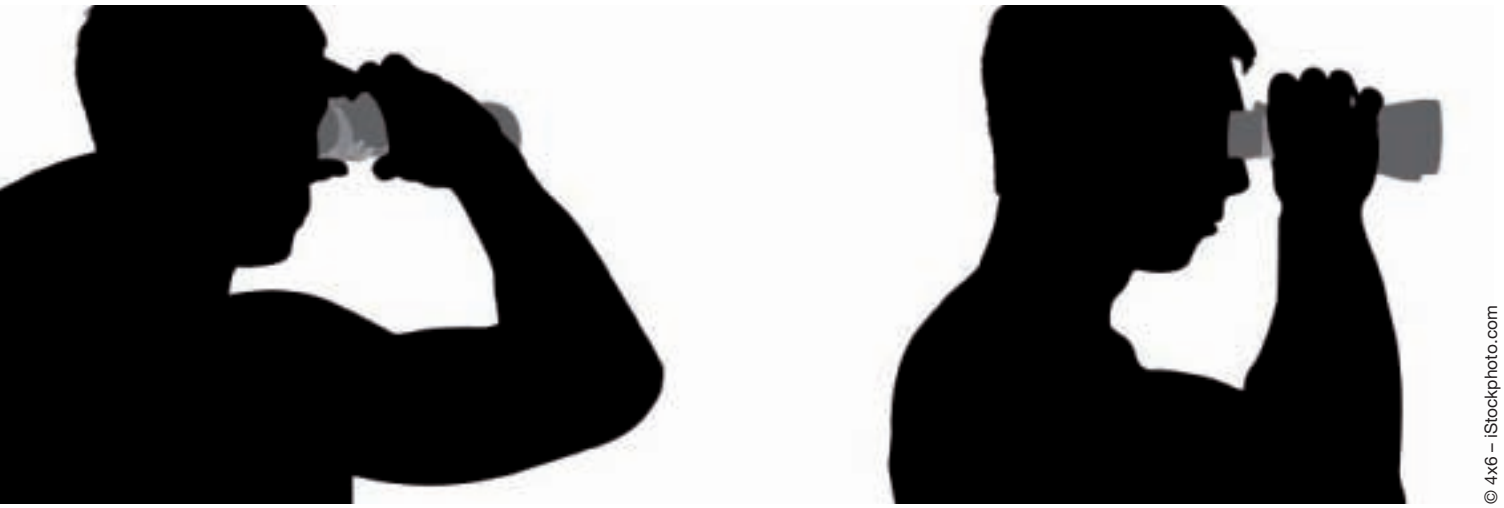
Geht es um mögliche Cyberangriffe gegen die eben genannten Zielgruppen im Behördenumfeld, so können mit Hilfe des in Kapitel 2 (Tabelle 1) entwickelten Katalogs intentionaler Cyberrisiken die vier folgenden Kategorien unterschieden werden, die im Alltag miteinander kombiniert werden können:

Politisch motivierte Aktionen

Politisch motivierte Aktionen gegen IT-Systeme staatlicher Einrichtungen verfolgen in der Regel einen kommunikativen Zweck. Sie richten sich gegen Behörden als Symbol der Staatsmacht und sollen die grundsätzliche Verwundbarkeit des Staates im Informationsraum offenlegen. Je nach Ausmaß und Dauer des Angriffs geht es auch darum, die Unfähigkeit der staatlichen Behörden bei der Bewältigung der verursachten Probleme zu illustrieren. Das Motivationsspektrum ist breit:

1. Es beinhaltet beispielsweise den Protest gegen staatliche Maßnahmen. Jüngstes Beispiel ist der Anonymous-Angriff gegen die Website des britischen Innenministeriums im April 2012 aus Anlass bekannt gewordener Pläne zur möglichen Internetüberwachung in Großbritannien.[143]
2. Politisch motivierte Aktionen gegen staatliche Einrichtungen können auch das Ergebnis geplanter Informationsoperationen sein. Wie das Beispiel des russisch-georgischen Konflikts im Sommer 2008 verdeutlichte, können diese wiederum mit militärischen Handlungen koordiniert werden.
3. Eher dem Bereich der allgemeinen Propaganda sind jene Aktionen zuzuordnen, die in Folge eines Zwischenfalls zwischen zwei Ländern aus patriotischen Motiven lanciert wurden. Zu dieser Kategorie zählt beispielsweise die 2001 lancierte Attacke gegen IT-Systeme des US-Verteidigungsministeriums, nachdem ein US-Spionageflugzeug den chinesischen Luftraum verletzt hatte.[144]
4. Auch wenn staatliche Einrichtungen weniger das Ziel, sondern die teilweise durchführenden Instanzen sind, ist als weitere Kategorie politisch motivierter Aktionen im Informationsraum auch die zunehmende Überwachung, Zensur und Beeinflussung anders denkender politisch-gesellschaftlicher Kräfte zu nennen. Allerdings gibt es inzwischen verschiedene Anwendungen, um diese Kontrollen zu umgehen.[145]

140 Stewart/Bartz/Wolf/Mason, „Special report: Government in cyber fight but can't keep up".
141 Verfassungsschutzbericht 2010, S. 367.
142 Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht 2009/2, S. 5; Rief, „Chinesen hacken Österreichs Außenministerium".
143 Layton, „Hacktivists Anonymous claim to have taken down Home Office website".
144 Nazario, „Politically Motivated Denial of Service Attacks".
145 Siehe beispielsweise das Angebot des US-amerikanischen Unternehmens Nomadio: <http://nomadio.net/> (Zugriff: 9. April 2012).



© 4x6 – iStockphoto.com

Spionage

Spionage gegen staatliche Einrichtungen und im staatlichen Auftrag arbeitende private Einrichtungen zählt zu den allgegenwärtigen Gefahren, die die Nutzung moderner IKT mit sich bringt. Die Liste der jüngsten Beispiele ist lang und umfasst beispielsweise

- das französische Finanzministerium, aus dem Ende 2010 Daten im Zusammenhang mit der Vorbereitung des G-20-Vorsitzes entwendet wurden;[146]
- das kanadische Finanzministerium, dessen Rechner im Januar 2011 mit einer Schadsoftware infiziert wurden und über dessen System der Zugang zu Computern von Entscheidungsträgern möglich war;[147]
- die Europäische Kommission, die im Vorfeld des EU-Gipfeltreffens im März 2011 Opfer eines Cyberangriffs wurde, dessen Hintergrund allerdings bis heute unklar ist;[148]
- den internationalen Währungsfonds, dessen System offenbar im Juni 2011 mit dem Ziel gehackt wurde, Zugriff auf sensible Daten zu erhalten.[149]

Von besonderem Interesse ist die Feststellung, dass sich gut verdeckte Spionagevorgänge im Informationsumfeld staatlicher Einrichtungen ebenfalls über eine sehr lange Zeit erstrecken können, bis sie entdeckt werden.[150]

Stören der Leistungs- und Einsatzfähigkeit

Die Störung einsatzrelevanter staatlicher IKT-Systeme stellt eine ganz besondere Risikokategorie dar. Sie eröffnet den Tätern nicht nur die Möglichkeit, staatliche Behörden und Einsatzkräfte auszuspionieren und sich entsprechend auf deren geplante Aktionen vorzubereiten, sondern verschafft diesen auch die Möglichkeit, die Kontrolle solcher Systeme zu übernehmen. Aufsehenerregende Beispiele aus der jüngsten Vergangenheit umfassen erfolgreiche Einbrüche in das IT-System der NASA mit dem Ergebnis, dass Außenstehende die Kontrolle über kritische Systemelemente übernehmen konnten, und die angebliche „Entführung“ einer US-amerikanischen Drohne durch staatliche Einrichtungen des Iran, denen es gelungen sein soll, in das Steuerungssystem der Drohne einzudringen und diese damit von ihrer eigentlichen Flugroute abzubringen.[151] 2009 führte die Verbreitung des Computerwurms Conficker in den IT-Systemen verschiedener europäischer Streitkräfte dazu, dass die Kommunikation deutlich erschwert und einzelne Waffensysteme nicht mehr betrieben werden konnten.[152]

Das Risiko der Störung einsatzrelevanter Systeme wird gerade im staatlichen Sicherheitsumfeld mit der generellen Problematik

unsicherer Wertschöpfungsketten (Supply Chain Risk Management) in Verbindung gebracht. Dahinter steht die zunehmende Verwundbarkeit moderner IKT z.B. durch Rückgriff auf kommerzielle Standardprodukte, die an Einsatzanforderungen der Sicherheits- und Streitkräfte angepasst werden, die Verwendung von Bauteilen, deren Herkunft und Funktionalität angesichts der vielgliedrigen Arbeitsteilung kaum durchgehend verfolgt und überprüft werden kann, sowie die Abhängigkeit von Lieferanten, denen eine besondere Nähe zu nachrichtendienstlichen Einheiten ihrer Ursprungsländer nachgesagt wird.[153] In den USA ist die Sensibilität für diese Gefahren besonders ausgeprägt und daher wird intensiv an Vorschlägen gearbeitet, wie die aus den IKT-Wertschöpfungsketten resultierenden Risiken vermindert werden können.[154]

Kriminelle Handlungen

Kriminelle können versucht sein, sensible Daten aus Regierungsrechnern zu entwenden, um daraus Profit zu schlagen. Ein besonders krasses Beispiel ereignete sich 2006 in Israel. Nach seiner Entlassung aus dem Dienst des Sozialministeriums (Welfare Ministry) entwendete ein Vertragsbediensteter die biometrischen Datensätze von neun Millionen Israelis. Die Datenbank enthielt neben den Namen und den Geburtsangaben der jeweiligen Personen auch Einträge zu ihren Familienangehörigen und ihre Sozialversicherungsnummern. Zudem waren in der Datenbank Gesundheitsdaten und Familienangaben von mehreren hunderttausend adoptierten Menschen enthalten. Die Datensätze wurden nach Presseberichten an Kriminelle weiterverkauft und frei verfügbar ins Internet gestellt. Der Täter wurde erst im Oktober 2011 von den israelischen Behörden gefasst. [155]

146 „France: cyber-attaque contre le ministère des Finances“.
147 Weston, „Foreign hackers attack Canadian government“.
148 „Hackerangriff auf EU-Kommission“.
149 Wolf/Maclean, „IMF cyber attack aimed to steal insider information: expert“.
150 So wurde beispielsweise in den USA das Rechnersystem eines Bundesstaates während 25 Monaten unbemerkt ausspioniert. Siehe: Alperovitch, Revealed: Operation Shady RAT, S. 7.
151 Martin, „NASA Cybersecurity: An Examination of the Agency’s Information Security“, S. 5; Majumdar, „Iran’s Captured RQ-170: How Bad is the Damage?“, S. 4.
152 „Hunderte Bundeswehr-Rechner von Conficker befallen“; „MoD probes virus security breach“; „How Conficker virus felled the Military“.
153 Hierzu weiterführend: Mission Impact of Foreign Influence on DoD Software; High Performance Microchip Supply; Krekel/Adams/Bakos, „Occupying the Information High Ground“, S. 82–93.
154 Boyens, „Notional Supply Chain Risk Management Practices for Federal Information Systems“.
155 Ungerleider, „The Dark Side of Biometrics: 9 Million Israelis’ Hacked Info Hits the Web“.

7.3. Cyberrisiken im Behördensektor: Österreichische Bewertung

Stärker als die Interviewpartner der anderen Infrastruktursektoren haben die Behördenvertreter die Risikobewertung aus ihrer Doppelsicht als mögliche Betroffene von Cyberrisiken[156] und Verantwortliche für den Schutz Dritter im Cyberspace vorgenommen. Dabei fällt die hohe Übereinstimmung bei der Bewertung der Top-Cyberrisiken auf.[157] Mindestens drei, meistens sogar vier der fünf befragten Experten bzw. Expertengruppen haben zehn der in Abbildung 12 dargestellten Risikofelder als hoch- bzw. sehr hochrelevant eingestuft. Mehrere Aspekte fallen bei den Antworten der Behördenvertreter auf:

- Erstens gibt es ein ausgeprägtes Bewusstsein für die eigene Betroffenheit. Das zeigt sich an der Bewertung der Risikofaktoren Social Engineering, Cybercrime und Cyberspionage in Verbindung mit der Gefahr des Diebstahls bzw. der Manipulation digitaler Identitäten im Allgemeinen und Bürgerdaten im Besonderen. Cybercrime und Cyberspionage dürften auch deshalb in ihrer Relevanz so hoch eingestuft worden sein, weil die Behördenvertreter in ihrer Zuständigkeit für die gesamtstaatliche Gefahrenabwehr und die öffentliche Sicherheit für die Minimierung dieser Risiken zuständig sind.
- Zweitens gibt es eine gewisse Varianz in der Beurteilung derjenigen Risikofaktoren, die sich zum einen aus der Grundaufgabe der Behördenvertreter und damit ver-

Abbildung 12: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Behördensektors

Quelle: KSÖ-Interviewserie

156 Siehe zum Stand des Informationssicherheitsmanagements in der österreichischen Bundesverwaltung weiterführend: Gottwald, „Österreichische Bundesverwaltung: Erhebung der organisatorischen Verankerung der Informationssicherheitsmanagement-Zuständigkeit“, S. 112–136.

157 Bei den anderen Risikokategorien gab es dagegen teilweise markante Bewertungsdifferenzen. So wird beispielsweise das Risiko eines Cyberwar nur von der Landesverteidigung als sehr relevant eingestuft, während die anderen Behördenvertreter dessen Relevanz als niedrig bzw. sehr niedrig erachten.

bunden auch der Rolle der IKT erklären.[158] Zum anderen ist zu berücksichtigen, ob die Behörden in direktem Kontakt mit Bürgerinnen und Bürgern sowie Unternehmen stehen und dazu etwa auf internetgestützte Dienste zurückgreifen. In diesem Fall ist die Betroffenheit bei Ausfall der entsprechenden Dienste entsprechend höher.

- Drittens kommt in den Antworten der Behördenexperten auch die Sorge um die Abhängigkeiten zwischen verschiedenen Infrastruktursektoren zum Ausdruck, was sich in der hohen Bewertung der potenziellen Manipulation der IKT-Systeme in den Sektoren Energie, Verkehr, Kommunikation und Finanzen niederschlägt.

Im Einzelnen können die Interviewaussagen zu den Top-15-Cyberrisiken aus Sicht der Behördenvertreter wie folgt zusammengefasst werden:[159]

Cybercrime

Auch wenn einige Behördenvertreter darauf hinweisen, dass zahlreiche Maßnahmen ergriffen werden, um das Eintreten dieses Risikos im eigenen Umfeld zu verhindern, besteht Einigkeit bezüglich der hohen Relevanz. Das gilt insbesondere für jene Behörden, die sensible Daten (z.B. Patientendaten) verwalten. In diesem Zusammenhang wurde auch betont, wie wichtig es sei, dass den Behörden – und in weiterer Folge auch den Partnern in der Wirtschaft – Fähigkeiten zur Verfügung stehen, die es erlauben, Gefahren frühzeitig zu erkennen und zu bewerten. Dabei wurde die Rolle eines möglichen Cyberlagebildes bzw. Cyberlagezentrums als künftiges Handlungserfordernis angesprochen (Kapitel 8.2).

Cyberspionage

Die Behördenvertreter haben die Relevanz von Cyberspionage und Cybercrime als potenzielle Gefährdungen identisch bewertet. Interessant sind die teils leichten Wahrnehmungsdifferenzen zwischen Bundes- und Länderebene, da Vertreterinnen und Vertreter auf Länderebene das Risikopotenzial etwas niedriger einstuften. Das erklärt sich zum einen aus der relativ höheren Attraktivität von Bundesbehörden als Ziele der Cyberspionage. Mit Blick auf besonders wirtschaftsrelevante Aspekte wie die regionale Wirtschaftsförderung stellt sich allerdings die Frage, ob sich das Risikobild für Landesbehörden nicht gleich darstellt wie auf der Bundesebene.

Social Engineering

Im Wissen darum, dass Behörden aufgrund ihrer Aufgaben und der von ihnen verwalteten Daten attraktive Ziele für Cybertäter darstellen, messen die Vertreter dem Risiko des Social Engineering hohe Bedeutung bei. Vorfälle in der Vergangenheit, bei denen Unbefugte durch den Erwerb von Daten mittels Social Engineering beispielsweise auf Geräte ziviler Sicherheitskräfte zugreifen konnten, unterstreichen aus Sicht der Gesprächspartner die Relevanz des Themas. Diese Feststellung muss auch im Zusammenhang mit der Risikokategorie „mangelndes Sicherheitsbewusstsein“ betrachtet werden.

Fehlerhafte, inkompatible Codes/Software

Wie die Vertreter der Privatwirtschaft sind sich auch die Behördenexperten dieses Risikos bewusst, verweisen aber ebenfalls auf die Schwierigkeiten, Codes und Software im Alltag umfassend auf ihre korrekte Funktionsfähigkeit zu testen, bevor diese eingesetzt werden. Einzelne Gesprächspartner haben darauf hingewiesen, dass sie dazu übergehen, vor allem bei fremdentwickelter Software entsprechende Vorgaben an die Entwickler zu richten. Zudem bestehen in einigen Bereichen auch strenge Zulassungs- und Abnahmekriterien.

Mangelndes Sicherheitsbewusstsein

Sämtliche Gesprächspartner unterstreichen die Notwendigkeit, in diesen Bereich zu investieren, um das Eintreten des Risikos zu verhindern bzw. dessen Auswirkungen weitgehend zu beschränken. Vor allem jene Behörden, die täglich in direktem Kontakt mit den Bürgerinnen und Bürgern stehen, sind sich des Reputationsschadens, der als Folge dieses Risikos eintreten kann, sehr deutlich bewusst.

Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

In verschiedenen sensiblen Bereichen ist der Behördensektor selbst von der Energieversorgung abhängig. Das gilt beispielsweise für weite Teile des Gesundheits-/Krankenwesens, für das Verkehrsleitmanagement, aber auch für die Einsatz- und Rettungskräfte, deren Kommunikationsinfrastruktur mit Strom versorgt werden muss. Insofern werden mögliche Manipulationen der IKT-Systeme der Energieerzeugung/-versorgung auch aus Behördensicht als hochrelevant erachtet. Teilweise kann der öffentliche Sektor auf Notfallkapazitäten zurückgreifen, deren Leistungsfähigkeit allerdings zeitlich ebenso beschränkt ist wie in der Privatwirtschaft.

