BVSW | BRAINLOOP

CORPORATE TRUST
business risk & crisis management

FUTURE REPORT

Weltweite Mega-Trends und ihre Sicherheitsherausforderungen

Inhalt

The trouble with the future is that it usually arrives before we are ready for it.

Arnold H. Glasow (Autor, 1905-1998)

Vorwort

Alfred Czech
Geschäftsführer
Corporate Trust

Sicherheit ist ein elementares Bedürfnis von uns allen. Ohne Sicherheit gibt es keine freie Gesellschaft. Auch unseren Wohlstand verdanken wir in erheblichem Maß der Sicherheit in unserem Land. Wie aber wirkt sich der permanente globale Wandel auf unsere Sicherheit aus? Welchen neuen Herausforderungen müssen wir uns stellen? Und: Wo stehen wir in 10, 15 oder 20 Jahren?

Dieser Future Report kann sicherlich keine Antworten auf alle Zukunftsfragen geben. Er untersucht jedoch ausführlich die großen Sicherheitstrends der kommenden Jahre, skizziert mögliche künftige Entwicklungen samt ihren Folgen und entwirft Lösungsansätze.

Der Report ist aus einer Zusammenarbeit von Corporate Trust mit dem Bayerischen Verband für Sicherheit in der Wirtschaft e.V. (BVSW) und der Brainloop AG hervorgegangen. Er besteht aus drei Teilen, die ein möglichst umfassendes Bild der künftigen Sicherheitsherausforderungen geben sollen.

Der erste Teil stellt die Ergebnisse einer Kurzstudie dar, in der Unternehmen aus Österreich und Deutschland zum Thema Sicherheit befragt wurden. Sie zeigt, welche Schäden sie in den vergangenen Jahren tatsächlich erlitten haben und wie sie die künftige Bedrohung einschätzen.

Im zweiten Teil finden sich Risk Maps für das Jahr 2017. Sie veranschaulichen die aktuelle weltweite Sicherheitslage im Hinblick auf vier Hauptrisiken: Krisen & Konflikte, Informationsabfluss, Investitionssicherheit und Medizinische Risiken.

Für den dritten Teil des Reports haben wir zehn große Sicherheitsthemen untersucht: von neuen Formen der Organisierten Kriminalität über Wettrüsten im Cyberraum bis hin zu Terrorismus einer neuen Dimension. Für die-

se Trends haben wir auch Zukunftsszenarien entwickelt. Orientiert haben wir uns dabei an den wichtigsten globalen Risiko-Trends der nächsten Jahre, wie sie das World Economic Forum[1] in Davos in seinem „Global Risks Report 2017" definiert hat – und daraus zehn abgeleitet, die uns besonders relevant für das Thema Sicherheit erschienen.
So viel ist schon heute klar: In Zukunft werden sich immer mehr Menschen einen immer kleineren Teil der Erde teilen müssen, in dem sie sicher leben können und ausreichend versorgt sind. Das hat mehrere Gründe. Zum einen wächst die Weltbevölkerung dramatisch. Laut STATISTA, einem weltweit führenden Statistik-Portal, ist die Zahl der Menschen von 5,32 Milliarden im Jahr 1990 auf 7,35 Milliarden im Jahr 2015 gestiegen – ein Plus von 2 Milliarden in nur 25 Jahren.[2] Die Vereinten Nationen schätzen, dass die Zahl bis 2100 auf 11,21 Milliarden Menschen anschwellen wird.

Zum anderen führt der Klimawandel bereits heute dazu, dass ganze Landstriche von Dürre betroffen sind, Naturkatastrophen sich häufen und folglich immer mehr Menschen auf der Flucht sind. In der Zukunft wird es vermutlich Kriege um Wasser und Nahrung geben. Dies kann zwar noch etwas länger dauern als die Zeitspanne, die dieser Report betrachtet. Erste Auswirkungen spüren wir aber schon heute. Instabile politische Systeme, korrupte Machthaber und eine steigende Zahl von Unruhen beschleunigen solche Entwicklungen.

Darüber hinaus wird die Digitalisierung die Sicherheit in allen Lebensbereichen grundlegend verändern. Computersteuerung in allen Produktionsmaschinen, Sprachassistenten im eigenen Haus, vernetzte Elektrofahrzeuge mit umfassender Sensorik, Drohnen im Logistikprozess und Wearables[3] für alle Lebenslagen: Das sind nur einige Dinge, die teilweise schon heute Realität sind und uns künftig noch viel häufiger im Alltag begleiten werden.

Es stellt sich die Frage: Sind wir Menschen überhaupt bereit für die Digitalisierung? Können wir noch selbst mit der Technik umgehen, sie verstehen – und steuern? So sehr wir auch die neuen digitalen Angebote schätzen: Es wird künftig immer schwieriger werden, sich im Dschungel der Vernetzung zurechtzufinden. Um dabei nicht allzu viel aus der Hand zu geben, werden sich die Nutzer verstärkt mit der Technik auseinandersetzen müssen. Tun sie das nicht, wird ein Gefühl der Ohnmacht eintreten.

Wird sich auch unsere gefühlte Sicherheit ändern? Diese hängt von vielen Faktoren ab. Zwei sehr wesentliche sind, inwieweit wir tatsächlich in einem von Gefahren geprägten Umfeld leben und wie sehr wir uns mit solchen Risiken bewusst auseinandersetzen. Österreich ist zwar ein sehr sicherer Rechtsraum. Um unser gutes Sicherheitsgefühl zu bewahren, müssen wir uns aber schon heute mit den künftigen Herausforderungen befassen, damit wir bei Bedarf rechtzeitig und angemessen handeln können.

In diesem Sinne wünsche ich Ihnen viel Vergnügen bei der Lektüre des Future Reports. Selbstverständlich freuen wir uns immer über Anregungen und auf einen Austausch mit Ihnen über Ihre Erfahrungen mit sicherheitsrelevanten Themen.

Ihr

Alfred Czech

1) Das Weltwirtschaftsforum (World Economic Forum, kurz: WEF) ist eine in Cologny im Schweizer Kanton Genf ansässige Stiftung, die in erster Linie für das von ihr veranstaltete Jahrestreffen gleichen Namens in Davos bekannt ist. Dabei kommen international führende Wirtschaftsexperten, Politiker, Intellektuelle und Journalisten zusammen, um über aktuelle globale Fragen zu diskutieren. Diese umfassen neben der Wirtschafts- auch die Gesundheits- und Umweltpolitik. Das Forum gibt auch Forschungsberichte heraus.

2) https://de.statista.com/statistik/daten/studie/1717/umfrage/prognose-zur-entwicklung-der-weltbevoelkerung/

3) Wearables sind tragbare Computersysteme, die während der Anwendung am Körper des Benutzers befestigt sind. Wearable Computing unterscheidet sich von der Verwendung anderer mobiler Computersysteme dadurch, dass die hauptsächliche Tätigkeit des Benutzers nicht die Benutzung des Computers selbst, sondern eine durch den Computer unterstützte Tätigkeit in der realen Welt ist.

Vorwort

Univ.-Prof.
Dr. Marion A. Weissenberger-Eibl
Ordinaria für Innovations- und TechnologieManagement am Karlsruher Institut für Technologie KIT und Institutsleiterin des Fraunhofer-Instituts für System- und Innovationsforschung ISI

Sicherheit und Innovation ein zukunftsweisendes Spannungsfeld

Sicherheit ist vor dem Hintergrund der Diskussionen im World Economic Forum ein nicht nur spannendes, sondern angesichts der großen Herausforderungen in der Gesellschaft ein drängendes Thema. Extreme Wetterereignisse, großflächige unfreiwillige Migration, zerstörerische Naturkatastrophen, Terrorattacken oder Datenbetrug beeinflussen die Volkswirtschaften, das Zusammenleben in der Gesellschaft ebenso wie die individuell wahrgenommene Sicherheit.

Sicherheit in Form objektivierter und subjektiver Sicherheiten ist durch komplexe Wirkmechanismen und unterschiedliche Akteure gekennzeichnet und ist sowohl Treiber im als auch konstituierendes Merkmal und Prüfstein des Innovationssystems einer Volkswirtschaft.

Aktuelle Überlegungen zu Sicherheitstrends greifen deshalb beispielsweise neue Formen der Organisierten Kriminalität, moderne Propaganda im 21. Jahrhundert, Datenschutz in Verbindung mit Big Data, politische und religiöse Agitation in Firmen oder die Digitalisierung der Gesellschaft auf.

Die Digitalisierung der Gesellschaft ist ein weitreichender Treiber, um unternehmerische und wirtschaftspolitische Überlegungen anzustellen und sich mit möglichen zukünftigen Konsequenzen und der Ableitung des heutigen Tuns zu beschäftigen. Betrachtet man den damit verbundenen Transformationsprozess in Wirtschaft und Gesellschaft, so wird deutlich, welche erheblichen Potenziale in der Verknüpfung von Digitalisierung und Sicherheit stecken, und diese gilt es engagiert zu erschließen. Allein die Tatsache, dass gemäß des Innovationsindikators 2017 Deutschland im Digitalisierungsindex auf Rang 17 von 35 untersuchten Volkswirtschaften liegt, zeigt den enormen Handlungsbedarf auf (vgl. Innovationsindikator 2017, Hrsg. acatech und BDI, S. 7, S. 36).

Um angemessene Lösungen zu finden, sind kreative Ideen, realisierbare Entwicklungspfade und Umsetzungsschritte, die die gesamte Gesellschaft einbeziehen, zu entwickeln. Vordenker und Gestalter der Wettbewerbsfähigkeit im Sinne von Sicherheit und Lebensqualität sind mehr denn je gefragt. Das heißt aber auch, sich der Ängste der Betroffenen und der möglichen Skepsis technischer Entwicklungen in der Gesellschaft anzunehmen. Hierfür sind Experimentierräume zur Interaktion aufzusetzen, der Dialog und die Partizipation mit der Zivilgesellschaft aktiv methodisch zu gestalten, politische und regulatorische Rahmenbedingungen zu erörtern, die Umsetzung zu begleiten und mit Wirkungsanalysen und -szenarien zu hinterlegen.

Um dieser - auch unternehmenspolitischen - Bedeutung gerecht zu werden, bedarf es unabhängiger Forschungsinstitutionen, die ergebnisoffen und wissenschaftlich fundiert agieren, Orientierung und Erklärung geben, Debatten anstoßen und handelnde Akteure im „Innovationssystem Sicherheit" begleiten. Wahrnehmungen, Erwartungen und Gefühle zu Sicherheit in den Phänomenbereichen Kriminalität, Terrorismus, Naturkatastrophen und technische Großunglücke sind zu bewältigende Herausforderungen, die einen systemischen Blick notwendig machen. Dabei ist zu berücksichtigen, dass die Wahrnehmung von Sicherheit in die soziale Sicherheit eingebettet ist. Hieraus ergibt sich eine theoretische und empirische Abhängigkeit von einem allgemeinen Sicherheitskonzept sowie von dem Vertrauen in die eigene und gesellschaftliche Fähigkeit zur Bewältigung von Risiken.

Die Resilienz der Gesellschaft hat heute mehr denn je damit zu tun, die wirtschaftliche Leistungs- und Wettbewerbsfähigkeit zu stärken, indem Handlungsspielräume erhalten werden. Im Vordergrund stehen Reflexions- und Zukunftsfähigkeit im Innovationssystem Sicherheit, die proaktive Auseinandersetzung mit Ungewissheit, mit wahrgenommener Un-Sicherheit, um vorausschauend, flexibel und verlässlich im dynamischen Umfeld agieren zu können.

Im Unternehmenskontext bedeutet dies, Entwicklungs- und Produktionsprozesse nachhaltig zu gestalten, aber auch partizipative Verfahren der Technikgestaltung einzusetzen und weiterzuentwickeln. Damit kann das Bestehen von Unternehmen beispielsweise der Sicherheitswirtschaft und die vor- und nachgelagerten Wirtschaftsbereiche in einem sich wandelnden Umfeld langfristig gewährleistet werden. Die Auseinandersetzung mit Foresight und Impact ist im Kontext der Wirtschaft aber auch der Politik und Zivilgesellschaft ein hierfür überaus geeignetes Instrument, um mögliche sozioökonomische Auswirkungen in einem frühen Stadium zu signalisieren.

Der Future Report zeigt wichtige Facetten des Innovationssystems Sicherheit aus der Perspektive der Wirtschaft auf und ist somit ein guter Kompass für Akteure aus Politik, Wirtschaft und der Zivilgesellschaft, ergebnisoffen zu diskutieren und für Unternehmen und zum Wohl der Menschen wichtige Entscheidungen zur Erfolgs- und Wohlstandssicherung einzuleiten oder vorzubereiten.

Ihre

Prof. Dr. Marion A. Weissenberger-Eibl

Vorwort

Rechtsanwalt Heinrich Weiss
Geschäftsführer
Bayerischer Verband für Sicherheit
in der Wirtschaft, BVSW e.V.

BVSW

Wer immer sich die Zukunft vorstellt, wird daran scheitern. Oder haben wir eine Chance vorherzusehen, welche Trends die Menschheit beeinflussen und verändern werden?

Vor zehn Jahren kam das iPhone auf den Markt und begann die Welt zu verändern. Nun eröffnet das iPhone X einen weiteren digitalen Trend. Nicht die eigene Gesichtserkennung, hier das Face ID, ist die wegweisende Entwicklung, sondern die Tatsache, dass dies erst die Vorstufe eines Trends ist, der ebenfalls die Welt verändern wird. Im Zusammenspiel mit der Künstlichen Intelligenz wird die erweiterte innovative Face ID den sozialen Status eines Menschen ablesen können, möglicherweise seine sexuelle Orientierung oder seine kriminelle Veranlagung. Wir werden wissen, welcher Herkunft er ist, ohne ihn danach fragen zu müssen. Wir brauchen unser Gegenüber also zukünftig nur in unser iPhone X „future" blicken lassen, um dieses Wissen zu erhalten.

Aus staatlicher Sicht ist das eine Entwicklung, die bereits in Versuchen mit freiwilligen Bürgern in öffentlichen Videoüberwachungssystemen umgesetzt wird. Hier werden Bürger durch Gesichtserkennung erfasst und auf eine mögliche Gefährdung hin analysiert. Das verspricht Sicherheit und sozialen Frieden, schränkt aber sicherlich die freie persönliche Handlungsfreiheit der Bürger ein, die unser Grundgesetz garantiert.

Aussagen zur Sicherheit und Freiheit beförderten schon immer die zentralen Diskussionen um die Frage, wie soll sich die Gesellschaft organisieren, um ihre Resilienz , also ihre psychische Widerstandsfähigkeit und ihre Fähigkeit Krisen zu bewältigen, zu erhalten und sie durch Rückgriffe auf persönliche, wirtschaftliche und sozial vermittelte Ressourcen für Entwicklungen zu nutzen.

Hier setzt dieser Zukunftsbericht an und dies ist der Grund, warum wir als Bayerischer Verband für Sicherheit in der Wirtschaft diese Studie mit betreut und mit gefördert haben.

Hier sehen wir unsere satzungsmäßige Aufgabe, die zukünftigen Trends der Gefährdungen für unsere Gesellschaft und unserer Wirtschaft zu analysieren, diese in die öffentliche Diskussion einzubringen, zu politisieren und in die Wissenschaft zu transformieren.

Das vorstehende Vorwort von Prof. Dr. Marion A. Weissenberger-Eibl zeigt dies deutlich auf. Im Bereich der Sicherheit bedeutet dies, verantwortungsvolle Forschung und Innovation (Responsible Research and Innovation, RRI) zu beachten, um einerseits die gesellschaftlichen Strukturen zu bewahren, andererseits den sozialen Zusammenhalt der Bürger nicht zu gefährden. So kann Wissenschaft insbesondere im Bereich der Genetik die Identität eines Men-

schen analysieren, sie aber auch generieren und fälschen. Die im Bericht aufgezeigte Digitalisierung wird unseren Alltag und damit auch alle unsere Sicherheitsprozesse komplett neu gestalten. Wer trifft zukünftig diesbezügliche Entscheidungen und wer setzt diese um? Computer und Roboter?

Nichts desto trotz und gerade aus diesem Blickwinkel heraus zeigt dieser Bericht die Trends auf, die unsere Sicherheit in allen Facetten beeinträchtigen werden und welchen Gefährdungen die Wirtschaft ausgesetzt werden wird.

Diese Trends aufzuzeigen ist absolut notwendig, um einerseits Forschung in verantwortungsvoller Weise zu betreiben, andererseits die wirtschaftlichen Prozesse so zu entwickeln, dass wir in 10 - 20 Jahren die Resilienz der heutigen gesellschaftlichen Strukturen erhalten oder verbessert haben.

Unsere Verbandsaufgabe sehen wir darin, Forschungs- und Innovationsthemen in die Öffentlichkeit zu tragen, mögliche Konsequenzen vorherzusehen und die Gesellschaft zu sensibilisieren. Wir wollen den sozialen Frieden bewahren und die Sicherheit der Gesellschaft garantieren, indem wir helfen, Brücken zu bauen, Brücken zwischen den Risiken, die bevorstehen und Chancen, die wir erarbeiten und nutzen müssen.

Dieser Bericht bietet einen Querschnitt durch die Risiken, die uns bevorstehen, zeigt aber auch die Chancen auf, diesen Risiken zu begegnen.

Es war ein Bedürfnis unseres Vorstandes, diesen Report mit zu initiieren, denn gemäß unserer Satzung wollen wir unsere Wirtschaft vor Schäden bewahren, die durch Terror, organisierter Kriminalität und Extremismus auf unsere Gesellschaft einwirken.

Es wäre uns eine Freude, wenn Sie Gefallen und Nutzen an diesem Bericht finden und dieser Bericht Sie unserem Verband näher bringt. Sicherheit ist eine Kernaufgabe der gesellschaftlichen Verpflichtungen und diese Verpflichtung kann nur durch Beteiligung aller Kräfte an den Prozessen erfüllt werden, die auch unser Verband verfolgt.

Gerne würden wir uns mit Ihnen über eine gemeinsame zukünftige Zusammenarbeit unterhalten und Wege diskutieren, die unsere Wirtschaft stärken und erhalten lassen.

Gelegenheiten dazu bieten unsere Arbeitskreise in München, Nürnberg, Regensburg oder Passau, unsere Businessfrühstücke am Flughafen München oder unsere Veranstaltungen insgesamt. Hier bieten Ihnen unsere Wintertagung (der deutsche Sicherheitsgipfel) am Spitzingsee, der Sicherheitstag im Sommer des BVSW und des BDSW, (Bundesverband der Sicherheitswirtschaft) und die Security Tour im Herbst eine Palette und ein Portfolio an Informationsaustausch und an Möglichkeiten, ihr Netzwerk zu erweitern, die seinesgleichen in Deutschland suchen. Besuchen Sie bitte dazu unsere Webseite (www.bvsw.de).

In diesem Sinne lassen wir uns das Thema nach den Worten von Karl Valentin angehen: „Die Zukunft war früher auch besser!"

Mit freundlichen Grüßen und vielen Dank

Ihr

Heinrich Weiss

Vorwort

Martin Ehling
Leiter Vertrieb Deutschland
Industrie und Handel
Brainloop AG

BRAINLOOP

Mit der Digitalisierung, Industrie 4.0 und dem Internet of Things (IoT) haben auch Datendiebstahl, Spionage und Sabotage Hochkonjunktur. Besonders gefragt: deutsches Technologie-Know-how.

Die Kluft zwischen Arm und Reich wird immer größer – das gilt für Menschen und für Staaten. Im Rahmen dieser Entwicklung wird die Umverteilung von Wohlstand mit illegitimen Methoden Mittel zum Zweck. Besonders begehrte Honigtöpfe sind Österreich und Deutschland. Als reiche, hoch technisierte Länder mit starken Branchen wie dem Kraftfahrzeug- und Maschinenbau oder der chemischen Industrie wecken Österreich und Deutschland Begehrlichkeiten bei internationalen Wettbewerbern, staatlichen Institutionen und Kriminellen gleichermaßen. Unternehmen, denen es gelingt, das geistige Know-how eines Konkurrenten anzuzapfen, sparen sich schließlich Entwicklungskosten und können Produkte schneller und günstiger auf den Markt bringen.

Vernetzung befeuert Cyber-Kriminalität

Unabhängig davon besteht allerdings die Notwendigkeit der Kollaboration innerhalb von Unternehmensgrenzen und darüber hinweg. In Verbindung mit einer starken Vernetzung von Systemen und Maschinen steigt damit das Risiko enorm. Wie viele andere musste dies in jüngster Vergangenheit die thyssenkrupp AG am eigenen Leib erfahren. Der Stahl- und Technologieriese war Ende 2016 einer Großattacke auf die eigene IT-Infrastruktur zum Opfer gefallen. Bei den Angreifern handelte es sich vermutlich um eine Gruppe, die planmäßig mit staatlicher Unterstützung vorgegangen ist. „Hochspezialisierte Profis", so die offizielle Verlautbarung des Konzerns, hatten es auf den Diebstahl von Know-how und Forschungsergebnissen abgesehen. Konkret richtete sich die Industriespionage gegen die Sparte Industrial Solutions, in der thyssenkrupp die Entwicklung von industriellen Großanlagen für Dünger- und Zementfabriken sowie sein Geschäft mit dem Bau von Schiffen und U-Booten vereint. Ferner waren die Cyber-Agenten in die IT des Walzwerks Hohenlimburg bei Hagen eingedrungen, das in erster Linie für die Autozulieferindustrie produziert.

Viele Unternehmen kompromittiert

Dass es sich bei der Attacke auf den Essener Industriegiganten beileibe nicht um einen Einzelfall und in Sachen digitaler Kriminalität längst nicht mehr um Kavaliersdelikte pubertärer Computer-Nerds handelt, beweist eine aktuelle Erhebung von Corporate Trust unter rund 4.738 Unternehmen in Österreich und Deutschland. Demnach erklärten fast 58 Prozent der österreichischen Unternehmen, bereits mit einem Angriff durch Organisierte Kriminalität konfrontiert worden zu sein. Etwa 34 Prozent waren in den vergangenen drei Jahren Opfer von Spionage oder Informationsabfluss. Als Konsequenz erhöhen Organisati-

onen in Österreich (92 Prozent) ihre IT-Sicherheit. Ähnlich besorgniserregend liest sich eine Studie von BITKOM vom Juli 2017 unter knapp 1.070 Geschäftsführern und Sicherheitsverantwortlichen aus unterschiedlichen Branchen. So wurde mehr als die Hälfte der befragten Unternehmen in Deutschland (53 Prozent) in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl. Der entstandene Schaden in diesem Zeitraum: rund 110 Milliarden Euro.