Diebstahl und Manipulation von Bürgerdaten bzw. systematischer Diebstahl digitaler Identitäten

Vor allem jene Behördenvertreter, die direkt mit Bürgerdaten umgehen, haben dieses Risiko als massive Bedrohung ihres Kerngeschäfts bewertet. Darüber hinaus wird der Diebstahl digitaler Identitäten auch im Behördenbereich als sehr relevant beurteilt, weil unter Verwendung gestohlener digitaler Identitäten der unerlaubte Zugang zu kritischen Behördeneinrichtungen möglich werden kann. Darauf wurde am Beispiel des Gesundheitswesens, aber auch mit Blick auf sensible Führungs-, Kommunikations- und Einsatzsysteme hingewiesen. Der enge Zusammenhang mit dem Problem der Cyberkriminalität verstärkt aus Sicht der Behördenvertreter die möglichen negativen Auswirkungen des Diebstahls digitaler Identitäten. Die Aktualität und Relevanz des Themas für die Behörden wurde im September 2011 durch die Ver-

158 Ein Ministerium mit einer Vielzahl von Außenstellen in verschiedenen Ländern der Welt weist eine andere Abhängigkeit von funktionsfähiger IKT auf als eine primär im Inland und mit anderen Behörden interagierende Dienststelle. Interview, Wien, 20. März 2012.
159 Die Ausführungen stützen sich auf Interviews, die am 8., 14., 20. und 28. Februar 2012 sowie am 20. März 2012 durchgeführt wurden.

öffentlichung der persönlichen Daten von gut 25.000 Polizisten in Österreich unterstrichen. Presseberichten zufolge könnten die Daten von einem Sympathisanten der Hackergruppe Anonymous, der für die International Police Association tätig ist, weitergegeben worden sein.[160]

Fehlendes Fachpersonal

Der Mangel an qualifiziertem Fachpersonal im Bereich der IKT-Sicherheit ist allgemein relevant, doch schaffen es die Behördenvertreter nach eigener Beurteilung, für ihre Aufgaben genügend Experten zu rekrutieren. In Einzelfällen wurden sogar auf Landesebene spezifische Einrichtungen wie ein CERT etabliert und personell bestückt. Allerdings wiesen die Behördenvertreter auch darauf hin, dass zusätzliche Flexibilisierungen des Dienstrechts das kurzfristige Beiziehen von Experten aus dem nichtstaatlichen Umfeld erleichtern könnten.

Manipulation der IKT-Systeme des Verkehrssektors

Die Gesprächspartner haben dieses Risiko differenziert bewertet und danach unterschieden, ob die Behörden als Betreiber relevanter Infrastrukturkomponenten (z.B. Verkehrsleitsysteme) oder als Arbeitgeber (z.B. Mitarbeiter erreichen Arbeitsort aufgrund des möglichen Verkehrschaos nicht mehr) betroffen sind. Auf der Bundes- und Landesebene gab es teilweise Bewertungsunterschiede, die sich mit dem eher lokalen bzw. regionalen Charakter der Störung einzelner Verkehrsträger erklären lassen.

Manipulation von Kommunikations- und Satellitenverbindungen

Tritt dieses Risiko ein, wirkt es sich negativ auf die Verfügbarkeit von Behördenleistungen aus. Besonders Einsatzkräfte können dabei in ihrer Leistungsfähigkeit beeinträchtigt werden. Hinzu kommt, dass gewisse Kommunikationsdienste nur von sehr wenigen Anbietern bereitgestellt werden, sodass sich deren möglicher Ausfall noch stärker auswirken würde. Daher wird die Manipulation von Kommunikations- und Satellitenverbindungen aus Behördensicht als relevantes Risiko bewertet.

Manipulierte bzw. unsichere Hardware

Bei der Bewertung des Risikos zeigten sich die Gesprächspartner zwar darin einig, dass die potenzielle Gefahr groß ist, die Betroffenheit jedoch je nach Behörde und Aufgabenbereich variieren kann. Während ein Gesprächspartner darauf hinwies, dass das Risiko so gut wie nicht eintreten und über den Qualitätssicherungsprozess beim Einkauf entsprechend abgewehrt werden könne, waren sich die restlichen Befragten darin einig, dass es bislang keine wirklich guten Prüfsysteme zur Verifizierung der Zuverlässigkeit von Hardwarekomponenten gebe.

Nicht erkannte (IKT)-Anomalien

Die Gesprächspartner haben zum Ausdruck gebracht, dass sich die Behörden in unterschiedlicher Weise mit dem Problem beschäftigen. Dabei sind sie allerdings wie die Partner in der Privatwirtschaft auch abhängig von den Sicherheitsvorkehrungen, die Hard- und Softwarehersteller sowie die IKT-Provider ergreifen. Einzelne Behörden verfolgen daher genau, welche Maßnahmen in der Privatwirtschaft ergriffen werden. Andere bemühen sich wiederum selbst um den Aufbau entsprechender Monitoringsysteme für Vorfälle. Dass gerade die Vertreterin einer Landesregierung auf dieses Beispiel hinwies, deutet interessante Möglichkeiten der föderalen Zusammenarbeit an.

Cyberterrorismus

Auffällig bei der Bewertung dieses Risikos ist, dass nur die Vertreter zweier Ressorts von einer sehr hohen bzw. hohen Relevanz sprechen, während die Übrigen das Risiko mit Verweis auf das Fehlen konkreter Beispiele in der Praxis mit niedriger Relevanz bewerten. Deutlich wurde, dass der hohe Wert und die relativ große Streuung der Bewertungsergebnisse mit unterschiedlichen Interpretationen des Phänomens zusammenhängen, wobei nicht immer klar zwischen Hacktivism und möglichem Terrorismus im Cyberspace unterschieden wurde. Das legt die Schlussfolgerung nahe, dass der hohe Durchschnittswert die wirkliche Einschätzung der Experten möglicherweise etwas verzerrt zum Ausdruck bringt.

Geknackte digitale Schlüsselsysteme

Werden Zertifikate gestohlen oder digitale Schlüsselsysteme geknackt, sind die Behörden als Anwender davon direkt betroffen. Weitgehende Einschränkungen der E-Government-Dienste könnten die Auswirkung sein, so die Gesprächspartner. Allerdings gibt es staatliche Einrichtungen, die selber digitale Schlüssel entwickeln, auditieren und zertifizieren – eine Fähigkeit, die zugunsten der Privatwirtschaft weiterentwickelt werden könnte (Kapitel 8.5).

Ebenfalls mit dem Durchschnittswert von 2,6 bewerteten die Behördenvertreter die Macht der sozialen Netze und deren Manipulation, die Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen, unzureichendes Cyberlagebewusstsein/-verständnis sowie verteilte Angriffe auf Systeme (DDoS).

160 Breuss/Kocina, „Anonymous veröffentlicht Daten von 25.000 Polizisten“.

HANDLUNGS-
ERFORDERNISSE

© pagadesign – iStockphoto.com

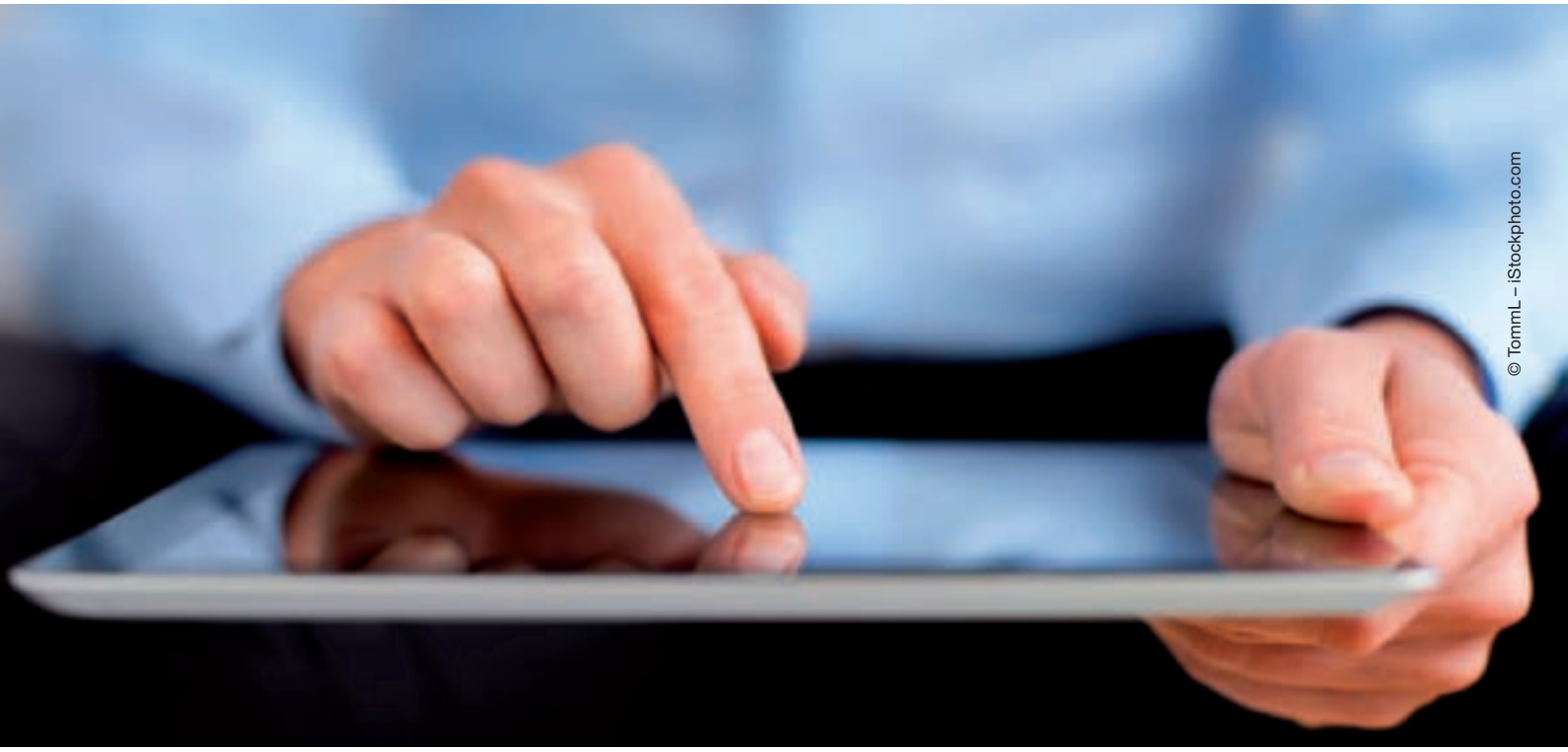
8.1. Bewusstsein für Cyberrisiken fördern und Nutzer qualifizieren
8.2. Aktuelle und künftige Cyberrisiken erkennen, verstehen und bewerten
8.3. Zusammenarbeit im Umgang mit Cyberrisiken systematisch organisieren
8.4. Cyberrisikoprävention stärken
8.5. Cybersicherheit mit Verhaltensanreizen fördern

8

Ebenso vielfältig wie die Bewertung der angesprochenen Risikopotenziale sind die Vorstellungen darüber, welche Maßnahmen am besten geeignet sind, um diese frühzeitig zu erkennen und zu bewältigen. Die von den Gesprächspartnern genannten Vorschläge können zu folgendem umsetzungsorientierten Fünf-Punkte-Programm zusammengefasst werden:

1. Bewusstsein für Cyberrisiken fördern und Nutzer qualifizieren
2. Aktuelle und künftige Cyberrisiken erkennen, verstehen und bewerten
3. Zusammenarbeit im Umgang mit Cyberrisiken systematisch organisieren
4. Cyberrisikoprävention stärken
5. Cybersicherheit mit Verhaltensanreizen fördern

Die fünf Themenbereiche sind inhaltlich miteinander verknüpft, d.h., sie unterstützen und bedingen einander gegenseitig. Mit Blick auf deren konkrete Ausgestaltung ist es wichtig, vorhandene Unterschiede und Gemeinsamkeiten der verschiedenen strategisch relevanten Infrastruktursektoren zu berücksichtigen. Die Ergebnisse der Risikopotenzialanalyse haben deutlich gemacht, dass zwar alle Sektoren von den entsprechenden Risiken betroffen sind, dass diese Betroffenheit aber auch vom gegenwärtigen Vorbereitungsstand abhängt. Damit ist nicht nur die Sicherheitsvorsorge eines jeden Betreibers angesprochen, sondern auch die sicherheitsbezogene Zusammenarbeit innerhalb und zwischen den Sektoren. Diese unterschiedlichen Ausgangslagen führen dazu, dass die Handlungserfordernisse nicht bis ins kleinste Detail beschrieben werden, sondern als allgemein handlungsanleitende Prinzipien zu verstehen sind. Dieser Ansatz soll dazu beitragen, notwendige Gemeinsamkeiten für das Vorgehen zu identifizieren und bei der Umsetzung individuelle, d.h. sektor- und betreiberspezifische Lösungen zu ermöglichen. Dabei geht es immer um das Zusammenspiel von Mensch, Technik und Organisation in einem staatlichen, privatwirtschaftlichen sowie öffentlich-privaten Umfeld.



8.1. Bewusstsein für Cyberrisiken fördern und Nutzer qualifizieren

Bewusstseinsbildung für aktuelle Cyberrisiken und für Maßnahmen, die dazu beitragen, diese zu minimieren, stand auf der Empfehlungsliste zahlreicher Gesprächspartner ganz oben. Dabei wurde allerdings auch ein wichtiges **Spannungsfeld** deutlich:

- Auf der einen Seite wurde argumentiert, dass das Lernen aus Vorfällen wichtig ist und daher die Veröffentlichung realer Zwischenfälle eine kommunikative und edukative Funktion hat.
- Auf der anderen Seite waren Klagen zu hören, dass die Kommunikation über reale Zwischenfälle oftmals zu einer „Stigmatisierung“ und Anprangerung der betroffenen Unternehmen führt. Diese fürchten dadurch um ihre Reputation, sodass ein offener Dialog über Zwischenfälle und deren Bewältigung schwierig wird.

Gefragt ist damit ein **Kommunikationsansatz,** der beide Aspekte berücksichtigt. Kommunikationsverantwortliche der Unternehmen und der Behörden sollten gemeinsam mit den Medien Eckpunkte eines gemeinsamen Vorgehens diskutieren. Dabei ist es sinnvoll, in der Berichterstattung über mögliche Zwischenfälle nicht nur die Probleme in den Vordergrund zu stellen, sondern auch aufzuzeigen, was Behörden und Unternehmen tatsächlich tun, um die Probleme zu lösen. Das gilt ganz besonders für einzelne Infrastruktursektoren, die wie die Energieversorgung in der allgemeinen Mediendarstellung überwiegend als Risikobereiche beschrieben werden, ohne dass der **Stand der Sicherheitsvorbereitungen** ebenso umfassend dargestellt wird. Darüber hinaus sollte auch verstärkt aufgezeigt werden, welche **Chancen** sich österreichischen Unterneh-

men und wissenschaftlichen Einrichtungen auf dem nationalen und internationalen Markt für Sicherheitslösungen eröffnen, wenn deren Produkte und Dienstleistungen auf innovative Weise dazu beitragen, Cyberrisiken zu beheben.

Auf dieser Basis ist auch zu klären, wessen Bewusstsein wofür geschärft werden soll. Neben den Führungsverantwortlichen und Mitarbeitenden im öffentlichen bzw. privatwirtschaftlichen Sektor wurden immer wieder Kinder und Jugendliche als wichtige Zielgruppe angesprochen.

Der Fokus auf **junge Anwender** ergibt sich aus ihrer Affinität für soziale Medien, Smartphones, Online-Spiele und dergleichen. Wie sich Kinder und Jugendliche vor den Risiken dieser Anwendungen schützen können, sollte nach Ansicht verschiedener Gesprächspartner Teil der Lehrpläne sein.[161] Je nach Ausbildungsstufe könnten unterschiedliche Inhalte vermittelt werden, z.B. die Förderung des Bewusstseins dafür, was persönliche Daten überhaupt bedeuten, welche Risiken mit dem Austausch mobiler Endgeräte verbunden sind, wie Betreiber von Internetplattformen mit persönlichen Daten umgehen und wie persönliche Daten, die von jedem Nutzer selbst bereitgestellt werden, von anderen genutzt werden können. Dabei sollte besonders beachtet werden, dass sich Jugendliche sehr stark an Gleichaltrigen orientieren. Kurse, in denen Jugendliche als Betroffene (z.B. von Cyberstalking oder digitalem Identitätsdiebstahl) und Experten (z.B. Nutzung sozialer Medien) sprechen, könnten daher besonders sinnvoll sein.

Gerade der richtige und sichere Umgang mit **sozialen Medien** ist auch im Bereich der Infrastrukturbetreiber ein wichtiges Thema. Dabei geht es um verschiedene Aspekte, wie z.B. die Preisgabe persönlicher sowie behörden- und unternehmensrelevanter Daten in sozialen Medien, die Nutzung sozialer Medien im Arbeitsumfeld und die Sensibilisierung für die notwendige Berücksichtigung verschiedener Rechtsfragen (z.B. Datenschutz, Urheberrecht oder Persönlichkeitsschutz).[162] Zahlreiche Gesprächspartner wiesen darauf hin, dass die Mitarbeitenden in ihren Unternehmen entsprechend geschult werden bzw. diesbezüglich bereits interne Verhaltensrichtlinien erlassen wurden.[163] Vor diesem Hintergrund ist zu überlegen, ob die Sensibilisierungsmaßnahmen einzelner Unternehmen innerhalb der jeweiligen Sektoren oder sogar sektorübergreifend zu allgemeinen Initiativen weiterentwickelt werden könnten. Damit könnten sektorspezifische Besonderheiten von Beginn an entsprechend berücksichtigt werden. Ebenso würden auf diesem Wege auch Wissen und Erfahrungen zwischen den Unternehmen ausgetauscht (Good Practice). Behördenvertreter könnten entsprechende Kampagnen unterstützen und auch an die besonderen Belange des öffentlichen Sektors anpassen.[164]

Weitere Maßnahmen der Bewusstseinsförderung wurden mit Blick auf die **kleinen und mittelgroßen Unternehmen** (KMU) angesprochen. In Zusammenarbeit mit den Wirtschaftskammern sowie Hard- und Softwareherstellern könnten branchenspezifische Kampagnen entwickelt werden, um das Verständnis für die Verwundbarkeit und mögliche Abwehrmaßnahmen zu fördern.[165] Bevor solche Ideen umgesetzt werden, ist es allerdings ratsam, das bestehende Angebot der Behörden und der Verbände auf ihre inhaltlichen Schwerpunkte und die Bewertung aus Sicht der angestrebten Zielgruppe zu prüfen. Zu überlegen ist gleichzeitig, ob solche Initiativen auch weiterhin auf freiwilliger Basis angeboten werden, oder ob es sinnvoll ist, die Teilnahme an entsprechenden Veranstaltungen auch für KMU-Vertreter in speziellen Fällen vorzuschreiben.

161 Interview, 3. April 2012.
162 Auf die Bedeutung der verschiedenen Rechtsfragen wiesen mehrere Behördenvertreter bei der Diskussion der Ergebnisse der vorliegenden Studie am 2. Mai 2012 in Wien hin.
163 Interviews, 2., 7. und 10. Februar 2012.
164 Das gilt beispielsweise auch für Anwender sozialer Medien in besonders sensiblen Aufgabengebieten. So haben in den USA die Heeres-, Luft- und Seestreitkräfte eigene Handbücher für die Nutzung sozialer Medien im Rahmen der Kommunikationsarbeit veröffentlicht.
165 Interview, 26. März 2012.