Angreifer haben es indes nicht immer direkt auf digitale Daten abgesehen. Häufigstes Delikt ist nach wie vor der Diebstahl von IT- oder Telekommunikationsgeräten wie Notebooks oder Smartphones. Davon war fast ein Drittel der Unternehmen in den vergangenen 24 Monaten betroffen. Ein weiteres Vorgehen, das mitunter sogar von Einreisebehörden zumindest „toleriert" wird: Es mehren sich die Beschwerden von Geschäftsreisenden, dass gewisse Staaten die Einreise mit verschlüsselten IT-Geräten verwehren – oder Festplatten bei Grenzüberquerungen von Beamten kopiert wurden. Ein weiteres Ergebnis: 41 Prozent der betroffenen Organisationen machen Wettbewerber, Kunden, Lieferanten oder Dienstleister für die Angriffe verantwortlich.

Hacker aus aller Herren Länder

Längst trifft der Vorwurf der Wirtschaftsspionage indes nicht mehr nur Unternehmen und staatliche Institutionen bekannter Plagiatorenländer wie China. Vor allem die GUS-Staaten zeigen ein besonderes Interesse daran, sich wirtschaftliches Know-how für ihre Firmen illegal anzueignen. Und auch die USA sind mit Hilfe ihrer Abhörpraktiken nicht erst seit den Enthüllungen von Whistleblower Edward Snowden weltweit gut im Bilde – in puncto Terrorabwehr und wenn es um Vorteile für die amerikanische Wirtschaft geht. Snowden wörtlich in der „Welt": „Es gibt keine Zweifel, dass die USA Wirtschaftsspionage betreiben. Wenn es bei Siemens Informationen gibt, von denen sie meinen, dass sie für die nationalen Interessen von Vorteil sind, nicht aber für die nationale Sicherheit der USA, werden sie der Information hinterherjagen und sie bekommen."

So kommen 23 Prozent der registrierten Angriffe aus Osteuropa, 20 Prozent aus China und 18 Prozent aus Russland. Danach folgen die USA (15 Prozent), die Summe aller westeuropäischen Länder (12 Prozent) und Japan (7 Prozent).

Doch auch die Angriffe aus ärmeren Ländern sollten nicht unterschätzt werden. Einerseits wächst die Kluft zu den Industriestaaten, andererseits wird die Technik immer billiger. Diese Kombination wird sich in einer höheren Anzahl an Spionage-Versuchen aus Schwellen- und Entwicklungsländern niederschlagen. Die gesamte Bedrohungslage wird sich also in den nächsten Jahren massiv verschärfen.

Organisatorische und technische Abwehrmaßnahmen unumgänglich

Zahlen und Fakten, die schonungslos offenlegen: Unternehmen müssen viel mehr für die digitale Sicherheit tun. Dazu gehören im Zusammenhang mit Industriespionage grundsätzlich zwei Dimensionen – organisatorische und technische. So ist es im Hinblick auf das organisatorische Engagement zunächst wichtig, Mitarbeiter sowie Management umfassend über die Risiken der Vernetzung zu informieren und dafür zu sensibilisieren: Rund 72 Prozent der österreichischen Unternehmen haben deshalb laut Corporate Trust ihre Mitarbeiter entsprechend vorbereitet.

In diesem Zusammenhang sollte eine dedizierte Sicherheitskultur etabliert werden, mit Schulungen und regelmäßigen Trainings. In das Feld der organisatorischen Maßnahmen gehört mitunter auch die Einrichtung eines Wirtschaftsschutz-Beauftragten, zumindest in größeren Unternehmen. Organisatorische Maßnahmen umfassen zudem ein präventives Risikomanagement, in dem externe Gefahren identifiziert oder interne Schwachstellen aufgedeckt werden können, sowie die Tests auf Praxistauglichkeit und regelmäßige Überprüfung interner Sicherheitsregularien. Auch zählen individuelle Zugriffsrechte auf sensible Daten, ein Notfallmanagement für den Krisenfall, ein Besuchermanagement für den Umgang mit Gästen sowie die eindeutige Kennzeichnung von Betriebsgeheimnissen zu den Sicherheitsstandards.

Ein virtueller Tresor für geistiges Eigentum

Zu den technischen Aspekten gehören Punkte wie die Informationssicherheit auf Geschäftsreisen mit Firmenequipment ebenso wie die korrekte Vorgehensweise mit verdächtigen E-Mails, die Verwendung externer Speichergeräte oder die Direktive, unsichere File-Sharing-Plattformen zu meiden. Eine Kombination aus mehreren wichtigen Sicherheitsfunktionen stellen virtuelle Datenräume dar, die den sicheren Austausch hoch sensibler Daten und Dokumente gewährleisten. Damit sind Unternehmen in der Lage, in Wertschöpfungsketten zu kollaborieren

Vorwort

und mit externen Partnern so einfach und sicher zusammenzuarbeiten wie mit den internen Kollegen. Virtuelle Datenräume ermöglichen es unter anderem, gemeinsam sicher an vertraulichen Dokumenten zu arbeiten oder sie geschützt zur Verfügung zu stellen. Dabei sollte auf die Wahl des Anbieters und den Standort des Betreibers geachtet werden: Insbesondere der Unternehmenssitz in Verbindung mit dem Serverstandort bestimmen, welche Rechtsgrundlagen für den Datenschutz gelten. Der Serverstandort Österreich oder Deutschland alleine reicht nicht aus – ein Thema, das seit der Einführung des Patriot Act durch die US-Sicherheitsbehörden eine zentrale Bedeutung gewonnen hat. Durch den Einsatz eines virtuellen Datenraums ist sichergestellt, dass das geistige Eigentum nicht durch Industriespionage in falsche Hände gerät.

Fazit:
Mit der zunehmenden Vernetzung und der Notwendigkeit der Kommunikation über mehrere Parteien hinweg steigt das Risiko von Spionage, Sabotage und Datendiebstahl enorm. Organisationen sind in der Pflicht, ihr geistiges Eigentum durch organisatorische und technische Maßnahmen bestmöglich zu schützen. Für die technische Umsetzung eignen sich virtuelle Datenräume. Sie haben sich als Mittel der Wahl für die sichere Zusammenarbeit mit externen Partnern bewährt und ermöglichen es auch Geschäftsreisenden, jederzeit und mit jedem Endgerät auf Informationen zuzugreifen.

Ihr

Martin Ehling

Sicherheit erreicht man nicht, indem man Zäune errichtet,
Sicherheit gewinnt man, indem man Tore öffnet.

Urho Kekkonen
(Finnischer Politiker, 1900 - 1986)

Ergebnisse in Kürze

- Mehr als die Hälfte aller österreichischen Unternehmen (exakt 57,4 %) wurde bereits Opfer eines Angriffs durch die Organisierte Kriminalität. Dabei kam vor allem Social Engineering[1] durch Spear-Phishing-Mails[2] und Watering-Hole-Angriffe[3] zum Einsatz.

- Über ein Viertel der Unternehmen (exakt 27,9 %) gab an, bereits durch einen Terroranschlag geschädigt worden zu sein. Allerdings kam es glücklicherweise bisher zu keinem konkreten Personenschaden. Die häufigsten Schäden waren Projektverzögerungen (21,3 %) und Ausfälle beim Öffentlichen Personennahverkehr (18,0 %).

- Obwohl die tatsächlichen Schäden durch Terrorismus relativ gering sind, sehen 57,4 Prozent der Unternehmen Terrorismus als künftiges Risiko für ihr Unternehmen. Allerdings beeinträchtigt die Angst vor einem Anschlag nur in sehr geringem Maße die Geschäftstätigkeit der Unternehmen. 57,4 Prozent gaben an, dass dieses Risiko ihre Geschäftstätigkeiten in Österreich überhaupt nicht beeinträchtige (Stufe 0 auf der Skala). Für knapp ein Fünftel der Unternehmen (18,0 %) spielt die Angst vor Terrorismus jedoch eine gewisse Rolle beim Auslandsgeschäft. Sie bewerteten die Auswirkungen mit 2 auf einer Skala von 0 (kein) bis 5 (hoch).

- Know-how-Verlust durch Spionage oder sonstigen Informationsabfluss stellt nach wie vor ein großes Problem für österreichische Unternehmen dar. Nur weniger als die Hälfte der Unternehmen (42,6 %) konnte bestätigen, dass sie in den letzten drei Jahren von einem solchen Vorfall verschont wurden. Bei 34,4 Prozent gab es einen konkreten Know-how-Verlust. 23,0 Prozent wussten es nicht und hatten damit vermutlich keine ausreichenden Kontrollmöglichkeiten im Unternehmen, um einen Spionageangriff überhaupt feststellen zu können.

- Insgesamt gesehen geht laut Einschätzung der Unternehmen die größte Gefahr bei Spionage bzw. Informationsabflüssen von ausländischen Nachrichtendiensten aus. Auf die Frage, wie stark das Know-how ihres Unternehmens dadurch bedroht ist, bewerteten insgesamt 49,2 Prozent das Risiko mit „mittel" bis „hoch" (3, 4 oder 5) auf einer Skala von 0 (kein) bis 5 (hoch).

- Propaganda im aktuellen Zeitalter von Fake News und Desinformation stellt für Unternehmen immer häufiger ein Problem dar. 34,4 Prozent der Unternehmen waren schon einmal Opfer von manipulierten Informationen und hatten dabei mit gezielten Falschmeldungen in sozialen Medien oder der Presse zu tun.

1) Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwendung einer „Legende"). Social Engineering hat das Ziel, unberechtigt an vertrauliche Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

2) Unter dem Begriff Spear-Phishing versteht man die gezielt gegen eine Person oder Organisation gerichteten Versuche, über gefälschte E-Mails an persönliche Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Es handelt sich dabei um eine Form des Social Engineering, bei der die Gutgläubigkeit des Opfers ausgenutzt wird.

3) Bei einem sog. Watering-Hole-Angriff werden durch Cyberkriminelle gezielt Webseiten mit einem Schadcode infiziert, von denen der Angreifer weiß, dass seine potenziellen Opfer diese immer wieder aufsuchen (abgeleitet von Watering Hole – engl. für Wasserstelle, Kneipe, Bar). Das Ziel ist es, den Computer des Opfers zu infizieren, um sich darüber Zugriff auf das Netzwerk zu verschaffen.

- Propaganda und Manipulation der öffentlichen Meinungsbildung halten die meisten Unternehmen bei sich selbst für deutlich weniger gefährlich als in der österreichischen Wirtschaft allgemein. Dies kann ein Trugschluss sein. 42,6 Prozent gaben an, dass sie gar keine Gefahr (Stufe 0 auf der Skala von 0 bis 5) für ihr eigenes Unternehmen sehen und 16,4 Prozent bewerteten das Risiko mit Stufe 1 auf der Skala, also sehr gering. Für die gesamte Wirtschaft glauben dagegen nur 37,7 Prozent, dass es keine Gefahr (Stufe 0) gebe und 11,5 Prozent bewerteten mit Stufe 1.