Schließlich ist auch zu beachten, dass sich die Rolle der **Verbraucherinnen und Verbraucher** im Rahmen umfassend vernetzter und IKT-gestützter Wirtschaftsprozesse verändert. Diese werden zunehmend Teil der unternehmerischen Betriebsabläufe, was sich im Online-Banking bereits deutlich manifestiert und durch die Einführung intelligenter Stromnetze in der Energiewirtschaft abzeichnet. Die Diskussion der Cyberrisiken in den vorangehenden Kapiteln hat deutlich gemacht, dass beispielsweise Endgeräte und Anwendungen der Verbraucherinnen und Verbraucher zunehmend zum Ziel von Cyberkriminellen werden, um darüber an persönliche Daten zu gelangen oder andere kriminelle Taten zu begehen. Die veränderte Rolle der Verbraucherinnen und Verbraucher als „Ko-Produzenten" bzw. Beteiligte der unternehmerischen Betriebsabläufe muss in den Sicherheitskonzepten der Unternehmen entsprechend berücksichtigt werden. Hierfür empfiehlt sich ein sektorübergreifender Dialog unter Einbeziehung auch von Verbraucherverbänden und Datenschützern, damit alle relevanten Sicherheitsaspekte ausgewogen diskutiert werden können.

Die Forderung nach Bewusstseinsbildung und -förderung geht einher mit dem Bedarf an qualifizierter **Aus- und Weiterbildung** in Fragen der IKT-Sicherheit.[166] Auch wenn einige Interviewpartner darauf hingewiesen haben, dass ihre Organisationen in ausreichendem Umfang auf Experten zurückgreifen können, überwog bei der großen Mehrheit die Sorge um fehlendes Fachpersonal. Das spiegelt sich auch in der hohen Relevanz, mit der das Risiko bewertet wurde (Rang 11 von 37 bewerteten Risiken).[167] Die Lageeinschätzung in Österreich stimmt in diesem Punkt überein mit der Sorge, die in zahlreichen anderen Ländern auch geteilt wird. In den USA wurden daher kürzlich mehrere Gesetzesvorschläge eingebracht, um die Aus- und Weiterbildung von Experten im Bereich der Cybersicherheit staatlich zu fördern.[168]

Neben dem Staat können aber auch die Unternehmen und die Verbände einen wichtigen Beitrag zur Qualifizierung der Mitarbeitenden leisten. Zu überlegen ist daher erstens, ob Unternehmen und Verbände vorhandene Expertise und Finanzmittel zusammenlegen können, um geeignete Aus- und Weiterbildungsprogramme zu lancieren. Neben fach- und sektorspezifischen Aspekten sollten dabei vor allem auch Lerninhalte vermittelt werden, die die Experten bei der Bewältigung sektorübergreifender Probleme unterstützen und damit einen direkten Beitrag zur sektorübergreifenden Sicherheitsvorsorge leisten (Kapitel 8.4). Zweitens sollten gezielte Programme des **Personalaustauschs** zwischen Behörden und Unternehmen ins Auge gefasst werden. Damit können die Vertrautheit mit den Konzepten und Abläufen der Partner erhöht, persönliche Netzwerke gestärkt, das persönliche Vertrauen ausgebaut und effektives Handeln in Krisensituationen verbessert werden.

166 Mitunter wurde aber auch davor gewarnt, den Aspekt der IKT-Sicherheit zu stark zu betonen, weil es sich bei einer entsprechend umfassenden Betrachtung der Risiken, die für die Unternehmen relevant sind, nur um einen von mehreren Risikobereichen handelt. Interview, 13. April 2012.
167 Besonders deutlich wurde der Bedarf an Fachkräften von den Vertretern des IKT-Sektors artikuliert. Auch einzelne Vertreter von Behörden und Regulatoren vertraten diese Ansicht. Interviews, 8., 9., 13., 14., 22., 23. Februar 2012.
168 H.R. 76 Cybersecurity Education Enhancement Act; H.R. 2096 Cybersecurity Enhancement Act.
169 Interviews, 26. März 2012 sowie 3. und 16. April 2012.

„Ein gemeinsames Verständnis der Herausforderungen ist die zentrale Voraussetzung, um über Massnahmen zur Verbesserung der Cybersicherheit zu entscheiden.“

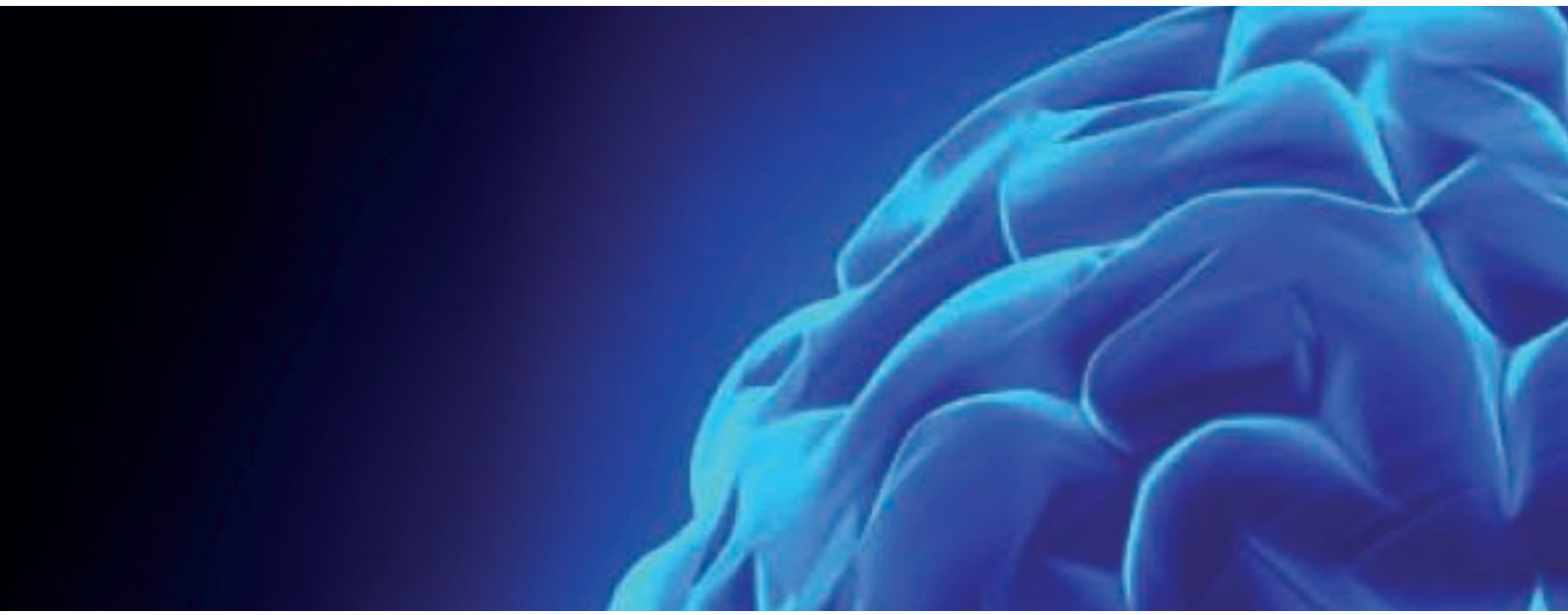
© Steve Cole – iStockphoto.com

Aktuelle und künftige Cyberrisiken erkennen, verstehen und bewerten

8.2.

Ein gemeinsames Verständnis der Herausforderungen ist unerlässlich, um darüber zu entscheiden, welche Maßnahmen erforderlich sind, damit die Cybersicherheit in Österreich verbessert werden kann. Diesbezüglich haben die Gesprächspartner mehrfach den Wert einer Organisationseinheit unterstrichen, in der alle relevanten Informationen zur Bewertung cyberrelevanter Vorgänge zusammenlaufen.[169]

Ein mögliches **Cyberlagezentrum,** so die vorläufige Bezeichnung verschiedener Gesprächspartner, würde eine wichtige Lücke in der bisherigen Cybersicherheitsarchitektur schließen. Mit Hilfe einer solchen Einheit



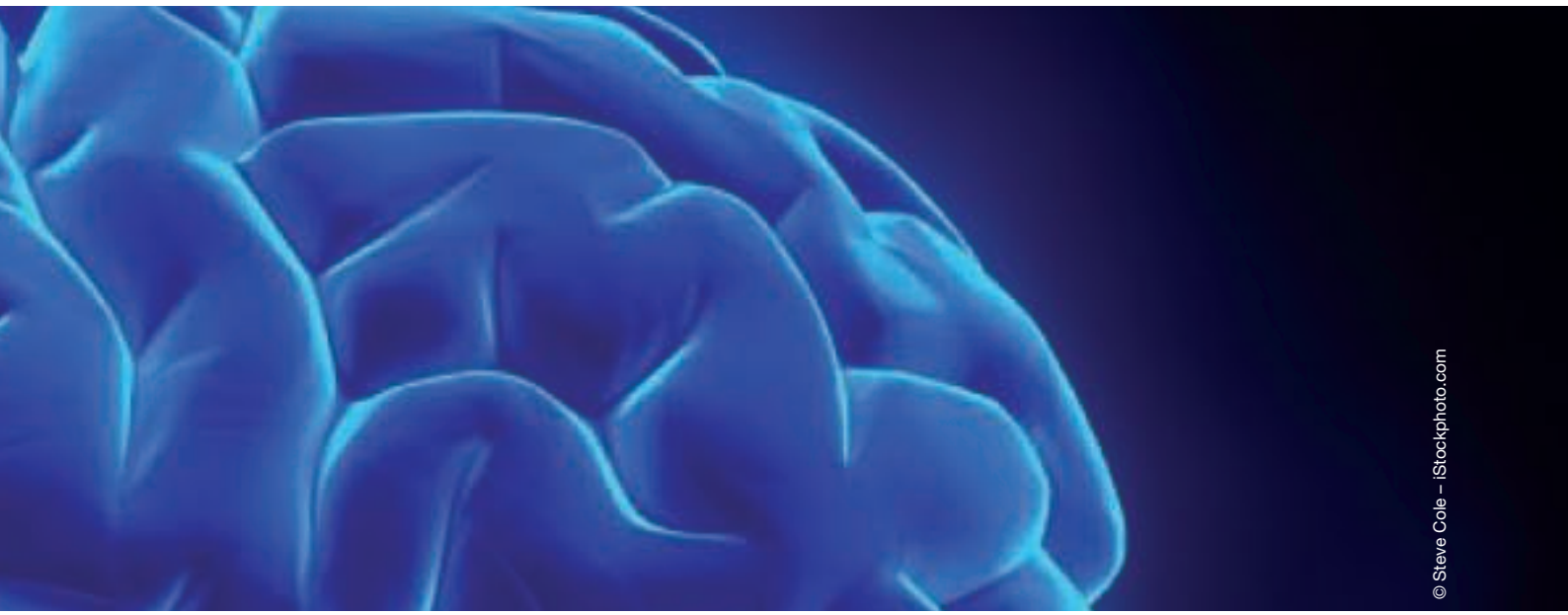
könnten gesicherte Informationen bezogen werden, die dem Erkennen, Verstehen und Bewerten von Cyberrisiken dienen. Die von einer solchen Einheit zu erbringenden Leistungen und die abzudeckenden Funktionalitäten sind zu unterscheiden von der organisatorischen Eingliederung und der Selektion der informationsbeitragenden und -beziehenden Akteure. Zu all diesen Punkten äußerten sich die Experten in den Interviews noch nicht bzw. erst ansatzweise, doch Antworten darauf werden entscheidend sein für die Frage, welche Beiträge von bestehenden Einheiten bereits erbracht werden und wie gegebenenfalls vorhandene Lücken geschlossen werden könnten.

Es dürfte sinnvoll sein, die **Hauptleistungen** eines Cyberlagezentrums darin zu sehen,

- die Informationen verschiedener staatlicher und privatwirtschaftlicher Akteure zu einem gemeinsamen Cyberlagebild zu integrieren;
- die cyberspezifische Lage und Lageentwicklung zu erfassen, zu bewerten und zu verfolgen;[170]
- bei sich abzeichnenden gravierenden Ereignissen alle relevanten Akteure über den Vorfall, die Merkmale der Gefährdung, die daran beteiligten Täter und Unterstützer (soweit identifizierbar), den vermutlichen Verlauf und die erwarteten Auswirkungen des Ereignisses zu informieren;
- die Aufklärung[171] bzw. die (nationale und internationale) Strafverfolgung im Zusammenhang mit einem Ereignis zu unterstützen und Ereignisse systematisch auszuwerten, um daraus Lehren für die Zukunft abzuleiten.

Neben diesen Beiträgen zum Risikomanagement und zur Krisenvorsorge ist zu diskutieren, welche Leistungen ein mögliches Cyberlagezentrum auch im Bereich des eigentlichen Krisenmanagements erbringen soll.[172] Diese Abgrenzung ist wichtig, weil durch das Krisenmanagement in bestehende Zuständigkeiten unterschiedlicher staatlicher Stellen und Infrastrukturbetreiber eingegriffen wird. Das gilt bereits für den einfachen Fall der Prioritätensetzung im Hinblick auf die Absicherung gewisser Komponenten des IKT-Netzes[173] und würde auf jeden Fall dann zu einem Thema, wenn Cyberabwehr- und -gegenmaßnahmen gesamtstaatlich und gesamtwirtschaftlich aufeinander abgestimmt werden müssten. Dieser Aspekt ist für die strafrechtliche Verfolgung möglicher Cyberzwischenfälle genauso relevant wie für den Umgang mit haftungsrechtlichen Ansprüchen, denen sich die Infrastrukturbetreiber im Falle einer angeordneten Unterbrechung ihrer Leistung möglicherweise gegenübersehen.

Ohne konkretere Vorstellungen über die Funktionalitäten, die ein mögliches Cyberlagezentrum abdecken soll, ist eine Diskussion über dessen organisatorische Eingliede-



rung verfrüht. Vor allem auch deshalb, weil einzelne Ressorts und auch Teile der Privatwirtschaft über Elemente verfügen, die als Nukleus einer solchen Einheit interpretiert werden können. Daher wird an dieser Stelle auf die Diskussion verschiedener Organisationsoptionen verzichtet.

Etwas anders liegt der Sachverhalt bei der Frage, welche **Akteure** sinnvollerweise mit dem Cyberlagezentrum verknüpft werden. Hierfür dürfte sich ein Schalenmodell anbieten, das nach der Relevanz einzelner Akteure unterscheidet. Auch hierfür wird es verschiedene Überlegungen geben. Es ist ratsam, zwischen staatlichen Behörden, Anbietern von Hard- und Softwareprodukten, IKT-Betreibern, Betreibern strategisch bedeutender Infrastruktureinrichtungen[174], der allgemeinen Wirtschaft sowie den Bürgerinnen und Bürgern zu unterscheiden.[175] Aus dieser Gliederung könnte in einem Folgeschritt auch abgeleitet werden, welche Informationsbeiträge von den einzelnen Akteuren erwartet würden bzw. zu liefern wären.

Wichtig ist in diesem Zusammenhang das Verhältnis zwischen freiwilliger Informationsweitergabe und Informationspflicht. Hierfür gibt es auch im europäischen Umfeld keine einheitlichen Lösungen. Staatliche Behörden und privatwirtschaftliche Partner werden sich hierüber verständigen müssen. Auf der staatlichen Seite wird darüber hinaus auch zu klären sein, wie die föderale Komponente im Cyberlagezentrum und im begleitenden Informationsverbund abgebildet wird. Hinweise einzelner Gesprächspartner, dass auf Länderebene eigene Monitoringsysteme z.B. zum Erkennen von Anomalien aufgebaut werden, eröffnen interessante föderale Kooperationsansätze.[176]

170 Denkbar ist im Sinne der Arbeitsteilung auch, dass sich das Cyberlagezentrum bewusst auf Aspekte konzentriert, für die seitens der Behörden und Betreiber keine ausreichenden Ressourcen bestehen. Das gilt, wie mehrere Gesprächspartner andeuteten, beispielsweise für den Umgang mit nicht erkannten (IKT-)Anomalien.
171 Interview, 24. April 2012.
172 Das gilt auch für die Frage, ob das mögliche Cyberlagezentrum beispielsweise konkrete Unterstützung durch Handlungsempfehlungen im Bereich der IKT-Sicherheit anbieten soll. Interview, 23. April 2012.
173 Interview, 18. April 2012.
174 Gemeint sind damit in erster Linie jene Betriebe, die vom Bundeskanzleramt und vom Bundesministerium für Inneres auf die sogenannte ACI-Liste gesetzt wurden. Neben den eigentlichen Betreibern wird auch zu beantworten sein, welche Rolle die Verbände in einem künftigen cyberbezogenen Informationsverbund spielen sollen und können.
175 Letztere dürften nur eine indirekte Verbindung aufweisen und vom Cyberlagezentrum über allgemeine Warnhinweise informiert werden.
176 Interview, 14. Februar 2012.

„Österreichs Cybersicherheitsarchitektur soll partnerschaftlich aufgebaut werden - darin sind sich alle Gesprächspartner einig.“

8.3. Zusammenarbeit im Umgang mit Cyberrisiken systematisch organisieren

Die Relevanz einer lückenhaften Cyber-Governance wurde in den Interviews zwar als gering eingestuft, doch die Diskussion um mögliche Handlungserfordernisse verdeutlichte, dass die Gesprächspartner bei den institutionellen Rahmenbedingungen großen Handlungsbedarf sehen, damit die Zusammenarbeit im Bereich der Cybersicherheit verbessert werden kann. Interessanterweise bezogen viele Experten ihre Einschätzung auf die Zusammenarbeit zwischen den Behörden, doch auch die sektorübergreifende Zusammenarbeit zwischen den Infrastrukturbetreibern und den übrigen Unternehmen ist ausbaufähig. Folgende Aspekte kamen zur Sprache:

Grundsätze

Österreichs Cybersicherheitsarchitektur soll partnerschaftlich aufgebaut werden, darin sind sich die Gesprächspartner einig. Damit herrscht in einem wichtigen Punkt Übereinstimmung zwischen den Behörden und der Wirtschaft, denn auch das bisherige Programm zum Schutz kritischer Infrastrukturen

und die Aussagen der Bundesinnenministerin zur künftigen Cybersicherheitsstrategie betonen die zentrale Rolle eines partnerschaftlichen, weitgehend auf Kooperation setzenden Ansatzes.[177] Allerdings gibt es auch in einem partnerschaftlichen Ansatz eine Rollenverteilung zwischen den Behörden und den Unternehmen. Wie diese mit Bezug auf das gemeinsame Ziel der Cybersicherheit aussehen könnte, ließen die Gesprächspartner noch weitgehend offen.

Um die Cybersicherheit wirklich spürbar zu verbessern, ist es unerlässlich, das Bekenntnis zur öffentlich-privaten Sicherheitspartnerschaft in allen relevanten Feldern der Zusammenarbeit zu realisieren. Das gilt für die Risikoanalyse und Früherkennung genauso wie für die Strategiedefinition, die Krisenprävention, das Krisenmanagement und die Krisennachsorge sowie für die unterstützenden Aufgabenfelder wie Ausbildung, Forschung und Entwicklung, Beschaffung, Finanzierung und Kommunikation.[178] Die Partnerschaft in diesen Feldern kann schrittweise wachsen, sollte jedoch von Beginn an so angelegt werden, dass alle Felder bedient werden können.