- Ein Viertel der Unternehmen sieht in der Einflussnahme durch Propagandamaßnahmen eine Gefahr für die öffentliche Meinungsbildung bei demokratischen Wahlen in Österreich. 21,3 Prozent bewerteten das Risiko einer Einflussnahme mit der Stufe 4 (relativ hoch) und 4,9 Prozent mit der Stufe 5 (hoch) auf der Skala von 0 bis 5.

- Die zunehmende Urbanisierung (Verstädterung) wird den Unternehmen in Zukunft vermutlich häufiger Probleme bereiten. So gaben 86,9 Prozent der befragten Unternehmen an, dass sie es als größte Herausforderung sehen, qualifizierte Mitarbeiter für Standorte in weniger attraktiven ländlichen Regionen zu finden. Steigende Kriminalität (68,9 %) oder soziale Unruhen durch sog. Gentrifizierung[4] (47,5 %), also die Aufwertung und Verteuerung städtischer Wohnlagen, wurden ebenfalls als Probleme erkannt. Nur 8,2 Prozent glauben, dass keine negativen Auswirkungen durch die Verstädterung zu befürchten sind.

- Ein Drittel der Unternehmen, exakt 37,7 Prozent, sehen Migrationsbewegungen als zukünftiges Risiko für ihr Unternehmen an. Als größte Herausforderung wird dabei eine ungenügende Integration als Nährboden für Radikalisierung (72,1 %) eingestuft. Dass es durch die Ausbildung von Migranten mittelfristig zu einen Know-how-Abfluss aus Österreich kommen könnte, befürchten immerhin noch 44,3 Prozent der Unternehmen.

- Die Digitalisierung der Gesellschaft wird die Unternehmen vor große Herausforderung stellen. So glauben 85,2 Prozent der Firmen, dass Cyberattacken eine wesentliche Gefahr für die österreichische Wirtschaft durch Industrie 4.0 bzw. das Internet of Things[5] darstellen. Weitere Gefahren werden durch Cyber-Terror (83,6 %), die zunehmende Abhängigkeit vom Internet (82,0 %), durch einen möglichen Blackout (70,5 %) oder die Produkthaftung nach einem Cyberschaden (59,0 %) gesehen. Die konkreten Risiken für das eigene Unternehmen werden dabei durchweg geringer eingestuft als für die österreichische Wirtschaft allgemein.

- Bei den Technologien werden vor allem die Social Networks (63,9 %), der Schwachstellenhandel mit sog. Zero-Day-Lücken[6] (63,3 %) und das User Profiling[7] (62,3 %) als risikobehaftet eingestuft. Wirklich kritisch für das eigene Unternehmen werden auch Drohnen (21,3 %) und die Vernetzung kritischer Infrastrukturen (18,0 %) bewertet.

- Datenschutz ist zwar generell wichtig, die neue EU-Datenschutz-Grundverordnung wird jedoch nicht uneingeschränkt positiv bewertet. Auf die Frage, ob sie diese neue Rechtsnorm als Chance oder eher risikobehaftet bzw. sogar kritisch beurteilen, gaben nur 36,1 Prozent an, darin eine Chance zu sehen. Fast zwei Drittel, nämlich genau 63,9 Prozent, finden dass sie eher risikobehaftet oder sogar kritisch für ihr Unternehmen ist.

4) Als Gentrifizierung (engl. gentry für „niederer Adel"), bezeichnet man den sozioökonomischen Strukturwandel bestimmter großstädtischer Viertel im Sinne einer Attraktivitätssteigerung für eine neue Klientel und dem anschließenden Zuzug zahlungskräftiger Eigentümer und Mieter. Damit verbunden ist der Austausch ganzer Bevölkerungsgruppen.

5) Als Internet of Things (Kurzform: IoT) bezeichnet man die Vision einer globalen Infrastruktur der Informationsgesellschaft, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen. Die immer kleineren eingebetteten Computer sollen Menschen unterstützen, ohne abzulenken oder überhaupt aufzufallen. So werden z. B. Industrieanlagen oder Haushaltsgegenstände vernetzt bzw. miniaturisierte Computer, sogenannte Wearables, mit unterschiedlichen Sensoren direkt in Kleidungsstücke eingearbeitet.

6) Eine Zero-Day-Lücke ist eine systematische Möglichkeit, um eine Schwachstelle in der EDV auszunutzen, die meist bei der Entwicklung eines Programms entstanden ist und die von Angreifern eingesetzt wird, bevor es einen Patch als Gegenmaßnahme gibt. Dabei werden mit Hilfe von Programmcodes Sicherheitslücken und Fehlfunktionen von Programmen oder ganzen Systemen ausgenutzt, um sich Zugang zu verschaffen. Entwickler haben dadurch keine Zeit (null Tage = engl. zero day) die Software so zu verbessern, dass der Angriff wirkungslos wird.

7) Als User Profiling wird die Erstellung eines Profils über das Nutzerverhalten einzelner Menschen im Internet, meist zu Marketingzwecken, verstanden.

Kurzstudie

Hintergrund und Methodik

Für die Kurzstudie wurden nach dem Zufallsprinzip 1.396 Unternehmen in Österreich und 3.342 Unternehmen in Deutschland befragt. Ziel der Erhebung war es, bisherige sicherheitsrelevante Vorfälle und die dabei erlittenen Schäden zu erfassen sowie eine Einschätzung künftiger Risiken und präventiver Maßnahmen aus Sicht der Unternehmen zu erhalten.

Die Sicherheitstrends der Zukunft betreffen alle Branchen der Wirtschaft und Unternehmen jeder Größe, vom Konzern über den Mittelstand bis hin zu den Kleinunternehmen, zudem fast alle Privatleute. Die Kurzstudie sollte eine möglichst umfassende Lageeinschätzung für Österreich und Deutschland ermöglichen. Daher wurden die Firmen repräsentativ ausgewählt, die Befragung wurde branchenübergreifend sowie quer über alle Unternehmensgrößen durchgeführt.

Da es keine verbindliche Definition für die Einordnung in eine Unternehmensgröße gibt, wurden für Österreich die KMU-Definition der Wirtschaftskammer Österreich und für Deutschland die Kriterien des Instituts für Mittelstandsforschung in Bonn herangezogen. Die Bewertung richtete sich daher nach der Anzahl der Mitarbeiter und dem Umsatzvolumen. Berücksichtigt wurden in beiden Ländern für die Studie nur Unternehmen mit mindestens zehn Mitarbeitern und einem Umsatz bzw. einer Bilanzsumme von mehr als einer Million Euro.

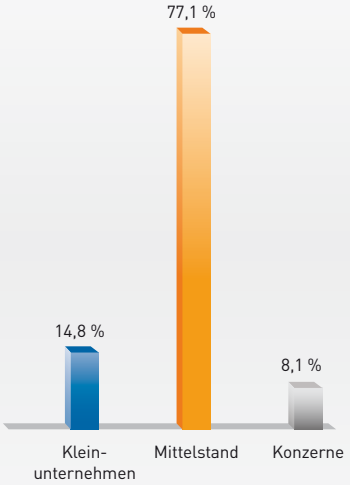
Darüber hinaus blieb es den Unternehmen überlassen, sich selbst in eine Kategorie (Konzern, Mittelstand, Kleinunternehmen) einzuordnen. Dies sollte vor allem inhabergeführten Unternehmen die Möglichkeit bieten, sich aufgrund ihrer mittelständisch geprägten Ausrichtung und Führungskultur dem Mittelstand zuzurechnen, obwohl sie häufig über mehr Mitarbeiter und ein größeres Umsatzvolumen verfügen.

Für die Befragung wurden im Juli 2017 insgesamt 4.738 Vorstände, Geschäftsführer bzw. Leiter der Bereiche Risikomanagement, Unternehmenssicherheit, Informationsschutz, Recht, Finanzen, Controlling, IT, Interne Revision, Compliance oder Personal angeschrieben. Die Befragung wurde online durchgeführt. Den Unternehmen war es freigestellt, die Antworten anonym zu geben. Um die Anonymität sicherzustellen, wurden in der E-Mail die für alle Teilnehmer gleichen Zugangsdaten (Benutzername und Passwort) mitgeteilt. Dies sollte gewährleisten, dass keine Zufallsbesucher der Studien-Webseite die Befragung ausfüllen konnten, sondern nur teilnahmeberechtigte Firmen. Zusätzlich wurden mit 21 Unternehmensvertretern telefonische Interviews über ihre Erfahrungen und Einschätzungen der künftigen Entwicklung geführt.

Von allen angeschriebenen Unternehmen antworteten genau 356 Teilnehmer, dies sind 7,5 Prozent aller befragten Firmen. Von den Teilnehmern stammten 102 Antworten aus Österreich (7,3 Prozent) und 254 Antworten aus Deutschland (7,6 Prozent).

Für eine bessere Übersichtlichkeit wurden in diesem Future Report jeweils nur die Ergebnisse der Befragung aus Österreich dargestellt. Sollten Sie auch die detaillierten Ergebnisse aus Deutschland interessieren, so kommen Sie bitte auf uns zu. Wir lassen Ihnen dann gerne auch die deutschen Auswertungen zukommen.

Teilnahme an der Studie

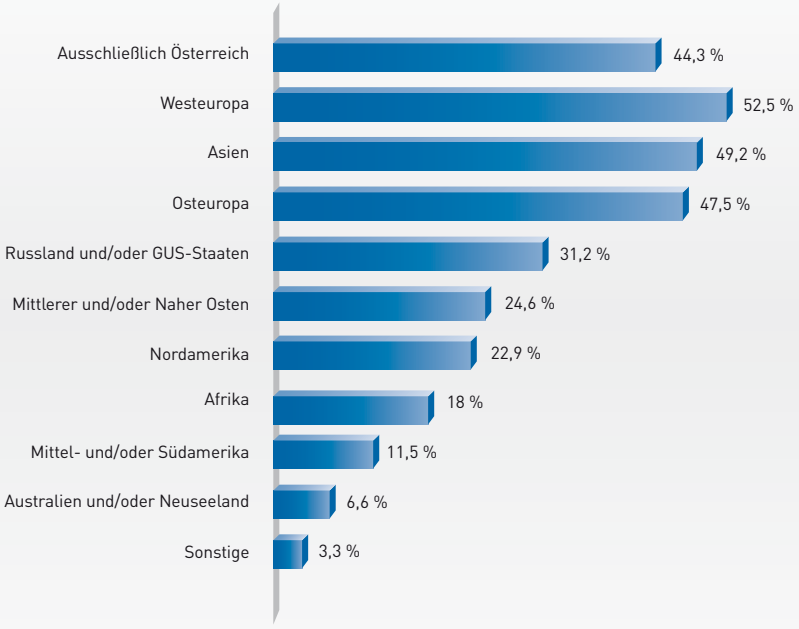


GRAFIK 1

Quelle: Corporate Trust 2017

In welchen Ländern/Regionen sind Sie geschäftlich aktiv bzw. haben Sie Niederlassungen oder Repräsentanzen?