Institutionen/Plattformen

Die Zusammenarbeit zur Förderung der Cybersicherheit soll in einem geordneten institutionellen Umfeld erfolgen. Dabei ließen die Gesprächspartner keine Zweifel aufkommen, dass die gegenwärtige Vielzahl unterschiedlicher Initiativen eher als Problem denn als Lösungsbeitrag interpretiert wird.[179] Erforderlich ist daher eine institutionelle Bereinigung durch Zusammenführung verschiedener Ansätze. Einige Gesprächspartner sprachen sich für drei Schwerpunkte aus: Diskussion strategisch relevanter Grundsatzfragen, Informationsaustausch zur Erstellung des Cyberrisikobildes (Kapitel 8.2) und Koordination von Maßnahmen. Dies könnte wie in den Niederlanden oder in Deutschland zu einem Modell mit einer Art Nationalem Cybersicherheitsrat und einem Cyberlagezentrum als „Arbeitsmuskel“ führen. Wer in den jeweiligen Gremien vertreten bzw. mit diesen verbunden sein sollte, ließen die Experten noch offen. Wichtig ist, dass der Gedanke der Partnerschaft konsequent umgesetzt wird, d.h. Behörden und Wirtschaft gleichermaßen in allen Gremien und auf allen Stufen vertreten sind.

Nicht explizit angesprochen, aber aus Sicht der Praxis genauso relevant ist die Frage, wie sich die Infrastrukturbetreiber und die jeweiligen Infrastruktursektoren künftig organisieren, um mit den Behörden in Fragen der Cybersicherheit – und in weiterer Folge auch zu anderen sicherheitsrelevanten Themen – zu kooperieren. Auch wenn die Entscheidung darüber grundsätzlich den Unternehmen und den sektorrelevanten Verbänden überlassen sein sollte, ist es sinnvoll, hierfür Grundsatzgedanken zu entwickeln. Gäbe es beispielsweise innerhalb der strategisch bedeutenden Infrastruktursektoren einen Leitverband, so könnte dieser Ansprechpartner für den Austausch sensibler Informationen benennen. Über den Verband bzw. über sektorspezifische CERTs auf Verbandsebene[180] könnten die Behörden mit den Unternehmen kommunizieren. In den Unternehmen selbst spricht vieles dafür, allgemeine Aspekte der Unternehmenssicherheit und spezifische Belange der IKT-Sicherheit aus einer Hand zu gestalten. Einige Unternehmen haben die Position eines Chief Information Security Officer (CISO) geschaffen. Unternehmen, die diesen Ansatz verfolgen, können als Rollenmodelle fungieren und gemeinsam mit den sektorrelevanten Verbänden dazu beitragen, dass auch andere Unternehmen den Übergang zu einer verstärkt integralen Betrachtung von Unternehmens- und IKT-Sicherheit einleiten.

177 Masterplan Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP), S. 11. Bundesinnenministerin Mag.ª Johanna Mikl-Leitner hat sich bei zwei Veranstaltungen am 20. September 2011 und am 27. Februar 2012 für den partnerschaftlichen Ansatz ausgesprochen.
178 Siehe hierzu die Grundsatzüberlegungen von: Fischer, „Sicherheitspartnerschaft zwischen Staat und Wirtschaft“, S. 27–46.
179 Interviews, 2. und 13. Februar 2012
180 Interview, 24. April 2012.

Zuständigkeiten

Die Zuständigkeiten in der normalen und in der außerordentlichen Lage müssen geklärt werden. Infrastrukturbetreiber wiesen diesbezüglich auf bestehende Zielkonflikte hin. So haben die Telekommunikationsbetreiber heute zwar bereits rechtlich die Möglichkeit, einen Nutzer vom Netz abzukoppeln, wenn dieser die technische Sicherheit des Netzes stört, doch wie ein solcher Vorgang vor dem Hintergrund des Postulats der Netzneutralität bewertet würde, war den Gesprächspartnern nicht klar.[181]

Offen ist darüber hinaus auch, wer wen wann worüber informiert und wer gestützt auf diese Informationen über welche Maßnahmen entscheidet und deren Koordination sicherstellt. Damit sprachen die Experten auch die Arbeitsteilung in einer künftigen österreichischen Cybersicherheitsarchitektur an. Deren Definition ist einer der zentralen Umsetzungsschritte. Gegenwärtig zeichnet sich lediglich ein Konsens darüber ab, dass es sinnvoll ist, Fähigkeiten zur Erkennung und Bewertung von Cyberrisiken an einer Stelle zu bündeln. Wie aber die Verbindung zwischen diesem Instrument der Risikoanalyse und -bewertung und den eher operativ tätigen Einheiten im Bereich Abwehr-/Gegenmaßnahmen aussehen soll, bleibt offen. Vereinzelt wurde angeregt, die operative Koordination beim Staatlichen Krisen- und Katastrophenschutzmanagement (SKKM) anzusiedeln.[182] Das ist mit Blick auf andere operativ tätige Einheiten im staatlichen Umfeld aber nur eine mögliche Option. Zudem lässt dieser Punkt die Frage unbeantwortet, ob es auch sinnvoll sein könnte, dass die Betreiber in ihren jeweiligen Sektoren operative Koordinationselemente schaffen, wie das beispielsweise in

181 Interview, 3. April 2012.
182 Interview, 3. April 2012.
183 Interviews, 2. Februar, 6. Februar 2012 und 26. März 2012.
184 Ein Gesprächspartner aus dem Finanzsektor wies explizit darauf hin, dass diese Möglichkeit bislang noch nicht gegeben sei. Interview, 4. April 2012.
185 Mehrheitlich sprachen sich die Experten für die Institutionalisierung des Informationsaustauschs zwischen staatlichen Stellen und Unternehmen aus. Nur in Einzelfällen wurde der Nutzen eines solchen Vorgehens unter Bezug auf bereits bestehende Einrichtungen und Initiativen bezweifelt. Interviews, 18. und 20. April 2012. Im Rahmen der Diskussion der Ergebnisse der vorliegenden Studie am 2. Mai 2012 in Wien betonten insbesondere die Vertreter der Privatwirtschaft, dass eine einseitige Meldepflicht der Unternehmen gegenüber den Behörden nicht ausreiche – Rückmeldungen und Informationsweitergabe der Behörden an die Unternehmen seien genauso wichtig.
186 Interviews, 24. Januar 2012 und 2. Februar 2012.
187 Interview, 2. Februar 2012.
188 Interview, 23. Februar 2012.
189 Interview, 18. April 2012.
190 Interviews, 6. Februar 2012 und 3. April 2012.
191 Interview, 15. Februar 2012.
192 Vertreter der Privatwirtschaft wiesen bei der Diskussion der Ergebnisse des vorliegenden Berichts am 2. Mai 2012 in Wien auf diesen Aspekt hin und fragten: Wenn ein Unternehmen beim Test von IKT-Systemen Lücken feststellt, an wen darf diese Information weitergegeben werden: Nur an den Hersteller oder auch an andere Nutzer in der gleichen Branche bzw. in anderen Sektoren?
193 Interview, 15. Februar 2012.

Deutschland im Versicherungssektor und in der Schweiz sowie in Schweden für den Telekommunikationssektor der Fall ist.

Ansprechpartner

Eng verbunden mit der geforderten Klärung der Zuständigkeiten ist auch die Identifizierung von Ansprechpartnern für Cybersicherheit im staatlichen und privatwirtschaftlichen Umfeld. Wichtig ist, dass die diesbezügliche Information breit kommuniziert wird, damit allen Beteiligten klar ist, wer sich im Falle welcher Cyberrisiken an wen wenden kann, und verhindert wird, dass Informationen nicht oder zu spät weitergegeben werden.[183]

Wenn es sich dabei um Ansprechpartner im staatlichen Bereich handelt, sollte allerdings auch sichergestellt werden, dass diese die erhaltenen Informationen gleich behandeln. Wenn es nämlich so ist, dass ein staatlicher Ansprechpartner die Informationen zur Anzeige bringt, der andere aber nicht, dürften die ungleichen Bedingungen auf der staatlichen Seite zur Informationsverzerrung beitragen. Ebenso sollten die Ansprechpartner innerhalb ihrer jeweiligen Organisationen über entsprechende Entscheidungskompetenzen verfügen, um Maßnahmen insbesondere im Ereignisfall beschließen zu können. Gerade im Umgang mit sensiblen Informationen ist auch zu klären, ob Ansprechpartner in gewissen Funktionen zwingend sicherheitsüberprüft werden sollen.[184]

Austauschprozesse

Die Notwendigkeit strukturierter und wechselseitiger Austauschprozesse zu verschiedenen Aspekten, die die Cybersicherheit betreffen, wurde mehrfach angesprochen.[185] Das Spektrum wurde breit definiert und umfasste u.a. folgende Anregungen:

- Verstärkter sektorübergreifender Dialog zwischen die Regulatoren, vor allem im Hinblick auf die Einführung neuer Technologien und den damit verbundenen Fragen der Cybersicherheit[186]
- Dialog mit den Herstellern von Steuerungssystemen im Hinblick auf erkannte Schwachstellen und Möglichkeiten, diese zu beheben[187]
- Sektorübergreifender Austausch von Erkenntnissen aus dem Bereich der Technologiefolgenabschätzung und möglichen Konsequenzen, die sich daraus für die IKT-Sicherheit ergeben können[188]
- Stärkung des internationalen Austauschs innerhalb und zwischen den Sektoren[189]
- Zusammenarbeit aller relevanten Akteure bei einem Cyberereignis[190]
- Aufarbeitung gravierender Cyberereignisse, um daraus für sich selbst und die Partner in anderen Sektoren Lehren ableiten zu können[191]

Damit ein systematischer Informationsaustausch überhaupt möglich ist, müssen verschiedene Grundsatzaspekte berücksichtigt und offene Fragen geklärt werden:

- Die rechtlichen Rahmenbedingungen des Informationsaustauschs müssen definiert werden. Dazu bedarf es eines Verständnisses darüber, wer welche Informationen an wen weitergeben darf, wer was damit tun darf und an welche Dritten diese Informationen weitergegeben werden können. Diese Fragen müssen im Hinblick auf den Austausch zwischen Behörden und Unternehmen genauso geklärt werden wie mit Bezug auf den Informationsaustausch zwischen Unternehmen.[192]
- Ebenso muss geklärt werden, auf welchem Weg der Informationsaustausch erfolgt und welche Verfahren bzw. Instrumente dafür eingesetzt werden. Wichtig ist dabei insbesondere der Schutz der Daten, wenn sie zwischen verschiedenen Beteiligten übermittelt werden.[193]
- Bestehende Meldewege und Informationsaustauschprozesse, die es in einzelnen Infrastruktursektoren für den Dialog zwischen Behörden und Betreibern gibt, müssen berücksichtigt werden.
- Doppelspurigkeiten bei den Informationswegen müssen vermieden werden. Das kann insbesondere auf der staatlichen Seite dazu führen, dass sich Ministerien und Behörden darüber verständigen müssen, welche Stellen als Informationsdrehscheiben für die Wirtschaft agieren.

8.4. Cyberrisikoprävention stärken

Aufgrund der Expertengespräche ist klar, dass die jeweiligen Unternehmen und Behörden bereits umfangreiche Maßnahmen ergriffen haben, um sich im Rahmen der betrieblichen Notfallvorsorge auf verschiedene Ausfallrisiken vorzubereiten. Das breite Spektrum der in Abbildung 13 illustrierten Maßnahmen unterstreicht, dass es sinnvoll ist, die jeweiligen Ansätze und die dabei gesammelten Erfahrungen im Sinne von Good Practices zur Sensibilisierung anderer Behörden und Unternehmen auszuwerten und aufzubereiten.

Gestützt darauf ergeben sich aus den Rückmeldungen der Gesprächspartner zwei eng miteinander verknüpfte Ansatzpunkte zum Ausbau der Cyberrisikoprävention in Österreich:

Nationales Cyberrisikomanagement

Richtigerweise haben einzelne Gesprächspartner darauf hingewiesen, dass es ein nationales Cyberrisikomanagement in Österreich bislang noch nicht gibt.[194] Der Aufbau eines solchen Rahmenmanagementsystems sollte daher im Zuge der Erarbeitung einer nationalen Cybersicherheitsstrategie angestrebt werden.[195] Mit den verschiedenen Initiativen und Plattformen, die in den letzten Monaten in Österreich lanciert wurden, bestehen hierfür erste Ansätze. Damit ein nationaler Cyberrisikomanagementansatz allerdings auch Wirkung erzielt, sind seine Bausteine klar zu definieren. Sinnvoll erscheint ein solcher Ansatz vor allem dann, wenn er dazu beiträgt,

- das gemeinsame Verständnis über aktuelle und künftige Herausforderungen der Cybersicherheit zu fördern;
- erkannte Cyberrisiken zu bewerten und zu verfolgen sowie die technischen und nichttechnischen Ursachen konkreter Gefährdungen im Einzelfall zu identifizieren.

Die Empfehlungen des vorliegenden Berichts sind bereits darauf ausgerichtet, diese drei Zielsetzungen zu unterstützen. Eine wichtige Umsetzungsaufgabe wird nun darin bestehen, einen geeigneten institutionellen Rahmen zu schaffen, der es ermöglicht, vorhandene Kräfte optimal zu bündeln und weiterzuentwickeln.

Sektorübergreifende betriebliche Notfallvorsorge (Business Continuity Management, BCM)

BCM leistet einen wichtigen Beitrag, damit Organisationen ihre Notfallvorsorge und Widerstandsfähigkeit im Umgang mit Störungen unterschiedlicher Art stärken können. Einzelne Betriebe setzen denn auch bereits konsequent auf BCM, das haben die Interviews gezeigt. Im Hinblick auf die Weiterentwicklung des Österreichischen Programms zum Schutz Kritischer Infrastruktur (APCIP) und die Stärkung der präventiven Cybersicherheit ist es ratsam, BCM als Schlüsselinstrument zu sehen, mit dem verschiedene Ziele gleichzeitig erreicht werden können. Zu diesem Zweck sollten Behörden, Betreiber strategischer Infrastrukturen und Verbände gemeinsam erörtern,

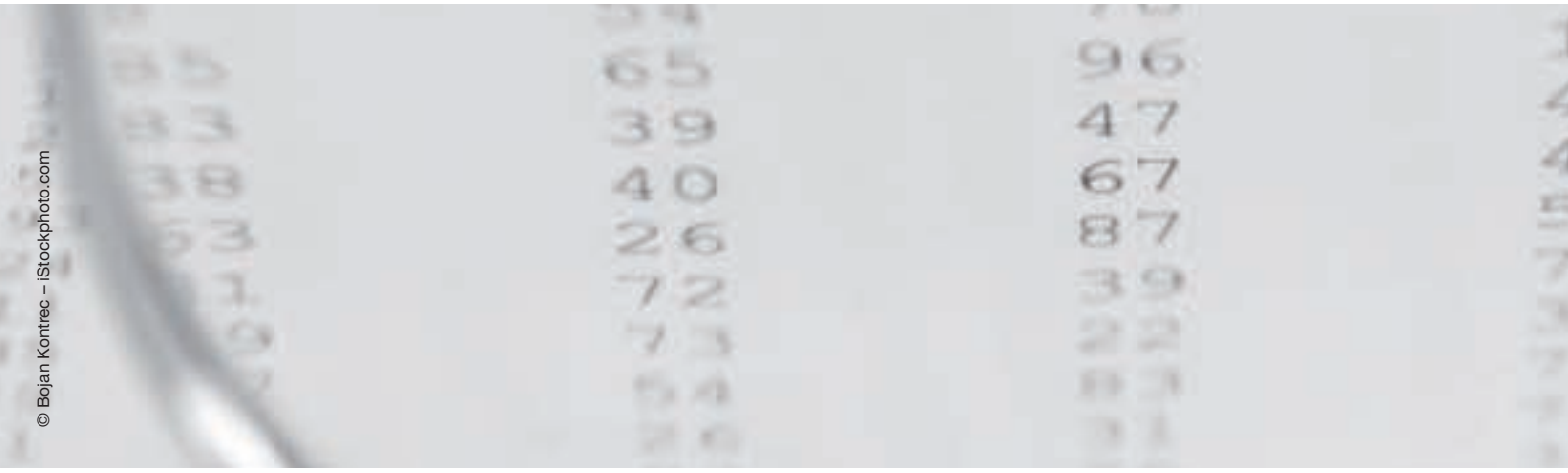
- Aufbau modernster Notstromsysteme
- Betrieb eigener, komplett unabhängiger Netze
- Betrieb mehrerer physisch voneinander getrennter Rechenzentren und alternativer Standorte für andere kritische IT-Prozesse
- Bündelung der Verantwortung für verschiedene Aspekte in der Position des Chief Information Security Officer (CISO)
- Definition besonderer Spezifikationen für Hard- und Software bei öffentlichen Ausschreibungen
- Durchführung von Lieferantenaudits
- Entwicklung eigener digitaler Schlüssel und Zertifikate
- Notfallpläne für verschiedene Krisenszenarien, Ausfall kritischer Systemelemente und Personalengpässe (z.B. Pandemie)
- Penetrationstests für kritische Systeme, die Verbindung zur Außenwelt ermöglichen (z.B. Wartungstunnel, Online-Systeme)
- Penetrationstests für kritische unternehmensinterne Systeme
- Qualitätssicherungsprozesse beim Einkauf von Hardware
- Richtlinien für Mitarbeitende zur Nutzung sozialer Medien
- Risikoaverse Unternehmenskultur in Bezug auf Einführung von IKT-Neuerungen
- Rückgriff auf gesicherte Leitungen, die teilweise von Bundesbehörden bereitgestellt werden
- Schulung der Mitarbeiter in Sicherheitsfragen
- Test der Mitarbeiter durch Einsatz staatlicher Sicherheitskräfte
- Übungen zum Test der eigenen Notfallpläne und der Abläufe in kritischen Unternehmenseinheiten
- Umfassendes Prozessmanagement und Zertifizierung nach ISO 27000
- Unternehmenseigene Programme zur Spionageabwehr
- Verfahren zum Test der Soft- und Hardware vor dem Einsatz

Abbildung 13: Beispiele aktueller Maßnahmen zur Stärkung der Cyberrisikoprävention in Österreich

Quelle: Interviews, 31. Januar, 1, 2., 6., 7., 9., 10, 13. und 14. Februar 2012

- wie BCM vor allem in den strategisch bedeutenden Infrastruktursektoren gefördert werden kann;
- ob es sinnvoll ist, BCM für die strategisch relevanten Infrastrukturbetreiber als verbindlich zu erklären;
- wie Wechselwirkungen zwischen den BCM-Vorkehrungen in den einzelnen Sektoren verstärkt sektorübergreifend koordiniert werden können;
- für welche Prozesse und Dienste, die sektorübergreifend von Bedeutung sind, möglicherweise eigenständige BCM-Vorgaben definiert werden sollten;
- wie und durch wen die Umsetzung von BCM in den strategisch relevanten Infrastruktursektoren überprüft wird (Kapitel 8.5) und
- mit welchen zusätzlichen Maßnahmen BCM-Zielsetzungen erreicht werden können.[196]

194 Interview, 3. April 2012.
195 Im Kontext des österreichischen Programms zum Schutz Kritischer Infrastruktur (APCIP) arbeiten das Bundeskanzleramt und das Bundesministerium für Inneres an einem Leitfaden Risikomanagement. Dieser spricht neben dem Chancen- und Risikomanagement auch das Business Continuity Management und das Corporate Security Management an. Der Leitfaden wird voraussichtlich in der zweiten Jahreshälfte 2012 veröffentlicht.
196 Mehrfach wurde in den Gesprächen auch die Rolle der strategischen Netzwerkstrukturplanung angesprochen. Diese könnte vor allem mit Blick auf das Risikopotenzial der Infrastrukturkollokation wertvolle Beiträge leisten. Das gilt neben der Bundes- vor allem auch für die Länderebene. Interviews, 2., 8., 14. und 22. Februar 2012.