(Mehrfachnennungen möglich)



GRAFIK 2

Quelle: Corporate Trust 2017

Kurzstudie

Schäden in den Unternehmen

Risiken der Zukunft lassen sich zu einem gewissen Teil aus den bereits erfolgten Angriffen und Schäden bei Unternehmen ableiten. Es lohnt sich also, die aktuelle Bedrohungslage zu hinterfragen, wenn man sich Gedanken über die künftigen Herausforderungen machen will. Für die Bewertung der aktuellen Situation wurden daher die Schäden durch Organisierte Kriminalität, Terrorismus, Industriespionage und moderne Propaganda abgefragt.

Auf ihre Erfahrungen mit Organisierter Kriminalität befragt, gaben 57,4 Prozent der österreichischen Unternehmen an, dass sie bereits Opfer eines Angriffs wurden. Dies sagt selbstverständlich noch nichts zu den konkreten Schadenszahlen aus, belegt aber deutlich, dass die Organisierte Kriminalität ein ernst zu nehmendes Problem für unsere Wirtschaft darstellt.

Aus den Erfahrungen der letzten Jahre ist festzustellen, dass die Organisierte Kriminalität zunehmend auf digitale Angriffe setzt, um daraus Profit zu schlagen. Bei den Unternehmen sind vermutlich noch nicht alle Sicherheitsmechanismen entsprechend angepasst, um auf die neuen Bedrohungen angemessen reagieren zu können. So hatten es 42,6 Prozent mit Spear-Phishing-Mails[1] oder einem Watering-Hole-Angriff[2] zu tun und weitere 21,3 Prozent waren bereits von einer sog. Fake President Attacke[3] betroffen. Die Angriffe in all diesen Fällen haben Social Engineering[4] als Grundlage. Dabei werden die Opfer im Vorfeld gezielt ausgespäht, welche Interessen oder sozialen Kontakte sie haben, um die Kontaktaufnahme daraufhin ganz gezielt abstimmen zu können.

Auch Bitcoin[5]-Erpressungen, bei denen die Täter versuchen über einen Ransomware-Angriff[6] den Computer zu kapern und die Festplatte zu verschlüsseln, um dann für die Entschlüsselung Geld in Form einer digitalen Währung zu erpressen, hatten bereits 19,7 Prozent der österreichischen Unternehmen zu verzeichnen.

BRAINLOOP

„Kryptotrojaner wie WannaCry und Petya zielen darauf ab, den Zugang zu lokal gespeicherten Daten zu blockieren. Besonders kritische Daten sollten deshalb in einer hochsicheren Umgebung außerhalb des Firmennetzwerks gelagert werden. Dies ermöglicht den Anwendern außerdem jederzeit den gesicherten Zugang auf ihre Daten unabhängig von Gerät oder Standort."

Martin Ehling
Leiter Vertrieb Deutschland Industrie und Handel
Brainloop AG

1) Unter dem Begriff Spear-Phishing versteht man die gezielt gegen eine Person oder Organisation gerichteten Versuche, über gefälschte E-Mails an persönliche Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

2) Bei einem Watering-Hole-Angriff werden durch Cyberkriminelle gezielt Webseiten mit einem Schadcode infiziert, von denen der Angreifer weiß, dass seine potenziellen Opfer diese immer wieder aufsuchen. Das Ziel ist es, den Computer des Opfers zu infizieren, um sich darüber Zugriff auf das Netzwerk zu verschaffen.

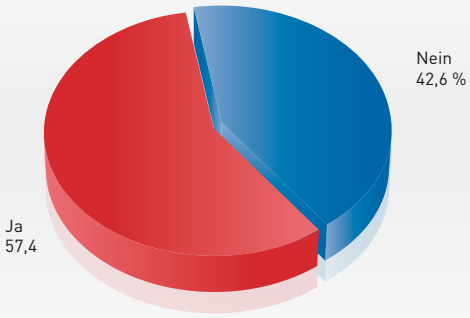
3) Fake President ist auch bekannt unter CEO Fraud. Dabei handelt es sich um eine Betrugsmasche, bei der Firmen unter Verwendung einer falschen Identität und meist gut gefälschten E-Mails, die einen anderen Absender vorgaukeln, zur Überweisung von Geld manipuliert werden.

4) Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an vertrauliche Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

5) Bitcoin (englisch sinngemäß für digitale Münze) ist eine digitale Währung eines weltweit verwendbaren und dezentralen Zahlungssystems. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet abgewickelt, so dass keine zentrale Abwicklungsstelle benötigt wird.

6) Ransomware (von englisch „ransom" für Lösegeld) sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf seine Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Die Daten auf dem Computer werden dabei meist verschlüsselt, um für die Entschlüsselung ein Lösegeld zu fordern.

Wurde Ihr Unternehmen bzw. das Management bereits Opfer eines Angriffs durch die Organisierte Kriminalität?

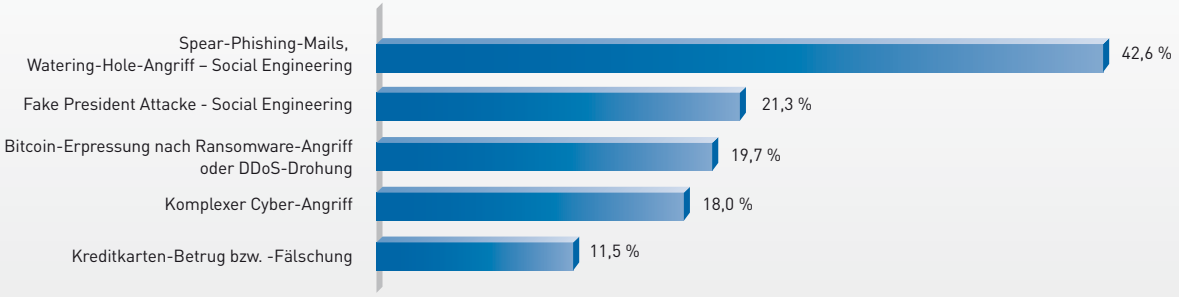


GRAFIK 3

Quelle: Corporate Trust 2017

Welche Schäden erlitten Sie durch einen solchen Angriff durch die Organisierte Kriminalität?

(Mehrfachnennungen möglich)



GRAFIK 4

Quelle: Corporate Trust 2017

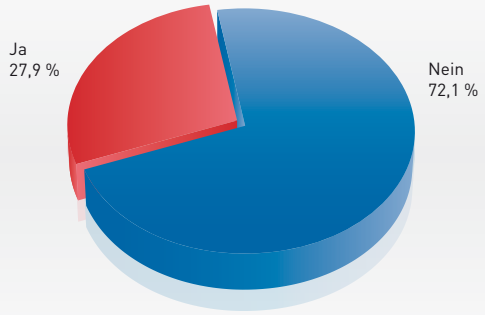
KURZSTUDIE

SCHÄDEN IN DEN UNTERNEHMEN

Terrorismus ist gefühlt eine immer stärker werdende Bedrohung. Mit jedem Anschlag wird uns deutlicher, wie verletzlich unsere Sicherheit eigentlich ist. In den Medien wird über solche Angriffe umfangreich berichtet und das Risiko eines Anschlags ist auch in Europa an der Tagesordnung. Daher ist es wichtig einmal aufzuklären, welche Schäden österreichische Unternehmen bisher tatsächlich erlitten haben.

Immerhin 27,9 Prozent der Unternehmen gaben an, bereits durch einen Terroranschlag betroffen gewesen zu sein. In 21,3 Prozent der Fälle war dies durch Projektverzögerungen und in 18,0 Prozent war es durch den Ausfall des Öffentlichen Personennahverkehrs (ÖPNV), mit dem die Unternehmen zu kämpfen hatten. Ein konkreter Personenschaden war nach Angaben der österreichischen Unternehmen bisher nicht zu verzeichnen. Erinnert man sich an die Terroranschläge 2016 in Brüssel, bei denen mehrere Selbstmordattentäter innerhalb kurzer Zeit an verschiedenen Stellen Bomben zündeten, und bei denen das öffentliche Leben für längere Zeit zum Erliegen kam, dann kann man diese Angaben gut nachvollziehen.

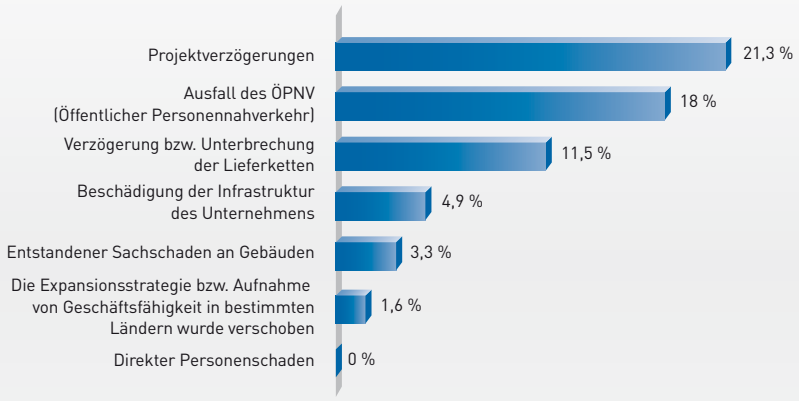
War Ihr Unternehmen bereits durch einen Terroranschlag betroffen?



GRAFIK 5

Quelle: Corporate Trust 2017

Welche Schäden erlitten Sie konkret durch den Terroranschlag ?
(Mehrfachnennungen möglich)



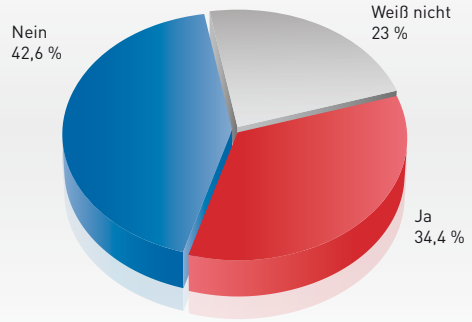
GRAFIK 6

Quelle: Corporate Trust 2017

Zu den Risiken durch Industriespionage hat Corporate Trust in den letzten Jahren bereits eine Studie erstellt. Dass es sich hierbei um ein hohes Risiko für österreichische Unternehmen handelt, ist dabei deutlich geworden. Im Rahmen dieses Future Reports sollten die konkreten aktuellen Zahlen erhoben werden, um festzustellen, ob es in den letzten Jahren eine gravierende Veränderung gegeben hat. Dies ist allerdings nicht der Fall. Die Ergebnisse sind ähnlich der Studie von 2014.

Nach ihren Erfahrungen mit Industriespionage befragt gaben 34,4 Prozent der Unternehmen an, dass sie in den letzten drei Jahren Opfer von Spionage oder Informationsabfluss geworden sind. 42,6 Prozent konnten dies zwar verneinen. Knapp ein Viertel der Unternehmen (exakt 23,0 %) wussten dies jedoch nicht und könnten somit ebenfalls bereits Opfer geworden sein. Dies zeigt abermals, dass vermutlich ein Großteil der österreichischen Wirtschaft in den letzten drei Jahren mit Industriespionage oder Informationsabfluss zu tun hatte.

Wurde Ihr Unternehmen in den letzten drei Jahren Opfer von Spionage oder Informationsabfluss?