© Bojan Kontrec – iStockphoto.com

8.5. Cybersicherheit mit Verhaltensanreizen fördern

Anreize dienen dazu, das Verhalten der Akteure in eine Richtung zu lenken, die es erlaubt, das Niveau der Cybersicherheit in Österreich zu verbessern.[197] Das Urteil der befragten Experten bestätigt die grundsätzliche Erkenntnis, dass Umfang und Notwendigkeit möglicher Verhaltensanreize sehr stark vom jeweiligen Sachgebiet abhängen. Im unmittelbaren staatlichen Umfeld und bei Betreibern, die sich mehrheitlich in staatlichem Besitz befinden, wird die Notwendigkeit einer anreizorientierten Regulierung als gering eingestuft. Strategisch wichtige Unternehmen in Infrastruktursektoren mit ausgeprägtem Wettbewerb und internationaler Ausrichtung begrüßen dagegen die Absicht, auch bei Sicherheitsfragen stärker über die Definition gezielter (positiver und sanktionierender) Anreize nachzudenken. Zu beachten ist darüber hinaus auch der Grad der sektorspezifischen Sicherheitsvorschriften, die bereits erlassen wurden. Je dichter das Netz bestehender Vorschriften, desto kleiner ist in der Regel der Handlungsspielraum, der für anreizorientierte Regulierungsansätze zur Verfügung steht. Besonders relevant ist gerade in diesem Zusammenhang eine verstärkt sektorübergreifende Betrachtung der bestehenden Vorgaben, um Wechselwirkungen zwischen bestehenden Regimes und deren Auswirkungen auf die Sicherheitsbemühungen der Infrastrukturbetreiber besser zu erfassen.

Gestützt darauf wurden in den Gesprächen vier Aspekte angesprochen, die aus Sicht der Interviewpartner verhaltenslenkend ausgestaltet werden können. Zusätzlich zu dem in Kapitel 8.3 angesprochenen Informationsaustausch zwischen den Behörden und den Infrastrukturbetreibern ging es dabei vor allem um Standards, konkrete Vorschläge zum Ausbau staatlicher Sicherheitsleistungen für die Infrastrukturbetreiber und gemeinsame Übungen.

Standards

Auch wenn eine Mehrheit der Gesprächspartner die Ansicht vertrat, dass Standards Verhaltensanreize definieren können, wurde die Rolle von Standards als Instrument zur Förderung der Cybersicherheit kontrovers diskutiert. Die Kontroverse lässt sich in vier Sachfragen zusammenfassen, die künftig klar beantwortet werden müssen:

Mehr Standards oder bessere Umsetzung?
Mehrfach wurde betont, dass die zentrale Herausforderung weniger in der Definition neuer oder der Weiterentwicklung bestehender Standards,[198] sondern in deren konsequenter Umsetzung besteht. Allerdings blieben die Gesprächspartner, die ein Umsetzungsdefizit ansprachen, die Antwort schuldig, worin die Gründe der mangelnden Beachtung und Umsetzung bestehender Standards liegen. Auf jeden Fall zeigt dieser Punkt, wie wichtig es ist, die Diskussion um Standards für Cybersicherheit zu präzisieren: Erstens mit Blick auf den Begriff der Cybersicherheit und dessen, was darunter konkret verstanden wird; zweitens mit Bezug zu

den konkreten Sicherheitsanforderungen, die sich daraus ergeben; drittens hinsichtlich der Anwendungsfelder, denn im staatlichen Umfeld gibt es genauso einen Bedarf nach Mindestsicherheitsstandards wie in der Wirtschaft;[199] und viertens bezüglich der Rolle, die gewisse Infrastrukturbetreiber bei der Um- und Durchsetzung bestimmter Standards spielen können.[200]

Welche Standards sind relevant?

Angesichts der Fülle unterschiedlicher Standards ist eine klare Linie notwendig, um zu definieren, welche Standards für welche Aspekte der Cybersicherheit in Österreich relevant sind.[201] Das gilt – und darin liegt die eigentliche Herausforderung – für die sektorspezifische genauso wie für die sektorübergreifende Betrachtung. Vor allem beim letzten Punkt sehen die Gesprächspartner unter Beachtung ihrer Aussagen zu BCM (Kapitel 8.4) entsprechenden Handlungsbedarf. Um diesen zu beheben, ist es ratsam, künftig verstärkt sektorübergreifende Risikoanalysen durchzuführen. Verschiedene Gesprächspartner regten auch die Definition eines Mindestschutzniveaus an und verwiesen in diesem Zusammenhang auf die im BSI-Grundschutzhandbuch enthaltenen Mindeststandards.[202] Andere Experten gaben allerdings zu bedenken, dass konkrete Entscheidungen der Unternehmen durch zu viele unverbindliche Empfehlungen erschwert werden können.[203] Standards können sich nicht nur auf technische Normen beziehen, sondern auch organisatorische Aspekte definieren. In diesem Zusammenhang wurde beispielsweise angeregt, die Ernennung eines Sicherheitsbeauftragten rechtlich vorzuschreiben. Dahinter steht die Annahme, dass es schwieriger ist, eine solche Position im Zuge von Rationalisierungsmaßnahmen zu streichen, wenn diese gesetzlich gefordert ist.[204]

Wer prüft was?

Aus der Verbindung von Standardisierung und Zertifizierung ist in den letzten Jahren ein eigenes Dienstleistungssegment entstanden. Die Gesprächspartner hoben hervor, dass innerhalb der einzelnen Infrastruktursektoren spezifische Audit-Expertise aufgebaut wurde, die von den Unternehmen in den jeweiligen Sektoren mitunter besser akzeptiert wird als die Leistung von Wirtschaftsprüfern.[205] Auch wenn diese Position fachlich nachvollziehbar ist, verstärkt sie zusätzlich die bereits schon deutlich ausgeprägte sektorale Zersplitterung der Denk- und Handlungsansätze. Hinzu kommt, dass es neben der Vielzahl verschiedener Akteure, die Audits durchführen (siehe nächster Absatz), auch Ab-

197 Siehe hierzu weiterführend: Borchert, Cybersicherheit intelligent regulieren, S. 40–41.
198 Bei der Diskussion der Ergebnisse der vorliegenden Studie am 2. Mai 2012 in Wien wurde seitens privatwirtschaftlicher Vertreter allerdings darauf hingewiesen, dass auch bei der sektorübergreifenden Weiterentwicklung von Standards noch Handlungsbedarf besteht. Dieser wurde vor allem anhand der Frage diskutiert, welche Mindeststandards im Bereich der IKT-Sicherheit sektorübergreifend als verbindlich erklärt werden könnten.
199 Eine Gesprächspartnerin regte an, Mindestsicherheitsstandards auch für Gemeinden zu definieren. Interview, 17. April 2012.
200 Infrastrukturbetreiber, die auf Basis eines natürlichen Monopols arbeiten bzw. auf andere Weise über eine besondere Marktposition verfügen, können die Sicherheit auf den vorgelagerten Stufen der Wertschöpfungskette erhöhen, indem sie die Einhaltung bestimmter Standards für verbindlich erklären. Interview, 16. April 2012.
201 Interview, 21. Februar 2012.
202 Interviews, 16. April 2012.
203 Interview, 23. Februar 2012.
204 Interview, 16. April 2012.
205 Interviews, 6. Februar 2012, 16. April 2012.

weichungen der inhaltlichen Schwerpunkte gibt, die mit Audits geprüft werden.[206] Daher drängt sich zusätzlich die Frage auf, wer nach welchen Kriterien die Prüfer prüft bzw. sicherstellt, dass die Prüfer ihre Fähigkeiten ebenfalls weiterentwickeln. Auch wenn in den Gesprächen anerkannt wurde, dass in dieser Hinsicht Fortschritte[207] erzielt wurden, blieben kritische Hinweise nicht aus. So äußerte ein Gesprächspartner sein Unbehagen darüber, dass bei spezifischen Sicherheitsprüfungen (z.B. Penetrationstests) nicht klar ist, wie die durchführenden Experten mit den gewonnenen Erkenntnissen umgehen.[208] Deshalb sollte unter Beteiligung aller relevanten Akteure dringend geklärt werden, welchen Beitrag Audits im Bereich der Cybersicherheit leisten können.[209]

Was geschieht bei Nichtbeachtung?

Diese Frage spricht die Sanktionsdimension an. Mehrmals wurde die Rolle des Haftungs- und Strafrechts vor allem mit Blick auf die Verantwortung des Managements angesprochen.[210] Wenn klar ist, welche Schutzziele erreicht werden sollen und welche Standards bzw. Maßnahmen hierfür erforderlich sind, könnten Ansätze entwickelt werden, die die Verantwortung des Managements für Sicherheitsmaßnahmen erhöht. Dabei wird es allerdings wichtig sein, dass zwischen der Verantwortlichkeit, den einzelnen Maßnahmen und den definierten Vorschriften auch ein direkter Zusammenhang besteht, der überprüft werden kann. Nur dann dürfte der Sanktionsmechanismus als legitim erachtet werden.[211]

Staatliche Sicherheitsleistungen

Verschiedene Unternehmensvertreter argumentierten, dass der Staat mehr machen könnte, um die Sicherheitsanstrengungen der Infrastrukturbetreiber zu unterstützen. Dieser Wunsch wurde von einigen Behördenvertretern indirekt geteilt, indem diese darauf hinwiesen, dass der Staat für sich selbst sicherheitsrelevante Dienste entwickelt hat, die auch der Wirtschaft angeboten werden könnten. Um diesbezüglich einen Abgleich zwischen Wünschbarem und Möglichem herbeizuführen, ist es sinnvoll, dass Staat und Wirtschaft gemeinsam ein Verständnis dafür entwickeln, welche Sicherheitselemente gefördert werden könnten.[212] Dafür ist es allerdings unerlässlich, vorab gemeinsame Ziele im Bereich der Cybersicherheit zu definieren. Ohne Verständigung darüber, bei welchen Kernprozessen in welchen strategischen Infrastrukturen beispielsweise welche Ausfallzeiten toleriert werden, ist es nicht möglich, Sicherheitsförderungsmaßnahmen zu definieren. Dieser Schritt sollte daher zuerst in Angriff genommen werden. Er kann auch dazu beitragen, unterschiedliche Erwartungshaltungen der beteiligten Akteure zu identifizieren und zu präzisieren.

Vor diesem Hintergrund nannten die Gesprächspartner folgende Beispiele konkreter staatlicher Sicherheitsunterstützung zugunsten Dritter:

- Verschiedene staatliche Behörden haben eigene digitale Schlüssel und digitale Zertifikate entwickelt. Diese könnten den privatwirtschaftlichen Partnern zur Verfügung gestellt werden.[213]
- In einigen staatlichen Bereichen wurden zur Überprüfung von Abläufen und zur Prüfung der Zuverlässigkeit einzelner Komponenten Auditverfahren definiert. Solche Auditdienste könnten der Privatwirtschaft ebenfalls angeboten werden.[214] Auch einzelne Gesprächspartner aus dem privatwirtschaftlichen Umfeld haben angeführt, dass ihre Unternehmen sehr strenge IKT-Sicherheitsaudits durchführen.[215] Daher ist zu überlegen, ob durch die Bündelung der vorhandenen Expertise in diesem Bereich eine gezielte Dienstleistung für Betreiber im Umfeld strategisch relevanter Infrastrukturen angeboten werden kann.
- Ausgewählte staatliche Behörden arbeiten an sicheren Cloud-Diensten. Diese könnten auch anderen Behörden zugänglich gemacht werden.[216]
- Um auch in Krisenfällen und bei Ausfall der Netze der Infrastrukturbetreiber die Erreichbarkeit und Konnektivität sicherzustellen, könnten staatliche Stellen ihre Netzwerkkapazitäten bereitstellen.[217]
- Experten aus staatlichen Behörden könnten bei Krisenereignissen die betroffenen Akteure in der Privatwirtschaft direkt vor Ort unterstützen.[218]
- Staatliche Behörden können Leitfäden und Musterkonzepte zu verschiedenen Aspek-

ten der Cybersicherheit erarbeiten, die insbesondere von KMU übernommen und angewendet werden könnten.[219]

Weitere wichtige Impulse – auch im Hinblick auf den Aufbau und den Erhalt von Expertisefeldern, die für die Cybersicherheit in Österreich wichtig sind – könnten die Behörden im Bereich der Rahmenbedingungen setzen, indem sie beispielsweise

- vorhandene Vorschriften vereinfachen, um Beschaffungsvorgänge zu beschleunigen[220] und die kurzfristige Beiziehung von Experten aus dem privatwirtschaftlichen Umfeld zu ermöglichen,[221]
- bei IKT-Ausschreibungen im öffentlichen Bereich nur mit zertifizierten Unternehmen arbeiten und mit diesem Verhalten eine Vorbildfunktion übernehmen.[222]

Bei der Diskussion möglicher staatlicher Unterstützungsleistungen ist allerdings ein Grundsatzaspekt zu beachten: Tritt der Staat im Bereich des Risiko- und Krisenmanagements zu cyberrelevanten Themen als Dienstleister auf, steht er in einem potenziellen Konkurrenzverhältnis zu Anbietern aus der Privatwirtschaft.[223] Es ist zu fragen, ob dieses Konkurrenzverhältnis ordnungspolitisch erwünscht ist und staatliche Stellen über ausreichende Expertise verfügen, um gewisse Dienste überhaupt erbringen zu können. Es empfiehlt sich daher, Wünschbarkeit und Machbarkeit staatlicher Sicherheitsleistungen sehr genau zwischen allen Beteiligten zu diskutieren. Ein Ansatz könnte darin liegen, dass sich die staatliche Unterstützung auf Leistungen bezieht, für die bewusst eine produkt- und herstellerunabhängige Expertise erforderlich ist oder die Akzeptanz für privatwirtschaftliche Leistungen nur beschränkt vorhanden ist (z.B. staatliches Audit für Mindestsicherheitsstandards).[224]

Übungen

Übungen und Planspiele stellen aus Sicht der Gesprächspartner ein geeignetes Mittel dar, um vorhandene Konzepte, Instrumente und Strukturen zu überprüfen. In der Energiewirtschaft, im Finanzsektor und im Behördenumfeld zählen Übungen bereits heute zum Standardrepertoire der Sicherheitsvorsorge. Übungen und Planspiele sollten in der künftigen österreichischen Cybersicherheitsstrategie eine prominente Rolle spielen. Neben dem Training sektorspezifischer Verhaltensweisen bei Ereignissen im und aus dem Cyberspace sollte der sektorübergreifenden sowie der öffentlich-privaten Zusammenarbeit besondere Aufmerksamkeit geschenkt werden. Übungen und Planspiele können aber nur dann sinnvoll eingesetzt werden, wenn die Akteure ein gemeinsames Verständnis darüber erzielen, welche Schutzziele im Kontext der Cybersicherheit angestrebt werden und welche Partner hierfür welche Beiträge erbringen sollen. Zieldefinition, Risikoanalyse, Überprüfung der Tauglichkeit bestehender Sicherheitsvorkehrungen sowie Übungen und Planspiele müssen daher systematisch aufeinander abgestimmt werden.

206 Interview, 13. Februar 2012.
207 Interview, 23. April 2012.
208 Interviews, 24. April 2012.
209 Gefordert wurde auch, der Staat solle verbindlich vorschreiben, welche Aspekte Gegenstand von Sicherheitsaudits bei Unternehmen in strategisch relevanten Infrastruktursektoren sein sollen. Interview, 4. April 2012.
210 Interviews, 4., 13. und 23. April 2012.
211 Dieser Mechanismus greift heute bereits im Bereich der Gaswirtschaft. Unternehmensverantwortliche werden nur dann aus ihrer strafrechtlichen Haftung entlassen, wenn sie nachweisen können, dass zum Zeitpunkt eines Zwischenfalls alle maßgeblichen Sicherheitsstandards eingehalten wurden. Hinweis eines Vertreters der Energiewirtschaft im Rahmen der Diskussion der Ergebnisse der vorliegenden Studie am 2. Mai 2012 in Wien.
212 Interview, 15. Februar 2012.
213 Interview, 28. Februar 2012
214 Interview, 8. Februar 2012, 17. April 2012. Ein Gesprächspartner deutete an, dass das Vertrauen in einen staatlichen Prüfer sogar größer sein sollte als bei den bisherigen Prüfern aus der Privatwirtschaft. Interview, 24. April 2012.
215 Interviews, 13. und 22. Februar 2012.
216 Interview, 8. Februar 2012.
217 Interview, 4. April 2012.
218 Interview, 17. April 2012
219 Interview, 16. April 2012.
220 Die US-Regierung hat mit dem Cyber Fast Track-Programm eine solche Grundlage geschaffen. Siehe: Nakashima, „Pentagon to fast-track cyberweapons acquisition“.
221 Interview, 20. März 2012.
222 Interview, 23. April 2012.
223 Interview, 18. April 2012
224 Interview, 17. April 2012.

ANHANG

© Jacob Wackerhausen – iStockphoto.com

9.1. Abbildungs- und Tabellenverzeichnis
9.2. Interviewpartner
9.3. Literatur
9.4. Glossar
9.5. Autorenhinweise

9

Abbildungs- und Tabellenverzeichnis

9.1.

Abbildung 1: Risikomanagement nach ISO 31000 17
Abbildung 2: KSÖ-Cyberrisikomatrix 18
Abbildung 3: Interviewpartner nach Sektoren 20
Abbildung 4: Cyberrisiken aus Sicht der Interviewpartner (Gesamtübersicht) 22
Abbildung 5: Top-15-Cyberrisiken aus Sicht der Interviewpartner (differenziert nach Sektoren) 24
Abbildung 6: Relevanz der Stromversorgung für die Gesellschaft 31
Abbildung 7: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Energiesektors 35
Abbildung 8: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Finanzsektors 46
Abbildung 9: IKT-Wertschöpfungskette 54
Abbildung 10: Top-15-Cyberrisiken aus Sicht der Interviewpartner des IKT-Sektors 59
Abbildung 11: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Transportsektors 70
Abbildung 12: Top-15-Cyberrisiken aus Sicht der Interviewpartner des Behördensektors 81
Abbildung 13: Beispiele aktueller Maßnahmen zur Stärkung der Cyberrisikoprävention in Österreich 99
Tabelle 1: Merkmale intentionaler Cyberrisiken 26

9.2. Interviewpartner

Den Interviewpartnern, die an der Erstellung der vorliegenden Risikobewertung teilgenommen haben, wurde Anonymität zugesichert. Daher werden an dieser Stelle nur die jeweiligen Institutionen in alphabetischer Reihenfolge angeführt.

A1 Telekom
Austrian Power Grid
Austro Control
Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG)
Bundesministerium für Inneres (BM.I)
Bundesministerium für Landesverteidigung und Sport (BMLVS)
Bundesrechenzentrum (BRZ)
Cisco Systems Austria GmbH
Cyber Security Austria (CSA)
Energie AG Oberösterreich
Energie-Control Austria (e-control)
Erste Group Bank AG
Flughafen Wien AG
Geldservice Austria (GSA)
Hutchison 3G Austria GmbH
IBM – Österreich
Land Niederösterreich
Magistratsdirektion der Stadt Wien
Microsoft Österreich
Oesterreichische Nationalbank
ÖBB Infrastruktur AG
OMV AG
ORF
Post AG
Raiffeisenlandesbank Niederösterreich-Wien AG
Rundfunk & Telekom Regulierungs-GmbH (RTR)
SIX Card Solutions Austria
Spar Österreich
T-Systems Österreich
Verbund AG
Wiener Stadtwerke Holding AG

© René Mansi – iStockphoto.com

9.3. Literatur

- „28C3: Hacker nehmen Eisenbahnsicherungen unter die Lupe“, Heise online, 30. Dezember 2011, <http://www.heise.de/newsticker/meldung/28C3-Hacker-nehmen-Eisenbahnsicherungen-unter-die-Lupe-1401949.html> (Zugriff: 10. April 2012).
- „Angriffe auf E-Mailkonten chinesischer Aktivisten“, golem.de, 2. Juni 2011, < http://www.golem.de/1106/83923.html > (Zugriff: 12. April 2012).
- „Bahrains’ Gulf Air Facebook page ‚hacked‘“, BBC, 9 April 2012, <http://www.bbc.co.uk/news/world-middle-east-17657775> (Zugriff: 10. April 2012).
- „Cloud Computing: ‚Wolke‘ mit Lücken. Massive Sicherheitsmängel bei Amazon Webservices entdeckt und behoben“, Presseinformation Nr. 336, Ruhr Universität Bochum, 24. Oktober 2011, < http://aktuell.ruhr-uni-bochum.de/pm2011/pm00336.html.de> (Zugriff: 12. April 2012).
- „Cyber-Attacken: US-Großbanken schmieden Allianz gegen Hacker“, Spiegel Online, 10. Januar 2012, <http://www.spiegel.de/wirtschaft/unternehmen/0,1518,808132,00.html> (Zugriff: 3. April 2012).
- „Das Smartphone als Verkaufsplattform. Mobile Anwendungen bieten viele Chancen für Unternehmen – vorausgesetzt, sie verstehen den Markt“, Neue Zürcher Zeitung, 24. November 2011, S. 35.
- „Datendiebstahl bei Emissionshändlern“, Euractiv, 3. Februar 2010, <http://www.euractiv.de/energie-und-klimaschutz/artikel/datendiebstahl-bei-emissionshandlern-002683> (Zugriff: 5. April 2012).
- „Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware“, Department of Justice, Press Release, 6 May 2010, < Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in

Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware > (Zugriff: 12. April 2012).
- „DigiNotar-Hack: Kritische Infrastruktur war unzureichend geschützt“, heise online, 6. September 2011, <http://www.heise.de/security/meldung/DigiNotar-Hack-Kritische-Infrastruktur-war-unzureichend-geschuetzt-1337378.html> (Zugriff: 3. April 2012).
- „EU-Emissionshandel nach Hacker-Angriff gestoppt“, Euractiv, 20. Januar 2011, <http://www.euractiv.de/222/artikel/eu-emissionshandel-nach-hacker-angriff-gestoppt-004245> (Zugriff: 5. April 2012).
- „Ex-employee of Airport Transportation Company Arrested for Allegedly Hacking Into Computer, Destroying Data“, Press Release, U.S. Department of Justice, 20 February 2003, <http://www.justice.gov/criminal/cybercrime/press-releases/2003/tranArrest.htm> (Zugriff: 10 April 2012).
- „France: cyber-attaque contre le ministère des Finances“, AFP, 3. März 2011, <http://archives.24heures.ch/france-attaque-informatique-spectaculaire-visant-ministere-finances-2011-03-07> (Zugriff: 9. April 2012).
- „Google wirft China die Störung von Google Mail vor“, golem.de, 21. März 2011, <http://www.golem.de/1103/82214.html> (Zugriff: 12. April 2012).
- „Group jailed after hacking online system“, Global Times, 8 April 2012, <http://www.globaltimes.cn/NEWS/tabid/99/ID/703805/Group-jailed-after-hacking-online-system.aspx> (Zugriff: 10. April 2012).
- „Hacker’s trial behind closed door“, Intelligence Online, 18. November 2010, S. 5.
- „Hackerangriff auf EU-Kommission“, Euractiv.de, 24. März 2011, <http://www.euractiv.de/digitale-agenda/artikel/hackerangriff-auf-eu-kommission-004560> (Zugriff: 9. April 2012).
- „How Conficker Virus felled the Military“, Intelligence Online, 5. Februar 2009, S. 1.
- „Hunderte Bundeswehr-Rechner von Conficker befallen“, heise online, 14. Februar 2009, <http://www.heise.de/security/meldung/Hunderte-Bundeswehr-Rechner-von-Conficker-befallen-195953.html> (Zugriff: 9. April 2012).
- „India’s Railway Email System hacked by Pakistan Cyber Army“, The Hacker News, 24 April 2011, <http://thehackernews.com/2011/04/indias-railway-email-system-hacked-by.html> (Zugriff: 10. April 2012).
- „MasterCard, VISA Warn on Processor Breach“, Krebs on Security, 30. März 2012, <http://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/> (Zugriff: 3. April 2012).
- „Micro-Blog Twitter gehackt“, heise online, 6. Januar 2009, <http://www.heise.de/security/meldung/Micro-Blog-Twitter-gehackt-Update-193709.html> (Zugriff: 12. April 2012).
- „MoD probes virus security breach“, BBC News, 20. Januar 2009, <http://news.bbc.co.uk/2/hi/uk_news/7839034.stm> (Zugriff: 9. April 2012).
- „Neue Sicherheitsstandards für den Emissionshandel. Mehrfachkontrollen ähnlich wie für Bankgeschäfte im Internet“, Frankfurter Allgemeine Zeitung, 27. Januar 2011, S. 10.
- „Nortel hit by suspected Chinese cyberattack for a decade“, CBS News, 14 February 2012, <http://www.cbc.ca/news/business/story/2012/02/14/nortel-chinese-hackers.html> (Zugriff: 12. April 2012).
- „Sources: Staged cyber attack reveals vulnerability in power grid“, CNN, 26. September 2007, <http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US> (Zugriff: 5. April 2012).
- „Summary of the Amazon EC2 and Amazon RDS Service Disruption“, Amazon Web Services, <http://aws.amazon.com/de/message/65648/> (Zugriff: 12. April 2012).
- „Telefonanlagen gehackt: Mehrere tausend Euro Schaden“, Teltarif, 4. Juli 2011, <http://www.teltarif.de/telefonanlage-hack-rechnung-betrug-gespraeche/news/43227.html> (Zugriff: 12. April 2012).
- „Telekom lockt Hacker zu Life-Angriffen auf Smartphone“, VDI-Nachrichten, 30. März 2012, <http://www.vdi-nachrichten.com/artikel/Telekom-lockt-Hacker-zu-Live-Angriffen-auf-Smartphones/58043/2> (Zugriff: 12. April 2012).
- „Visa: Regelmäßiges Wiegen der Kartenterminals schützt vor Manipulationen“, heise online, 9. Juli 2010, <http://www.heise.de/security/meldung/Visa-Regelmaessiges-Wiegen-der-Kartenterminals-schuetzt-vor-Manipulationen-1035169.html?view=print> (Zugriff: 3. April 2012).
- 2011 Norton Cybercrime Report, <http://www.symantec.com/content/en/us/

- home_homeoffice/html/cybercrimereport/> (Zugriff: 6. April 2012).
- 2012 Data Breach Investigations Report (New York: Verizon, 2012), <http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf> (Zugriff: 3. April 2012).
- Alperovitch, Dmitri, Revealed: Operation Shady RAT (Santa Clara: McAfee, 2011), <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> (Zugriff: 9. April 2012).
- Analysis of Cyber Security Aspects in the Maritime Sector (Heraklion: ENISA, 2011), <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1> (Zugriff: 10. April 2012).
- Arthur, Charles, „DigitNotar SSL certificate hack amounts to cyberwar, says expert“, The Guardian, 5 September 2011, <http://www.guardian.co.uk/technology/2011/sep/05/diginotar-certificate-hack-cyberwar> (Zugriff: 12. April 2012).
- Averill, Bruce and Eric A.M. Luiijf, „Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention“, Journal of Energy Security, 18. Mai 2010, <http://www.ensec.org/index.php?option=com_content&view=section&layout=blog&id=27&Itemid=361> (Zugriff: 5. April 2012).
- Banking Trojans (Mountain View: Symantec, 2011), <https://www4.symantec.com/mktginfo/whitepaper/user_authentication/21195180_WP_GA_BankingTrojansImpactandDefendAgainstTrojanFraud_062611.pdf> (Zugriff: 3. April 2012).
- Barnett, James Arden, „Cybersecurity: Threats to Communications Networks and Public-Sector Responses“, Testimony before the Subcommittee on Communications, Technology and the Internet, Committee on Energy and Commerce, U.S. House of Representatives, 28 March 2012, <http://Republicans.EnergyCommerce.house.gov/Media/file/Hearings/Telecom/20120328/HHRG-112-IF16-WstateJBarnett-20120328.pdf > (Zugriff: 12. April 2012).
- Barrett, Devlin, „Hackers Penetrate Nasdaq Computers“, The Wall Street Journal, 5. Februar 2011, <http://online.wsj.com/article/
- SB10001424052748704709304576124502351634690.html> (Zugriff: 3. April 2012).
- Bobi, Emil, „Gefährdetes Österreich. Eine ‚Risikomatrix‘ des Bundesheers zeichnet neue Bedrohungsszenarien auf“, Profil, 14. Juni 2011, <http://www.profil.at/articles/1124/560/299365/bundesheer-gefaehrdetes-oesterreich> (Zugriff: 6. April 2012).
- Borchert, Heiko, Cybersicherheit intelligent regulieren. Warum, wie und durch wen? Grundsatzüberlegungen im Spannungsfeld zwischen staatlichen Vorgaben, privatwirtschaftlicher Selbstverpflichtung und individuellen Grundrechten (Wien: Kuratorium Sicheres Österreich, 2012).
- Bowen, Brian M., Salvatore J. Stolfo, and Ramaswamy Devarajan, „Measuring the Human Factor of Cyber Security“, Homeland Security Affairs, IEEE 2011 Conference on Technology for Homeland Security: Pest Papers (May 2012), <http://www.hsaj.org/?article=supplement5.2> (Zugriff: 23. Mai 2012).
- Boyens, Jon et. al., Notional Supply Chain Risk Management Practices for Federal Information Systems. Draft NISTIR 7622 (Washington, D.C.: National Institute of Standards and Technology, 2012), < http://csrc.nist.gov/publications/drafts/nistir-7622/second-public-draft_nistir-7622.pdf > (Zugriff: 9. April 2012).
- Breuss, Daniel und Erich Kocina, „Anonymous veröffentlicht Daten von 25.000 Polizisten“, DiePresse.com, 26. September 2011, <http://diepresse.com/home/techscience/internet/sicherheit/695982/Anonymous-veroeffentlicht-Daten-von-25000-Polizisten> (Zugriff: 12. April 2012).
- Bronk, Christopher, Cody Monk and John Villasenor, „The Dark Side of Cyber Finance“, Survival, 54:2 (April–Mai 2012), S. 129–142.
- Cebula, James J. and Lisa R. Young, A Taxonomy of Operational Cyber Security Risks (Hanscom: Software Engineering Institute, 2011).
- Cisco Visual Networking Index: Forecast and Methodology, 2010–2015 (San Jose: Cisco, 2011), <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf> (Zugriff: 12. April 2012).
- Common Cybersecurity Vulnerabilities in In-

dustrial Control Systems (Washington, D.C.: Department of Homeland Security, 2011), <http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf> (Zugriff: 5. April 2012).
- Cybersecurity of Freight Information Systems. A Scoping Study (Washington, D.C.: Transportation Research Board, 2003), <http://www.nap.edu/catalog.php?record_id=10730> (Zugriff: 10. April 2012).
- Das Personal des Bundes 2011. Daten und Fakten (Wien: Bundeskanzleramt, 2011), <http://www.bka.gv.at/DocView.axd?CobId=40688> (Zugriff: 3. April 2012).
- Dinning, Michael G. „Introduction to Cyber Security Issues for Transportation“, Webinar Presentation, 7 December 2011, <http://www.pcb.its.dot.gov/t3/s111207/s111207_dinning_overview.pdf> (Zugriff: 10. April 2012).
- Durden, Tyler, „SkyNet Wars: How a Nasdaq Algo Destroyed BATS“, Zero Hedge, 27. März 2012, <http://www.zerohedge.com/news/skynet-wars-how-nasdaq-algo-destroyed-bats> (Zugriff: 3. April 2012).
- Emmerson, Bob, „M2M: the Internet of 50 billion devices“, Win-Win, January 2010, S. 19–22.
- Energy, transport and environment indicators (Luxemburg: Publications Office of the European Union 2011), <http://www.eds-destatis.de/downloads/publ/KS-DK-11-001-EN-N.pdf> (Zugriff: 3. April 2012).
- Europe's Digital Competitiveness Report 2010 (Luxembourg: Publications Office of the European Union, 2010), <http://ec.europa.eu/information_society/digital-agenda/documents/edcr.pdf> (Zugriff: 3. April 2012).
- Falliere, Nicolas, W32.Quakbot in Detail (Mountain View: Symantec, 2011), <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf> (Zugriff: 3. April 2012).
- Finkle, Jim, „Symantec Hack: Company Admits Hackers Stole Norton Source Code in 2006“, Huff Post, 17 January 2012, <http://www.huffingtonpost.com/2012/01/17/symantec-hack-norton-source-code_n_1211043.html> (Zugriff: 12. April 2012).
- Fischer, Uwe Christian, „Sicherheitspartnerschaft zwischen Staat und Wirtschaft: Anforderungen an die Sicherheitszusammenarbeit mit der Wirtschaft“, in Heiko Borchert (Hrsg.), Wettbewerbsfaktor Sicherheit. Staat und Wirtschaft im Grand Pas de Deux für Sicherheit und Prosperität (Baden-Baden: Nomos, 2008), S. 27–46.
- Gassmann, Michael, „Angriff auf den Emissionshandel. Hacker plündern europäische Register“, Financial Times Deutschland, 3. Februar 2010, S. 1.
- Gefahren durch Wirtschafts- und Industriespionage für die österreichische Wirtschaft (Wien: Bundesministerium für Inneres/Industriellenvereinigung/Wirtschaftskammer/FH Campus Wien, 2010), <www.fh-campuswien.ac.at/index.php?download=3067.pdf> (Zugriff: 7. Mai 2012).
- Global Energy Cyberattacks: Night Dragon (McAfee: Santa Clara, 2011), <http://www.mcafee.com/au/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf> (Zugriff: 5. April 2012).
- Gorman, Siobhan, „Electricity Grid in U.S. Penetrated by Spies“, Wall Street Journal, 8. April 2009, <http://online.wsj.com/article/SB123914805204099085.html> (Zugriff: 5. April 2012).
- Gorman, Siobhan, „FAA's Air-Traffic Networks Breached by Hakers“, The Wall Street Journal, 7 May 2009, <http://online.wsj.com/article/SB124165272826193727.html> (Zugriff: 10. April 2012).
- Gostev, Alexander, „Kasperksy Security Bulletin 2011/2012. Entwicklung der IT-Bedrohungen im Jahr 2011 und Ausblick auf das Jahr 2012“, <http://www.viruslist.com/de/analysis?pubid=200883772> (Zugriff: 3. April 2012).
- Gottwald, Robert, Österreichische Bundesverwaltung: Erhebung der organisatorischen Verankerung der Informationssicherheitsmanagement-Zuständigkeit. Master Thesis im Rahmen des Unversitätslehrgangs Information Security Management (Krems: Donau Universität Krems, 2011).
- H.R. 2096 Cybersecurity Enhancement Act of 2011, 6. Februar 2011, <http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.2096:> (Zugriff: 11. April 2012).
- H.R. 76 Cybersecurity Education Enhancement Act of 2011, 5. Januar 2011, <http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.76: > (Zugriff: 11. April 2012).