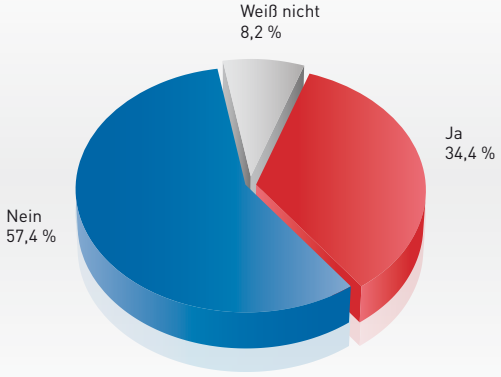


GRAFIK 7

Quelle: Corporate Trust 2017

Begriffe wie Fake News oder Alternative Fakten haben nach der Präsidentschaftswahl 2016 in den USA eine neue Bekanntheit erreicht. In der Gesellschaft entsteht zunehmend ein Bewusstsein, dass Informationen manipuliert oder falsch sein können und diese oft gezielt gesteuert werden, um die Öffentlichkeit oder eine bestimmte Zielgruppe zu beeinflussen. Daher war es interessant zu erfahren, ob auch Unternehmen in Österreich bereits Erfahrungen mit manipulierten Informationen gemacht haben. Es war überraschend, dass bereits 34,4 Prozent der Unternehmen schon einmal Opfer von Fake News oder gezielten Falschmeldungen in den Sozialen Medien wurden.

War Ihr Unternehmen schon einmal Opfer manipulierter Informationen (Fake News, Gezielte Falschmeldungen in Social Media etc.)?



GRAFIK 8

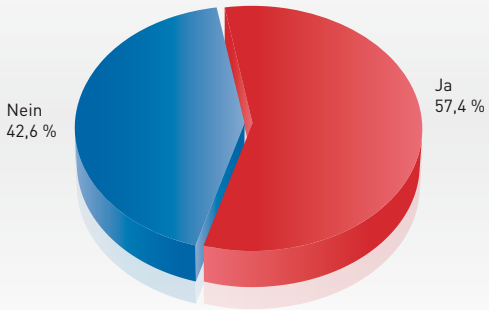
Quelle: Corporate Trust 2017

KURZSTUDIE

RISIKOBEWERTUNG FÜR DIE ZUKUNFT

Anschläge durch islamistische Selbstmordattentäter, Überfälle mit großkalibrigen Waffen oder Fahrzeuge, die in Menschenmengen rasen, gehören leider immer öfter zu den Tagesmeldungen. Geschah in früheren Jahren ein Großteil der Terroranschläge in fernen Ländern, die bereits als „kritisch" eingestuft wurden, gibt es solche Attacken heute immer öfter in europäischen Businessmetropolen. Es ist daher nicht verwunderlich, dass über die Hälfte aller Unternehmen in Österreich den weltweiten Terrorismus als künftiges Risiko für ihr Unternehmen betrachten.

Sehen Sie Terrorismus als künftiges Risiko für Ihr Unternehmen?



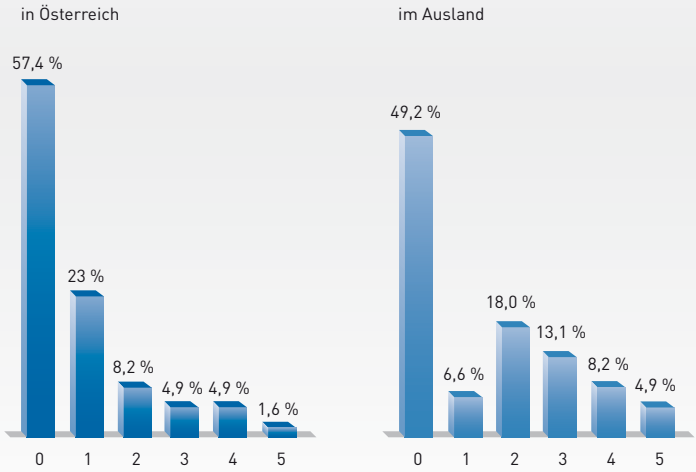
GRAFIK 9

Quelle: Corporate Trust 2017

Allerdings lassen sich die Unternehmen nicht von der Angst vor Terror lähmen. Auf die Frage, wie stark die Angst vor Terrorismus ihre Geschäftstätigkeit beeinflusst, gaben 57,4 Prozent der Unternehmen an, dass sie dies in Österreich gar nicht beeinträchtige. Immerhin noch 49,2 Prozent gaben an, dass die Angst vor Terrorismus auch bei den Auslandsaktivitäten keinerlei Einfluss auf ihre Geschäfte habe.

Generell ist festzustellen, dass das Risiko eines Terroranschlags im Ausland zwar etwas höher eingestuft wird als in Österreich, aber dennoch nur in geringem Ausmaß. Nur 4,9 Prozent der Unternehmen gaben an, dass die Angst vor Terrorismus ihre Geschäftstätigkeit im Ausland sehr stark beinträchtige (Stufe 5 auf der Skala). Der weltweite Terrorismus wird als Risiko wahrgenommen, die Unternehmen sehen ihn aber nicht als ganz große Bedrohung an.

Wie stark beeinträchtigt die Angst vor Terrorismus Ihre Geschäftstätigkeiten? Bewerten Sie bitte auf einer Skala von 0 (= kein) bis 5 (= hoch)



GRAFIK 10

Quelle: Corporate Trust 2017

Dies wird bei Industriespionage verständlicherweise ein wenig anders gesehen. Die Bedrohung kann sowohl von Wettbewerbern, der Organisierten Kriminalität, ausländischen Nachrichtendiensten oder den eigenen Mitarbeitern ausgehen. Nur etwa ein Drittel der Unternehmen gab an, dass ihr Know-how durch Spionage oder Informationsabfluss durch Wettbewerber oder eigene Mitarbeiter gar nicht bedroht sei (Stufe 0 auf der Skala).

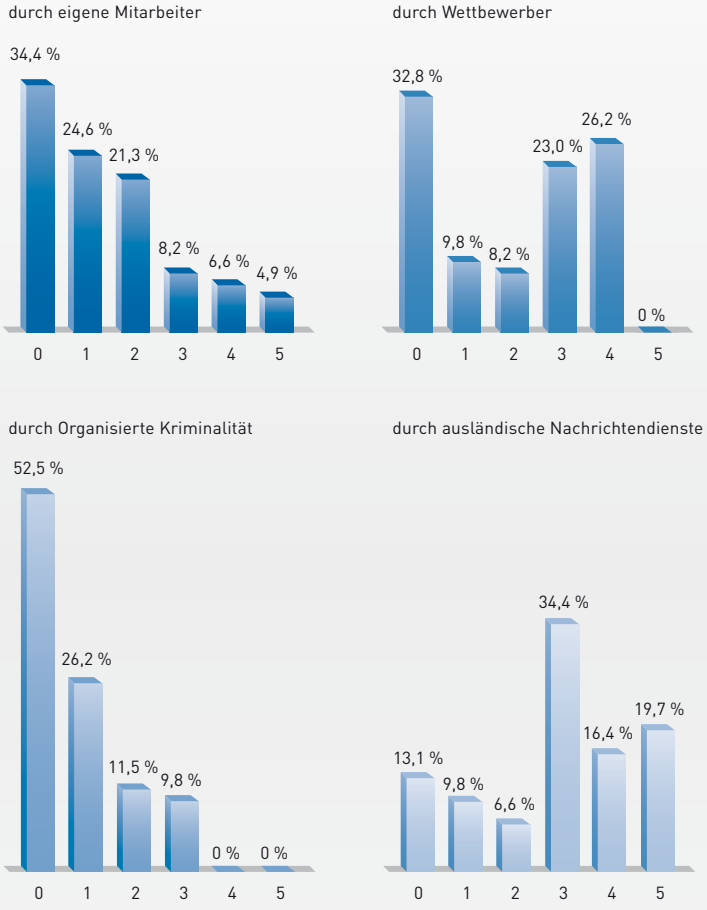
Die größte Bedrohung (Stufe 5 auf der Skala) geht nach Einschätzung der Unternehmen von den ausländischen Nachrichtendiensten (19,7 %) aus. Eine mittelhohe Bedrohung (Stufe 3 auf der Skala) für das Know-how des eigenen Unternehmens wird mit 34,4 Prozent ebenfalls den ausländischen Nachrichtendiensten zugeschrieben, gefolgt von der Bedrohung durch Wettbewerber (23,0 %) und die Organisierte Kriminalität (9,8 %).

BRAINLOOP

„Um sich gegen das moderne Raubrittertum zu wehren, müssen Firmen ihre Sicherheit stärken, sowohl in technischer Hinsicht als auch im Bewusstsein ihrer Mitarbeiter – nichts Geringeres als der Innovationsvorsprung der deutschen Hochtechnologiegesellschaft hängt davon ab."

Martin Ehling
Leiter Vertrieb Deutschland Industrie und Handel
Brainloop AG

Wie stark ist das Know-how Ihres Unternehmens durch die Gefahr von Spionage oder Informationsabflüssen bedroht? Bewerten Sie bitte auf einer Skala von 0 (= kein) bis 5 (= hoch)



GRAFIK 11

Quelle: Corporate Trust 2017

Kurzstudie

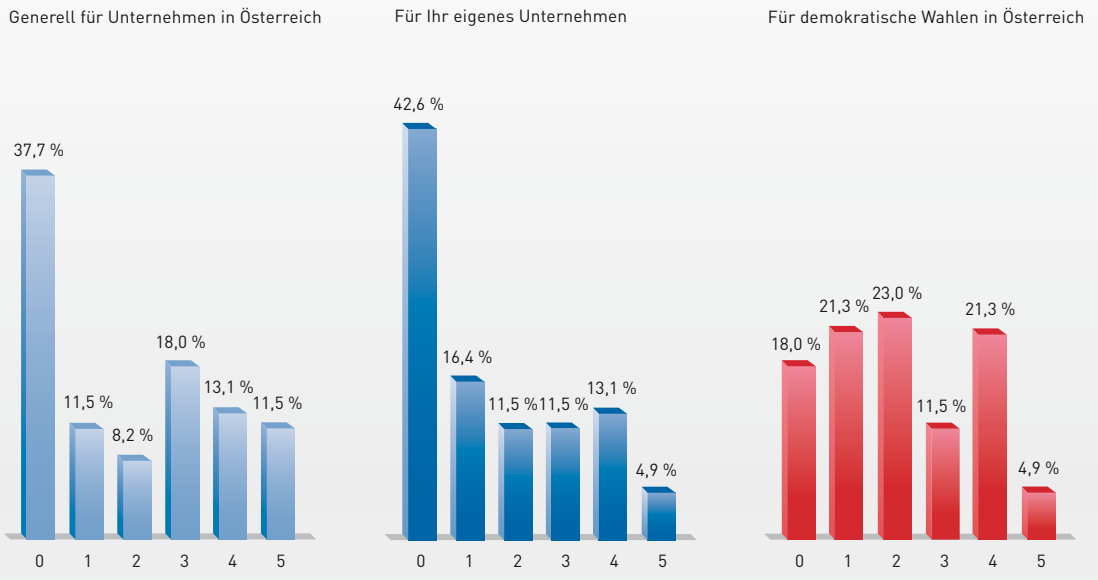
Risikobewertung für die Zukunft

Die öffentliche Meinungsbildung erfolgt überwiegend durch Medien, heute auch zunehmend durch soziale Netzwerke. Die Einflussnahme auf Inhalte, kritische Kommentare oder das „Faken" von Nachrichten wird immer einfacher. Dementsprechend wird die Meinungsbildung in Zukunft immer häufiger manipuliert werden. Sogenannte Fake News, Social Bots oder Trolle , über die massenhaft Kommentare oder Bewertungen im Internet generiert werden, stellen moderne Propaganda dar und können sich auch für Unternehmen schädigend auswirken.