- Hadnagy, Christopher, Social Engineering: The Art of Human Hacking (Indianapolis, Wiley Publishing, 2011).
- Henkel, Christiane Hanna, „Computerfehler steckt hinter blamablem Bats-Debüt. Alternative Handelsplattformen steigen dennoch unaufhaltsam auf“, Neue Zürcher Zeitung, 27. März 2012, S. 31.
- High Performance Microchip Supply. Report of the Defense Science Board Task Force (Washington, D.C.: Department of Defense, 2005), <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf> (Zugriff: 9. April 2012).
- High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. A Jointly Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop (Washington, D.C.: NERC, 2010), <http://www.nerc.com/files/HILF.pdf> (Zugriff: 5. April 2012).
- IABG, Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure. Report on behalf of the European Commission DG Justice, Freedom and Security (Berlin: IABG, 2009).
- ICT Continuity. Handlungsempfehlungen zur Sicherstellung der Versorgung (Aarau: Verband Schweizerischer Elektrizitätsunternehmen, 2011).
- IKT Made in Austria (Wien: FEEI – Fachverband der Elektro- und Elektronikindustrie, 2011), <http://www.feei.at/schwerpunktthemen/ikt_made_in_austria/> (Zugriff: 3. April 2012).
- Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht 2009/2 (Bern: Melde- und Analysestelle Informationssicherung, 2010).
- Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht 2011/1 (Bern: Melde- und Analysestelle Informationssicherung, 2011), <http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de> (Zugriff: 3. April 2012).
- ISO/IEC 17799 Information technology – Code of practice for information security management (Geneva: ISO, 2000).
- Koscher, Karl et. al., „Comprehensive Experimental Analysis of a Modern Automobile“, Proceedings of the 31st IEEE Symposium on Security and Privacy, 16–19 May 2010, <http://www.autosec.org/pubs/cars-oakland2010.pdf> (Zugriff: 10. April 2012).
- Krekel, Bryan, Pattoon Adams, and George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S. China Economic and Security Review Commission by Northrop Grumman (Washington, D.C.: U.S.-China Economic and Security Review Commission, 2012), <http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf> (Zugriff: 9. April 2012).
- Kuhl, Jackson, „How to Hack Into a Boeing 787“, FoxNews, 20 February 2008, <http://www.foxnews.com/story/0,2933,331088,00.html> (Zugriff: 10. April 2012).
- Lahrtz, Stephanie, „Rasantes Wachstum des Flughafens München. Non-Aviation liefert bereits mehr Umsatz als Flugzeuge“, NZZ, 19. Februar 2008, S. B1.
- Layton, Joshua, „Hacktivists Anonymous claim to have taken down Home Office website“, The Guardian, 7. April 2012, <http://www.guardian.co.uk/technology/2012/apr/07/anonymous-home-office-website> (Zugriff: 9. April 2012).
- Majumdar, Dave, „Iran's Captured RQ-170: How Bad Is the Damage?“, Defense News, 12. Dezember 2011, S. 4.
- Mapping the Mal Web. The World's Riskiest Domains (Santa Clara: McAfee, 2010), <http://us.mcafee.com/en-us/local/docs/MTMW_Report.pdf> (Zugriff: 6. April 2012).
- Marks, Paul, „Air traffic system vulnerable to cyber attack“, New Scientist, 12 September 2011, <http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html> (Zugriff: 10. April 2012).
- Martin, Paul K., „NASA Cybersecurity: An Examination of the Agency's Information Security“, Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space and Technology, 29. Februar 2012, <http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf > (Zugriff: 9. April 2012).
- Masterplan Österreichisches Programm

zum Schutz Kritischer Infrastruktur (APCIP) (Wien: Bundeskanzleramt, 2008).
- Mission Impact of Foreign Influence on DoD Software. Report of the Defense Science Board Task Force (Washington, D.C.: Department of Defense, 2007), < http://www.acq.osd.mil/dsb/reports/ADA486949.pdf > (Zugriff: 9. April 2012).
- Nakashima, Ellen, „Cyber intruder sparks massive federal response – and debate over dealing with threats“, The Washington Post, 9. Dezember 2011, <http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html> (Zugriff: 9. April 2012).
- Nakashima, Ellen, „Pentagon to fast-track cyberweapons acquisition“, The Washington Post, 9. April 2012, <http://www.washingtonpost.com/world/national-security/2012/04/09/gIQAuwb76S_story.html> (Zugriff: 14. April 2012).
- Nazario, Jose, „Politically Motivated Denial of Service Attacks“, Paper for the 2009 CCDCOE Conference on Cyber Warfare, Tallinn, 16-19 June 2009, <http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf> (Zugriff: 9. April 2012).
- Nerlich, Uwe and Frank Umbach, „European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat“, Journal of Energy Security, 27. Oktober 2009, <http://www.ensec.org/index.php?option=com_content&view=section&layout=blog&id=24&Itemid=352> (Zugriff: 5. April 2012).
- Netzentwicklungsplan 2011. Regelzone Austrian Power Grid AG – Planungszeitraum 2012–2021 (Wien: APG, 2012).
- OECD Communications Outlook 2011 (Paris: OECD, 2011).
- Öhlböck, Johannes und Balazs Esztegar, „Rechtliche Qualifikation von Denial of Services Attacken“, Journal für Strafrecht, 4/2011, S. 126–133, <http://www.raoe.at/uploads/media/JSt-4-2010_126-DDoS-Attacken.PDF> (Zugriff: 12. April 2012).
- ÖNORM ISO 31000. Risikomanagement: Grundsätze und Richtlinien (Wien: Österreichisches Normungsinstitut, 2010).
- Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten (Wien: Bundeskanzleramt, 2011), <http://www.bka.gv.at/site/3503/default.aspx> (Zugriff: 6. April 2012).
- Palmer, Jason, „Sat-nav systems under growing threat from ‚jammers'“, BBC, 23 February 2010, <http://news.bbc.co.uk/2/hi/science/nature/8533157.stm> (Zugriff: 10. April 2012).
- Reichhardt, Andreas und Georg Serentschy, „Der IKT-Masterplan“, Pressegespräch zur Präsentation des IKT-Masterplans, Wien, 9. November 2005, <http://www.rtr.at/de/pr/PInfo09112005TK/IKT_Masterplan_GeS.pdf> (Zugriff: 12. April 2012).
- Regierungsprogramm 2008–2013. Gemeinsam für Österreich (Wien: Bundeskanzleramt, 2008), <http://www.austria.gv.at/DocView.axd?CobId=32965> (Zugriff: 6. April 2012).
- Reißmann, Ole und Konrad Lischka, „Blackberry-Ausfall: Die Cloud-Katastrophe“, Spiegel Online, 14. Oktober 2011, <http://www.spiegel.de/netzwelt/web/0,1518,791624,00.html> (Zugriff: 12. April 2012).
- Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems (Washington, D.C.: Office of Inspector General, U.S. Department of Transportation, 2009), <http://www.oig.dot.gov/sites/dot/files/pdfdocs/ATC_Web_Report.pdf> (Zugriff: 10. April 2012).
- Richmond, Riva, „The RSA Hack: How They Did It“, Bits – New York Times Blog, 2 April 2011, <http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/> (Zugriff: 12. April 2012).
- Rief, Norbert, „Chinesen hacken Österreichs Außenministerium“, Die Presse, 1. Oktober 2010, <http://diepresse.com/home/techscience/internet/sicherheit/598953/Chinesen-hacken-Oesterreichs-Aussenministerium> (Zugriff: 9. April 2012).
- Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen (Berlin: Zukunftsforum öffentliche Sicherheit, 2008), <http://www.zukunftsforum-oeffentliche-sicherheit.de/downloads/Gruenbuch_Zukunftsforum.pdf> (Zugriff: 5. April 2012).
- Roadmap to Achieve Energy Delivery Systems Cybersecurity (Washington, D.C.: Energy Sector Control Systems Working Group, 2011), <http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf> (Zugriff: 5. April 2012).

- Rotenberg, Marc, „Cybersecurity: Threats to the Financial Sector“, Testimony before the United States House of Representatives, Committee on financial Services, Subcommittee on Financial Institutions and Consumer Credit, Washington, D.C., 14 September 2011.
- Sandawi, Sammi, „Cyber Weapons 2.0. Soziale Medien als Plattform von Desinformationskampagnen“, Public Security, 1/2011, S. 18–19.
- Schneier, Bruce, „Why being open about security makes us all safer in the long run“, The Guardian, 7 August 2008, <http://www.guardian.co.uk/technology/2008/aug/07/hacking.security> (Zugriff: 10. April 2012).
- Shannon, Gregory E., „Cybersecurity: Threats to the Financial Sector“, Testimony before the United States House of Representatives, Committee on financial Services, Subcommittee on Financial Institutions and Consumer Credit, Washington, D.C., 14 September 2011.
- Sicherheitsreport 2011. Eine repräsentative Studie zum Thema Sicherheit in Deutschland im Auftrag von T-Systems (Berlin: Deutsche Telekom/T-Systems, 2011), <http://www.t-systems.de/tsip/de/642064/startseite/uebertsystems/news/details/2011-09-19-sicherheitsreport> (Zugriff: 6. April 2012).
- Snow, Gordon, „Cybersecurity: Threats to the Financial Sector“, Testimony before the United States House of Representatives, Committee on financial Services, Subcommittee on Financial Institutions and Consumer Credit, Washington, D.C., 14 September 2011.
- Sreenivasan, Hari, „Gawker Data Breach Could Lead to Attacks on Government“, PBS, 12 Dezember 2010, <http://www.pbs.org/newshour/rundown/2010/12/gawker-data-breach-could-lead-to-attacks-on-government-agencies.html> (Zugriff: 12. April 2012).
- State of IT Security. Study of Utilities & Energy Companies (Traverse City: Ponemon Institute, 2011).
- Statistik Austria, Jahrbuch 2012 (Wien: Statistik Austria, 2012).
- Statistik Straße & Verkehr (Wien: Bundesministerium für Verkehr, Innovation und Technologie, 2012), <http://www.bmvit.gv.at/service/publikationen/verkehr/strasse/downloads/statistik_strasseverkehr2012.pdf> (Zugriff: 3. April 2012).
- Sternstein, Aliya, „Hackers manipulated railway computers, TSA memo says“, Nextgov, 23 January 2012, <http://www.nextgov.com/nextgov/ng_20120123_3491.php> (Zugriff: 10. April 2012).
- Stewart, Phil, Diane Bartz, Jim Wolf, and Jeff Mason, „Special report: Government in cyber fight but can’t keep up“, Reuters, 16. Juni 2011, <http://www.reuters.com/article/2011/06/16/us-usa-cybersecurity-idUSTRE75F4YG20110616> (Zugriff: 9. April 2012).
- Streissler, Agnes, Bedeutung der Banken für die österreichische Volkswirtschaft. Erstellt für die GF Bundessparte Bank und Versicherung (Wien: Agnes Streissler Wirtschaftspolitische Projektberatung, 2010), <https://www.voebb.at/showInfoDatei.jsp?file_id=101> (Zugriff: 2. April 2012).
- Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector. Report on behalf of the European Commission DG Justice, Freedom and Security (Oxfordshire: AEA, 2009), <http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf> (Zugriff: 5. April 2012).
- The Safety Promise and Challenge of Automotive Electronics. Insights form Unintended Acceleration (Washington, D.C.: Transportation Research Board, 2012), <http://www.nap.edu/catalog.php?record_id=13342> (Zugriff: 10. April 2012).
- Tibken, Shara and Steven Russolillo, „Amazon Glitch Hobbles Websites“, The Wall Street Journal, 22 April 2011, <http://online.wsj.com/article/SB10001424052748703983704576277000970161740.html> (Zugriff: 12. April 2012).
- Tillett, Brian, „Cybersecurity: Threats to the Financial Sector“, Testimony before the United States House of Representatives, Committee on financial Services, Subcommittee on Financial Institutions and Consumer Credit, Washington, D.C., 14 September 2011.
- Top 50 Bad Hosts and Networks. 4th Quarter 2011 – Report (o.O.: Host Exploit, 2012), <http://hostexploit.com/blog/14-reports/3536-cybercrime-friendly-hosts-or-industry-victims.html> (Zugriff: 6. April 2012).
- Top Management Challenges for Fiscal Year 2012. (Washington, D.C.: Office of In-

© Chad McDermott – iStockphoto.com

spector General, U.S. Department of Transportation, 2011), <http://www.oig.dot.gov/sites/dot/files/DOT%20Top%20Management%20Challenges%20for%20FY%202012.pdf> (Zugriff: 10. April 2012).

- Totzke, Scott, „Cybersecurity: Threats to Communications Networks and Public-Sector Responses“, Testimony before the Subcommittee on Communications, Technology and the Internet, Committee on Energy and Commerce, U.S. House of Representatives, 28 March 2012, <http://republicans.energycommerce.house.gov/Media/file/Hearings/Telecom/20120307/HHRG-112-IF16-Wstate-STotzke-20120307.pdf> (Zugriff: 12. April 2012).
- Transportation & Logistics 2030: Securing the supply chain (Düsseldorf: PwC and Supply Chain Management Institute, 2011), <http://www.pwc.com/gx/en/transportation-logistics/publications/security-transport-systems.jhtml> (Zugriff: 10. April 2012).
- Ungerleider, Neal, „The Dark Side of Biometrics: 9 Million Israelis' Hacked info Hits the Web“, Fastcompany.com, 24 October 2011, <http://www.fastcompany.com/1790444/the-downside-of-biometrics-9-million-israelis-records-hacked> (Zugriff: 9. April 2012).
- Verfassungsschutzbericht 2010 (Berlin: Bundesministerium des Innern), <http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2010/> (Zugriff: 9. April 2012).
- Verfassungsschutzbericht 2011 (Wien: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, 2011), <http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/BVT_VSB_2011_online.pdf> (Zugriff: 6. April 2012).
- Vijayan, Jaikumar, „Anonymous claims release of BART police officers' data“, Computerworld, 17 August 2011, <http://www.computerworld.com/s/article/9219285/Anonymous_claims_release_of_BART_police_officers_data> (Zugriff: 10. April 2012).
- Weston, Greg, „Foreign hackers attack Canadian government“, CBS News, 16. Februar 2011, <http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html> (Zugriff: 9. April 2012).
- Wilshusen, Gregory C., „Cybersecurity: Threats Impacting the Nation“, Testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, Washington, D.C., 24 April 2012.
- Wolf, Jim and William Maclean, „IMF cyber attack aimed to steal insider information: expert“, Reuters, 12. Juni 2011, <http://www.reuters.com/article/2011/06/12/us-imf-cyberattack-idUSTRE75A20720110612> (Zugriff: 9. April 2012).
- Zetter, Kim, „Hackers Breached Railway Network, Disrupted Service“, Wired Danger Room, 24 January 2012, <http://www.wired.com/threatlevel/2012/01/railway-hack/> (Zugriff: 10. April 2012).

© Dominik Pabis – iStockphoto.com

9.4. Glossar

Bösartige Software

Programme, die schadhafte Funktionen ausführen (Viren, Trojaner, Malware, Würmer). Dieser Schadcode kann Systeme, Netzwerke, Anwendungen oder einzelne Dateien unbrauchbar machen, sich eigenständig auf andere Netzwerke verbreiten und zu ungewünschten Aktivitäten verleiten. In SCADA-Umgebungen kann Malware die gesamte Steuerungs- und Regelfähigkeit von Industrieanlagen aufheben oder Fernzugriffe einrichten.

Cybercrime

Jede Form von Straftaten, die mit Hilfe von Informationstechnologien und Kommunikationsnetzen begangen werden. Auch die Internetkriminalität zählt dazu.

Cybersicherheit

Cybersicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit geeigneten rechtsstaatlichen Mitteln vor akteursbezogenen, technischen und naturbedingten Gefahren, die die Sicherheit des Cyberspace (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyberspace gefährden, in einem vernetzten und partnerschaftlichen Ansatz, der die relevanten staatlichen bzw. nicht-staatlichen Akteure einbezieht und damit dazu beiträgt, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.

Cyberspace
Raum, der durch die weltumspannende Nutzung der Informations- und Kommunikationstechnologie (KT) sowie die darüber transportierten Daten entsteht.

Cyberspionage
Spionage auf digitalem Weg, um Informationen aus elektronischen Datenbanken staatlicher Behörden und wissenschaftlicher Institute zu gewinnen, aufzuklären, wie diese miteinander kommunizieren, oder Innenansichten über die Position eines Staates zu Sachfragen zu gewinnen.

Cyberspionage gegen Industrie
Spionage auf digitalem Weg gegen Unternehmen, die damit Werte, Know-how und Ansehen oder durch Erpressung die Existenz verlieren können.

Cyberterrorismus
Dabei handelt es sich um organisierte Cybersabotage/-angriffe, die von politisch-fundamentalistischen bzw. terroristischen Gruppen oder Einzeltätern organisiert werden und sich gegen Staaten, Organisationen oder Unternehmen richten.

Cyberwar
Meint die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. In einem weiteren Sinne ist damit auch die Unterstützung militärischer Aktionen in den klassischen Operationsräumen Boden, See, Luft, Weltraum durch Maßnahmen aus dem virtuellen Raum angesprochen. Ganz allgemein sind damit auch die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischen Bereiche und Belange basieren.

Datendiebstahl und Manipulation von Bürgerdaten
Die öffentliche Verwaltung benötigt digitale Informationen zu den Bürgern, die in verteilten oder zentralen Datenbanken gespeichert sind. Ein Diebstahl oder eine Manipulation der Bürgerdaten würde das Vertrauen der Bürger und der staatlichen Institutionen in die über die Bürger gespeicherten Daten verletzen. Eine eindeutige Identitätsfeststellung und die Zuordnung von Rechten und Pflichten der Bürger wäre damit schwierig bis unmöglich.

Eigentümerstruktur strategischer IKT-Infrastrukturen
Veränderungen in der Eigentümerstruktur der strategisch bedeutenden IKT-Infrastrukturen können ein Risiko für die öffentliche Ordnung und Sicherheit darstellen, wenn neue Eigentümer mit entsprechendem Stimmen- und Kapitalanteil z.B. die personelle Besetzung der Führungsgremien verändern oder Einfluss auf die Geschäftsstrategie des entsprechenden Unternehmens nehmen.

Fahrlässiges Verhalten bei strategischen Infrastrukturbetreibern
Fahrlässiges Nutzerverhalten (unsichere Passwörter, Öffnen von Spam-eMails etc.) stellt immer noch die größte Gefährdung für IT-Systeme dar. Umso mehr ist dieses Verhalten bei strategischen Infrastrukturbetrieben problematisch und muss gezielt durch Schulungs- und Auditmaßnahmen verhindert werden.

Fehlende bzw. nicht aktuelle rechtliche Grundlagen
Rechtliche Regulierungen sind derzeit noch primär auf Datenschutz und nicht gesamtheitlich auf IT-Sicherheit fokussiert.

Fehlende strategische Netzwerkstrukturplanung
Die schnell wachsende Nachfrage nach Übertragungskapazitäten in den unterschiedlichsten Formen sowie die damit zusammenhängende Notwendigkeit der Steuerung und Verwaltung dieser Übertragungskapazitäten stellt neue Anforderungen an die Netzwerkstrukturplanung. Ohne eine strategische Planung der Entwicklung der Übertragungsnetzwerke (z.B. welche Kapazitäten werden bereitgestellt, welche Anschlüsse erfolgen wann und wo?) besteht das Risiko, dass diese den Anforderungen nicht standhalten und sich dadurch die Anfälligkeit für unbeabsichtigte und beabsichtigte Störungen erhöht.

Fehlender Regulierungsfokus auf IKT-Sicherheit
National und international gibt es verschiedene Standards zur Förderung der Unternehmenssicherheit im Allgemeinen und des Schutzes

der strategisch bedeutenden Infrastrukturen im Besonderen. Das Risiko besteht darin, dass Standards für die IKT-Sicherheit noch zu sehr aus einer sektorspezifischen Sichtweise definiert werden, womit der Blick für den Querschnittscharakter dieses wichtigen Aufgabenbereichs verloren geht. Daraus resultiert die Gefahr uneinheitlicher Anforderungen an die IKT-Sicherheit in unterschiedlichen strategisch bedeutenden Infrastruktursektoren.

Fehlendes Fachpersonal

Fehlendes oder nicht richtig ausgebildetes Fachpersonal kann die negativen Folgen bestehender technischer Schwächen zusätzlich verstärken.

Fehlendes oder unzureichendes BCM

Business Continuity Management (BCM) dient der Vorbereitung von Behörden und Unternehmen zur Bewältigung von Schadensereignissen. Ziel ist, dass die jeweilige Organisation möglichst schnell ihren Normalbetrieb wieder aufnehmen kann. Aufgrund der zunehmenden Vernetzung zwischen den Unternehmen und den strategisch bedeutenden Infrastruktursektoren besteht die große Herausforderung darin, BCM verstärkt organisationsübergreifend anzulegen. Das ist gegenwärtig oft noch nicht der Fall, sodass die Organisationen an den Schnittstellen zu ihren Drittlieferanten (Service Level Agreement) verwundbar sind.