Österreichische Firmen schätzen die Gefahr der Einflussnahme durch solche Propagandamaßnahmen für Unternehmen jedoch noch relativ gering ein. Etwa ein Fünftel, genau 18,0 Prozent, sehen in der Möglichkeit zur negativen Beeinflussung der öffentlichen Meinung ein mittleres Risiko (Stufe 3 auf der Skala) und nur 13,5 Prozent ein sehr hohes Risiko (Stufe 5 auf der Skala). Für ihr eigenes Unternehmen schätzen sie das Risiko sogar noch viel geringer ein. Nur 11,5 Prozent der Unternehmen sehen ein leicht erhöhtes oder mittleres Risiko (Stufen 2 und 3 auf der Skala) und nur 4,9 Prozent ein sehr hohes Risiko (Stufe 5 auf der Skala).

Fälle wie die vermutliche Beeinflussung des US-amerikanischen und französischen Wahlkampfs durch russische Hacker haben gezeigt, dass digitale Möglichkeiten heute bereits für Propaganda genutzt werden und eine solche Beeinflussung in Zukunft häufiger passieren könnte. Auch österreichische Firmen sehen dies so. Daher gaben 23,0 Prozent der Unternehmen an, dass sie eine leicht erhöhte Gefahr (Stufe 2 auf der Skala) der Einflussnahme durch Propagandamaßnahmen für demokratische Wahlen sehen. 21,3 Prozent meinten sogar, dass sie für die Zukunft eine relativ hohe Gefahr (Stufe 4 auf der Skala) durch derartige Praktiken vermuten.

Wie hoch bewerten Sie die Gefahr der Einflussnahme durch Propagandamaßnahmen auf die öffentliche Meinungsbildung? Bewerten Sie bitte auf einer Skala von 0 (= kein) bis 5 (= hoch)



GRAFIK 12

Quelle: Corporate Trust 2017

1) Als Troll bezeichnet man im Netzjargon eine Person, die ihre Kommunikation im Internet auf Beiträge beschränkt, die auf emotionale Provokation anderer Gesprächsteilnehmer zielt. Dies erfolgt mit der Motivation, eine Reaktion der anderen Teilnehmer zu erreichen.

Wenn immer mehr Menschen in die Städte ziehen und ländliche Regionen damit immer stärker verwaisen, kann dies zu ganz neuen Herausforderungen für die Kommunen und Problemen für die Unternehmen führen. Die Firmen wurden daher danach befragt, welche Herausforderungen sie durch die zunehmende Urbanisierung sehen.

Die überwiegende Mehrheit der Unternehmen (86,9 %) sah die Schwierigkeit, qualifizierte Mitarbeiter für Standorte in weniger attraktiven ländlichen Regionen zu finden, als größte Herausforderung an. Steigende Kriminalität wurde von 68,9 Prozent als mögliches Problem gesehen und 52,2 Prozent der Firmen gaben an, dass sie eine größere Gefahr für einen sozialen Abstieg sehen.

Lediglich 8,2 Prozent der Unternehmen glauben, dass die Urbanisierung keine Herausforderung für die Zukunft darstellt. Immerhin 47,5 Prozent glauben sogar, dass es zu sozialen Unruhen kommen könnte und 41,0 Prozent vermuten, dass Produktivitätseinbußen aufgrund der überlasteten Infrastrukturen die Wirtschaft negativ beeinflussen könnten.

Welche Herausforderungen sehen Sie durch die zunehmende Urbanisierung?
(Mehrfachnennungen möglich)

GRAFIK 13

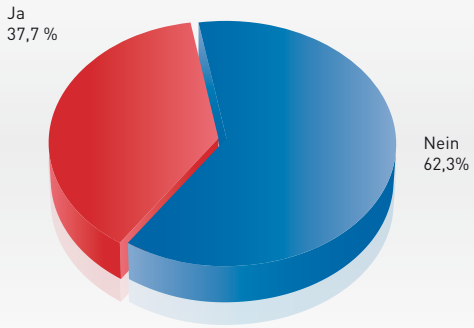
Quelle: Corporate Trust 2017

KURZSTUDIE

RISIKOBEWERTUNG FÜR DIE ZUKUNFT

Laut Migrationsbericht[1] der deutschen Bundesregierung wurden im Jahr 2015 genau 476.649 Asylanträge in Deutschland verzeichnet. Dies stellte einen Anstieg um 135 Prozent zum Vorjahr (202.834 Asylanträge in 2014) dar und bildet sogar nur die registrierten Zuwanderer ab. Darüber hinaus gab es auch eine ganze Menge von Migranten, die ohne behördliche Registrierung nach Deutschland einreisten. Auch für Österreich stellen die massenhaften Migrationsbewegungen ein Problem dar. In Verbindung mit der Angst vor unerkannt eingewanderten Terroristen oder den Berichten zu den Übergriffen am Kölner Hauptbahnhof in der Sylvesternacht 2015/2016, hat dies in Teilen der Gesellschaft zu einem Gefühl von Unwohlsein geführt. Österreichische Unternehmen bewerten das Risiko durch Migrationsbewegungen für ihr Unternehmen jedoch nicht sehr hoch. Nur ein Drittel, exakt 37,7 Prozent, gab an, dass sie hier ein Risiko sehen.

Sehen Sie die Migrationsbewegungen als zukünftiges Risiko für Ihr Unternehmen?



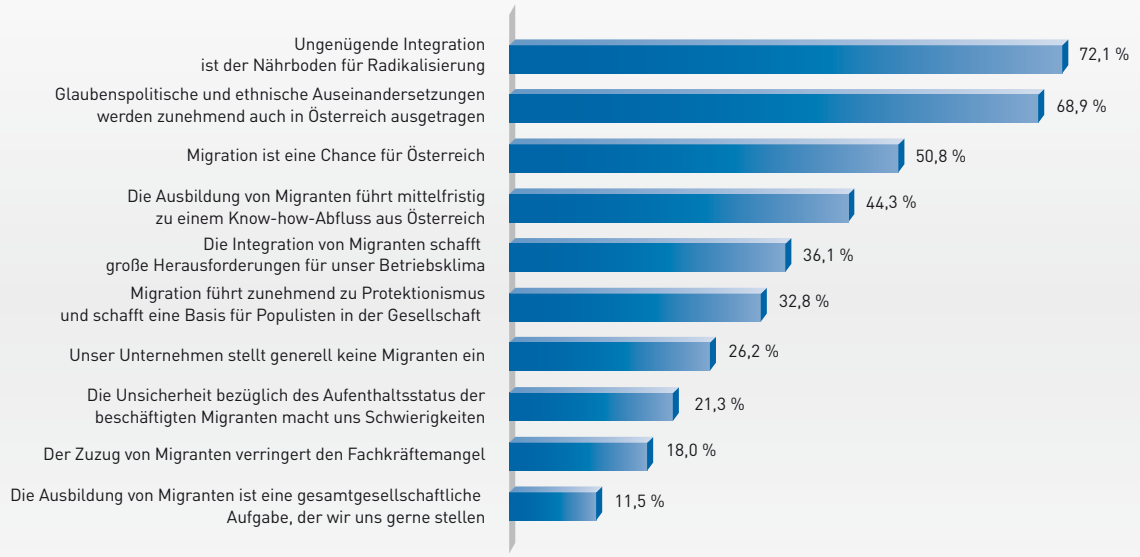
GRAFIK 14

Quelle: Corporate Trust 2017

1) https://www.bamf.de/SharedDocs/Anlagen/DE/Publikationen/Migrationsberichte/migrationsbericht-2015.pdf?__blob=publicationFile

Befragt nach den konkreten Herausforderungen, gaben 72,1 Prozent der Unternehmen an, dass sie eine ungenügende Integration als Nährboden für Radikalisierung sehen. Zwar finden 44,3 Prozent, dass die Ausbildung von Migranten eine gesamtgesellschaftliche Aufgabe ist, der sich auch ihr Unternehmen gerne stellt, aber 36,1 Prozent gaben an, dass die Integration von Migranten große Herausforderungen für ihr Betriebsklima schafft. 68,9 Prozent gehen sogar davon aus, dass glaubenspolitische oder ethnische Auseinandersetzungen zunehmend in Österreich ausgetragen werden. Bemerkenswert ist, dass nur etwa ein Viertel der Unternehmen (26,2 %) angaben, generell keine Migranten einzustellen.

Welchen der folgenden Aussagen stimmen Sie zu?
(Mehrfachnennungen möglich)



GRAFIK 15

Quelle: Corporate Trust 2017

Kurzstudie

Risikobewertung für die Zukunft

Die Digitalisierung schreitet mit großen Schritten voran, sowohl im Privat- als auch im Unternehmensbereich. Eine zunehmende Vernetzung von Produktionsmaschinen und Lieferketten sowie der Internetzugang für alle Gegenstände des täglichen Lebens schaffen jedoch nicht nur Möglichkeiten, sondern bergen auch Risiken in sich. Die Unternehmen wurden daher befragt, welche Gefahren sie durch Industrie 4.0 bzw. Internet of Things (IoT) sehen. Die Risikobewertung sollte immer allgemein für Österreich und dann konkret für ihr eigenes Unternehmen erfolgen.

85,2 Prozent sehen die Gefahr von Cyber-Terror als größte Bedrohungen für die österreichische Wirtschaft, gefolgt von der zunehmenden Abhängigkeit vom Internet (83,6 %). Immerhin noch knapp ein Drittel der Unternehmen (36,1 %) gehen davon aus, dass die technologischen Entwicklungen auch negative Konsequenzen für die Wirtschaft haben könnten.