Fehlerhafte, inkompatible Codes/Software

Programme bestehen aus hunderttausenden bis Millionen Zeilen langen Codes. Bei der Entwicklung können sich Fehler eingeschlichen haben in Bezug auf Verfügbarkeit, Funktion oder Sicherheit. Durch ständige Weiterentwicklung passen verschiedene Programme und Prozesse in der verwendeten Software oft nicht mehr korrekt zusammen, sie sind also inkompatibel. Es besteht die Gefahr, durch solche Fehler und Inkompatibilitäten handlungsunfähig zu werden, Wissen zu verlieren oder nur mit extremem Aufwand Systeme wieder zum Laufen zu bringen.

Geknackte digitale Schlüsselsysteme

Sichere Kommunikation im Internet basiert auf Verschlüsselungstechniken, die auf dem Prinzip beruhen, dass die Entschlüsselung einer geschützten Information ohne Kenntnis eines geheimen Schlüssels unmöglich und ein Ausprobieren von möglichen Schlüsseln zu aufwändig ist. Diese Sicherheit baut auf mathematischen Verfahren auf, für die keine einfachen Lösungen bekannt sind. Sollte eine mathematische Lösung für eines dieser Verschlüsselungsverfahren gefunden werden, könnte das Verfahren schlagartig nicht mehr für die Absicherung der Internetkommunikation benutzt werden. Eine Umstellung der gängigen Verfahren würde aber nur mit sehr hohem Aufwand durchführbar sein.

Kein Sicherheitsgütesiegel/Audits

Sicherheitsüberprüfungsstandards und Audits existieren, werden aber nur bei wenigen Zielgruppen (z.B. Smartcards) oder nur auf freiwilliger Basis (z.B. ISO 27001) durchgeführt. Ein einheitliches Sicherheitsgütesiegel und verstärkt durchgeführte Audits würden es den Anwendern erleichtern, eine Entscheidung betreffend der Sicherheit eines Produktes oder Betriebes zu treffen.

Keine systematische Technologiefolgenabschätzung

Neue Technologien werden durch entsprechenden Marktdruck und durch das Versprechen, aktuelle Probleme zu lösen, so rasch als möglich eingeführt. Eine Abschätzung von langfristigen Technologiefolgen entfällt oder wird nicht systematisch und für alle wesentlichen Technologien durchgeführt.

Lückenhafte Cyber Governance

Das Fehlen von Konzepten, Verfahren und Gremien/Plattformen für die öffentlich-private, öffentlich-öffentliche und privat-private Zusammenarbeit im Kontext der Cybersicherheit ist ein Risiko, weil staatliche und private Maßnahmen dadurch nicht gut genug aufeinander abgestimmt werden können. Lücken und möglicherweise auch widersprüchliche Maßnahmen können die Folgen davon sein.

Macht der sozialen Netze und deren Manipulation

Soziale Netze können gezielt manipuliert werden, um die öffentliche Meinung zu beeinflussen und Falschmeldungen zu verbreiten.

© pagadesign – iStockphoto.com

Mangelnde Sicherheitsstandards/ -bewusstsein im Gesundheitswesen

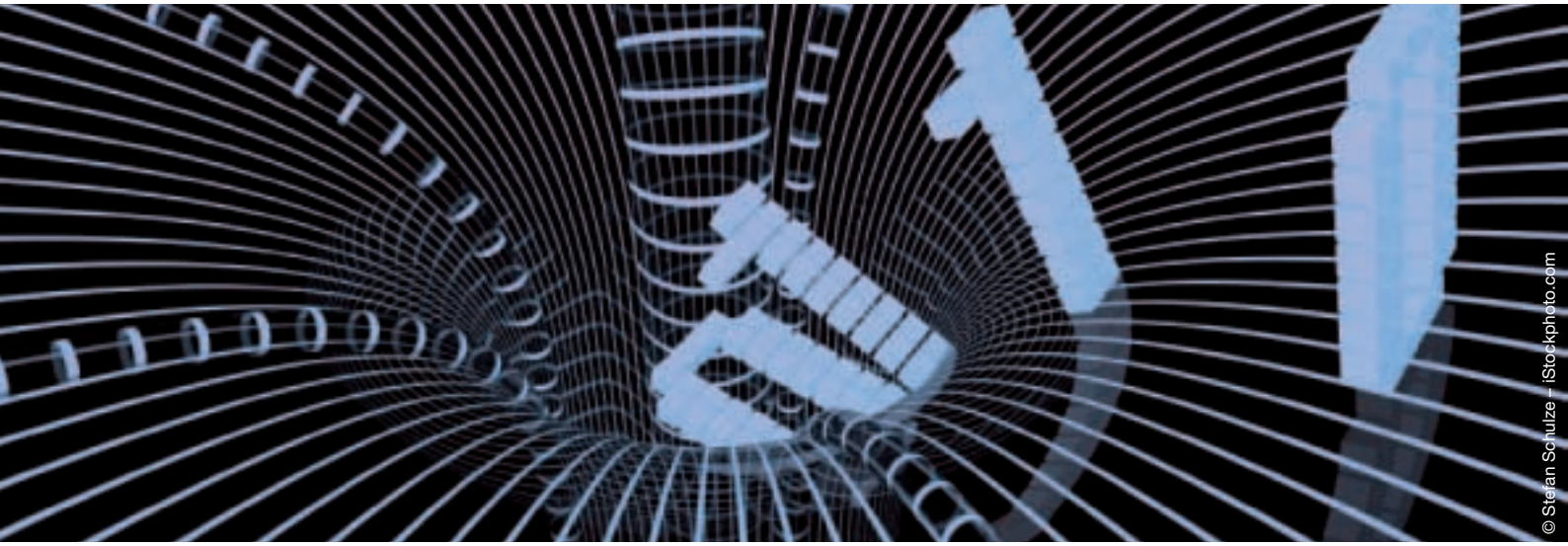
IKT-Systeme im Gesundheitswesen reichen von den Datenverarbeitungssystemen zur Speicherung der Patientendaten, über telemedizinische Anwendungen und technische Geräte, die für Operationen, die Überwachung und die Steuerung von Lebensfunktionen wichtig sind, bis hin zu Anwendungen, die älter werdende Menschen im Alltag unterstützen (Ambient Assisted Living). Aus der Möglichkeit, diese Systeme zu manipulieren, resultieren unterschiedliche Risiken, wie z.B. der Missbrauch von Patientendaten oder die bewusste Störung lebenserhaltender Geräte (z.B. Hacking von Herzschrittmachern oder Insulinpumpen).

Manipulation der IKT-Systeme der Energieerzeugung und -versorgung

Durch Störungen der SCADA-Systeme und Einbruch in die zentralen Verteilersysteme können Ausfälle herbeigeführt, Übertragungen gestört und die Erzeugung von Energie erheblich erschwert, wenn nicht sogar unmöglich gemacht werden. In Rechenzentren stellen Spannungsschwankungen, Spannungsspitzen sowie kurzer und längerer Stromausfall eine reale Bedrohung dar.

Manipulation der IKT-Systeme des Verkehrsmanagements (z.B. Schiene, Straße)

Im Verkehrssektor werden IKT-Systeme zur Steuerung des Verkehrsflusses (Verkehrsmanagement) und zum Betrieb der einzelnen Plattformen (z.B. Autos, Bahn, Schiffe, Flugzeuge) verwendet. Cyberrisiken können sich unkontrolliert verbreiten, denn die Netze sind durch den Einsatz von IKT miteinander verbunden und voneinander abhängig. Die Cybersicherheit von Verkehrsleitsystemen kann z.B. durch Malware gefährdet werden; ebenso besteht die Möglichkeit, dass Verkehrsleitsysteme durch das Einschleusen von Trojanern ferngesteuert werden. Die Folge ist ein bewusst angerichtetes Chaos im Verkehrssektor.



Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen

Der finanzielle Zahlungsverkehr ist für die reibungslose Funktion einer Volkswirtschaft von essentieller Bedeutung. Nicht nur der Bürger wickelt seinen Zahlungsverkehr elektronisch per Kreditkarte oder e-Banking ab; Gleiches gilt auch für die Geschäftsbanken und den Verkehr zwischen den Nationalbanken. Die bewusste oder zufällige Störung der elektronischen Systeme, die hierfür eingesetzt werden, kann die Liquiditätsversorgung Österreichs nachhaltig beeinflussen. Aufgrund der engen Verflechtung der nationalen Bankensysteme sind internationale Auswirkungen nationaler Liquiditätsengpässe nicht auszuschließen.

Manipulation der IKT-Systeme für Cloud Services

Cloud Services werden in drei Delivery-Modelle unterteilt: Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service. Es besteht keine Möglichkeit, tatsächlich festzustellen, wo sich die Daten physikalisch befinden, wer darauf Zugriff hat, wie diese Daten abgesichert sind und ob die lokalen Datenschutzbestimmungen den eigenen Erwartungen entsprechen.

Manipulation der IKT-Systeme in der Wasserwirtschaft

Damit ist eine Manipulation der Gesamtheit der Systeme für die Bereitstellung von Trinkwasser, Prozess-/Brauchwasser und die Entsorgung bzw. Wiederaufbereitung von Abwasser gemeint. Die Steuerungselemente (SCADA), die für Wassermanagementsysteme verwendet werden, sind für absichtliche Störungen/Manipulationen anfällig, was die Versorgung mit Wasser beeinträchtigen kann.

Manipulation von GPS (Zeitsynchronisation)

Über GPS beziehen viele IKT-Systeme eine hochgenaue Uhrzeit für synchronen Betrieb mit anderen Systemen, Logbucheinträge, Start und Stopp von Prozessen etc.

Manipulation von IKT-Systemen im Luft-, Bahn- und Straßenverkehr

Manipulation von IKT-Systemen, mit denen Flugzeuge, Bahn, Frachtverkehr etc. gesteuert und gelenkt werden. Meistens mit dem Ziel, Chaos anzurichten und Erpressungen durchzuführen.

Manipulation von Kommunikations- und SAT-Verbindungen

Beinhaltet die Manipulation aller möglichen Kommunikationsverbindungen, die zur Daten- (z.B. Internet) und Sprachverbindung notwendig sind. Eine Manipulation der Verbindungen kann durch Umleitung, Unterbrechung, Abhören und Einschleusen fehlerhafter bis bösartiger Informationen erfolgen.

Manipulierte bzw. unsichere Hardware

Hardware wird zur Kostenoptimierung und ohne Kontrollmöglichkeit für den Kunden verteilt auf mehrere Länder entwickelt und

in Massenprozessen hergestellt. Detaillierte Prüfungen der Hardware auf Manipulationen (z.B. Abhöreinrichtungen in Bankomat-Kassenterminals) oder Unsicherheiten (Öffnen von WLAN-Verbindungen, ohne dass dies konfiguriert wurde) können nur selten durchgeführt werden. Und auch die geprüfte Sicherheit eines Testexemplares garantiert nicht, dass nicht andere Exemplare der Hardware manipuliert oder unsicher sind.

Nicht erkannte (IKT-)Anomalien

Daten, die fehlerfrei erscheinen, aber einen versteckten Code enthalten, der bisher nicht als bösartig oder schadhaft erkannt wurde (z.B. Conficker-Virus) und gegen den deshalb keine Gegenmaßnahmen ergriffen werden können.

Social Engineering

Im Zusammenhang mit IT-Sicherheit wird der Begriff für eine Strategie von Online-Betrügern gebraucht. Indem sie individuell auf ihre Opfer zugehen, steigern sie ihre Erfolgsraten: zuvor ausspionierte Daten, wie etwa die Surfgewohnheiten oder Namen aus dem persönlichen Umfeld des Opfers, werden dafür verwendet, beispielsweise Phishing-E-Mails persönlich zu formulieren und dadurch Vertrauen zu erwecken.

Systematischer Diebstahl digitaler Identitäten

Eine digitale Identität ist die Teilmenge der Attribute einer Entität, welche diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten bestimmbar machen. Eine Entität kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere digitale Identitäten besitzen. Das von organisierten Gruppen oder Einzeltätern durch Trojaner ermöglichte Ausspähen und Nutzen von fremden ID-Attributen stellt eine sehr hohe Bedrohung dar.

Ungenügender Anreiz für Sicherheitsinvestitionen

Der Regulierungsfokus der meisten Länder, die staatliche Leistungen durch die Liberalisierung den Kräften des Marktes überlassen haben, liegt auf der Kostenseite. Durch die Liberalisierung sollen die Konsumenten von niedrigeren Preisen profitieren. Beispiele aus unterschiedlichen Infrastruktursektoren (z.B. Eisenbahn) zeigen aber, dass ein einseitiger Kosten-/Preisfokus nicht nur die Qualität der Leistungen, sondern auch deren Sicherheit beeinträchtigen kann. Sicherheitsinvestitionen stellen für Unternehmen direkte Kosten dar. Fehlen die Anreize für solche Investitionen, erfolgen sie in der Regel nicht.

Unklare Kompetenzlage der Behörden

Unklare Aufgabenverteilungen und Zuständigkeiten der Behörden für Cyberrisiken. Teilweise mehrfache Abdeckung von bestimmten Cyberrisiken durch mehrere Ministerien und Behörden.

Unsichere Steuerungssysteme (GmbH z.B. SCADA)

Industrielle Steuerungssysteme sind weit verbreitet und steuern sowie messen unzählige Produktionsprozesse. Die Verbreitung des Stuxnet-Wurms (der iranische Nuklearanlagen befallen hat) hat gezeigt, dass diese Systeme anfällig für Sicherheitsprobleme sind und deaktiviert, zerstört oder ferngesteuert werden können.

Unzureichendes Cyberlagebewusststein und -verständnis

Fehlendes Lagebewusstsein und Lageverständnis bezüglich der Vorgänge im Cyberspace führen dazu, dass die handelnden Akteure die Gefahren und deren mögliche Folgen nicht oder nicht rechtzeitig erkennen und damit unterschätzen. Negative Folgen können sein: unzureichende Vorbereitung, keine oder nicht ausreichende Abwehr- und Bewältigungsmaßnahmen/-mittel sowie mangelhafte Fähigkeiten zur Wiederherstellung des Normalbetriebs.

Verletzlichkeit der IKT-Infrastruktur durch Naturkatastrophen

IKT-Infrastruktur kann durch massive Naturkatastrophen (Hochwasser, Erdbeben etc.) beschädigt oder unerreichbar werden.

Verteilte Angriffe auf Systeme (DDoS)

„Distributed Denial of Service“: Angriffe, bei denen eine große Anzahl an Computern verwendet wird, um ein bestimmtes Computersystem durch eine hohe Anzahl an Anfragen zu blockieren.

9.5. Autorenhinweise

Dr. Heiko Borchert ist Inhaber und Geschäftsführer der Sandfire AG und seit 1997 in der sicherheitsstrategischen Beratung für Kunden im öffentlichen und privatwirtschaftlichen Sektor tätig. Zu seinen Themenschwerpunkten zählen der Schutz kritischer Infrastrukturen, die öffentlich-private Sicherheitszusammenarbeit, maritime Sicherheit, Energie- und Rohstoffversorgungssicherheit, die Transformation der Streitkräfte, Theorie und Praxis der Vernetzten Sicherheit sowie die sicherheitspolitische Vorausschau. Dr. Borchert hat an der Universität St. Gallen Internationale Beziehungen, Betriebswirtschaftslehre, Volkswirtschaft sowie Rechtswissenschaft studiert und dort auch promoviert.

Mag.ª Ursula Eysin ist seit Anfang 2011 Managerin bei der REPUCO Unternehmensberatung GmbH in Wien. Sie studierte Sinologie an der Universität Wien und in Beijing (VR China), Betriebswirtschaftslehre an der Wirtschaftsuniversität Wien und absolvierte das Masterstudium „Public Relations“ an der Universität Wien. Ihre Beraterkarriere begann Eysin nach mehrjähriger Tätigkeit als Produktionsmanagerin und Moderatorin im Kulturbereich (Theater, Film, Oper) im Jahr 2004 beim Technologieberatungsunternehmen eutema (European Technology Management) in Wien. Im Mai 2008 wechselte sie als Beraterin zu PLEON Publico, um dort hauptsächlich Kunden aus dem IKT-Umfeld zu betreuen. Im Jahr 2010 holte sie PricewaterhouseCoopers ins Unternehmen. Ihr Arbeitsschwerpunkt liegt in der Konzeption, Begleitung und Moderation komplexer Stakeholder- und Strategieprozesse.

Mag. Wolfgang Gattringer ist Inhaber und Geschäftsführer der REPUCO Unternehmensberatung GmbH in Wien. Er arbeitet seit mehr als 15 Jahren in Führungspositionen im öffentlichen und privatwirtschaftlichen Bereich. Nach seiner betriebswirtschaftlichen Ausbildung (Wirtschaftsuniversität Wien, UC Irvine) war er von 2003 bis 2007 Kabinettschef-Stellvertreter im Bundesministerium für Inneres, Wien. Danach wechselte er als Service Director zu Alcatel-Lucent in Ungarn und war im Anschluss Mitglied der Geschäftsführung der PR-Agentur PLEON Publico. Seine Arbeitsschwerpunkte sind die Konzeption, Begleitung und Moderation von komplexen Stakeholder- und Strategieprozessen an der Schnittstelle zwischen dem öffentlichen Bereich, der Wirtschaft, Industrie sowie weiteren Anspruchs- und Interessengruppen.

Wolfgang Rosenkranz arbeitet seit Mitte 2011 für die REPUCO Unternehmensberatung GmbH, Wien. Davor war er sieben Jahre für die Österreichische Staatsdruckerei als Direktor der Abteilung eGovernment Solutions und International Sales tätig, wo er unter anderem für die Einführung des elektronischen Reisepasses verantwortlich war. Die Arbeitsschwerpunkte von Wolfgang Rosenkranz sind eGovernment und IT-Projektmanagement. Er hat an der Technischen Universität Wien Technische Physik studiert.

Univ.-Prof. DI Karl Rose ist Inhaber und Geschäftsführer der Strategy Lab GmbH in Wien, Universitätsprofessor für strategisches Management und angewandte Unternehmensführung an der Karl-Franzens-Universität Graz, Director Policy and Scenarios des World Energy Council in London sowie Mitglied des Aufsichtsrats der Energie Steiermark AG und Aufsichtsratsvorsitzender der Steweag-Steg GmbH. Von 1985 bis 2010 war Univ.-Prof. Rose in unterschiedlichen Funktionen für den internationalen Energiekonzern Shell tätig, zuletzt als Chief Strategist. Seine Arbeitsschwerpunkte sind Strategieentwicklung, Szenarioplanung, Sicherheitspolitik, erneuerbare Energie und internationale Klimapolitik. Univ.-Prof. Rose hat Erdölwissenschaften an der Montanuniversität Leoben studiert und mit Auszeichnung abgeschlossen.

KURATORIUM SICHERES ÖSTERREICH