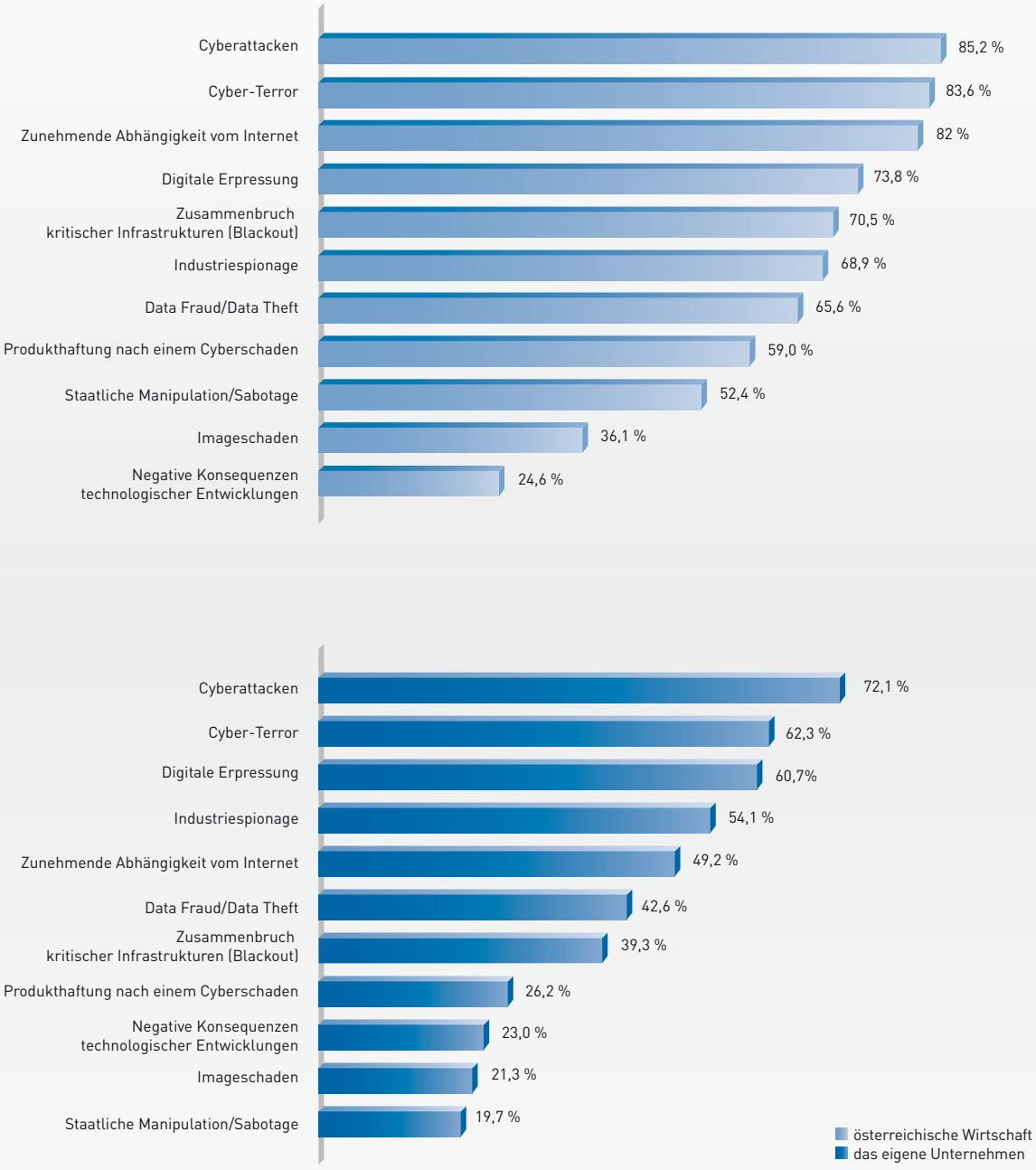
Die befragten Firmen schätzen die Bedrohung für ihr eigenes Unternehmen zwar durchwegs geringer ein als für die österreichische Wirtschaft allgemein, dass Cyberattacken bzw. Cyber-Terror die größte Bedrohung darstellen, sehen sie jedoch auch für ihr Unternehmen so. Die Risiken durch Industriespionage (54,1 %) und Data Fraud / Data Theft (42,6 %) sehen fast die Hälfte der Unternehmen als künftige Gefahren durch Industrie 4.0 bzw. Internet of Things.

BRAINLOOP

„Es bringt nichts, analoge Prozesse 1:1 in die die digitale Welt zu übertragen. Um einen maximalen Mehrwert zu liefern, müssen alle Prozesse geprüft und im Zweifelsfall neu aufgesetzt werden. Im Fokus sollten dabei die Kriterien Sicherheit, Kosteneffizienz und Leistung stehen."

Martin Ehling
Leiter Vertrieb Deutschland Industrie und Handel
Brainloop AG

Welche Gefahren sehen Sie durch Industrie 4.0 bzw. Internet of Things (IoT) für die österreichische Wirtschaft allgemein und konkret für Ihr Unternehmen?
(Mehrfachnennungen möglich)



GRAFIK 16

Quelle: Corporate Trust 2017

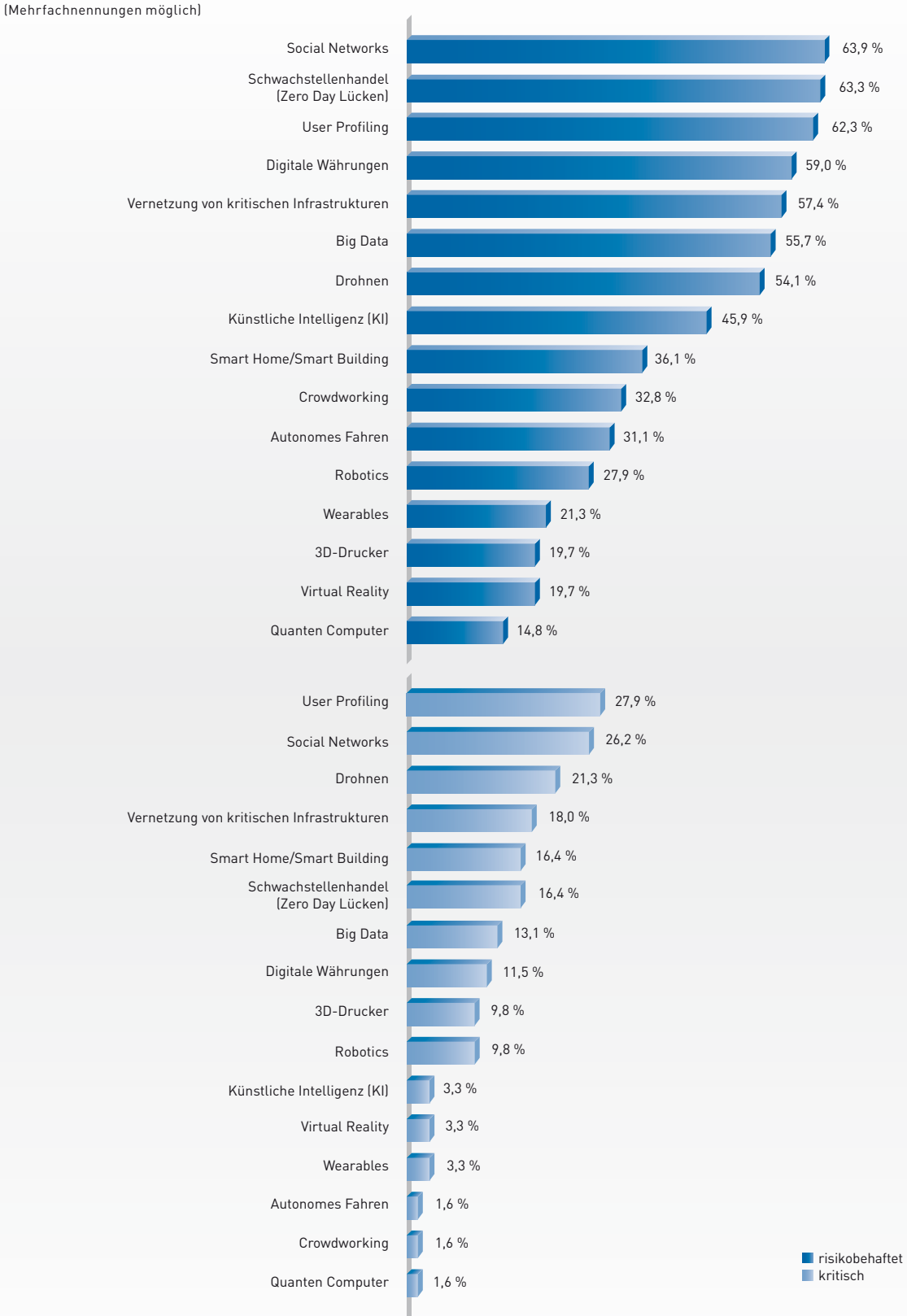
Kurzstudie

Risikobewertung für die Zukunft

Im Rahmen der Befragung wurde für die Bewertung des künftigen Risikos bei den Firmen erhoben, welche der neuen Technologien und Möglichkeiten der Digitalisierung für risikobehaftet oder sogar kritisch für ihr eigenes Unternehmen gehalten werden.

Über die Hälfte aller Unternehmen geht davon aus, dass Social Networks (63,9 %) und der Schwachstellenhandel mit Zero Day Lücken (63,3 %) risikobehaftet sind. Sogar der Einsatz von Virtual Reality und 3D-Druckern (beide 19,7 %) sowie Quanten Computern (14,8 %) ist nach Einschätzung der Unternehmen mit Risiken verbunden. Wirklich kritisch hingegen werden die neuen Technologien von den wenigsten Unternehmen gesehen. Exakt 27,9 Prozent halten das User Profiling für ein Problem für ihr eigenes Unternehmen und auch Drohnen werden von 21,3 Prozent für die Zukunft als möglicherweise kritisch eingeschätzt.

Welche der künftigen Technologien bzw. nachfolgenden Punkte bewerten Sie allgemein risikobehaftet oder sogar kritisch für Ihr Unternehmen?
(Mehrfachnennungen möglich)



GRAFIK 17

Quelle: Corporate Trust 2017

Kurzstudie

Risikobewertung für die Zukunft

Der Datenschutz ist ein wichtiges Gut in Europa. Allerdings macht das Internet keinen Halt an Landesgrenzen und vor allem im Hinblick auf die Digitalisierung und neue Technologien wird es zunehmend schwerer, Regulierungen umzusetzen, die nicht alle Internet-Teilnehmer gleichzeitig betreffen. Österreich ist ein Wirtschaftsstandort, der vor allem von Innovation und Erfindergeist lebt. Damit war die österreichische Wirtschaft im Zuge der Industrialisierung sehr erfolgreich. Wie sehr sind Innovationen und Erfindergeist jedoch noch möglich, wenn die Digitalisierung in Europa zu sehr reguliert wird, während in anderen Ländern der Welt die Möglichkeiten in vollem Umfang ausgeschöpft werden?

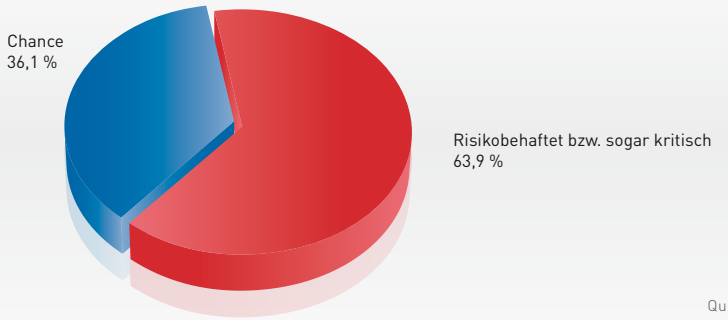
Nach ihrer Einschätzung zum Europäischen Datenschutzgesetz befragt, gaben 36,1 Prozent der Unternehmen an, dass sie dies als Chance sehen. Allerdings glauben 63,9 Prozent, dass dieses auch risikobehaftet bzw. kritisch für das eigene Unternehmen ist.

BRAINLOOP

„Die neue EU-Datenschutzgrundverordnung fördert einen lokalen Ansatz, wenn es um die Speicherung personenbezogener Daten geht. Der Serverstandort Deutschland alleine reicht nicht aus – ein Thema, das seit der Einführung des Patriot Act durch die US-Sicherheitsbehörden eine zentrale Bedeutung gewonnen hat."

Martin Ehling
Leiter Vertrieb Deutschland Industrie und Handel
Brainloop AG

Sehen Sie das Europäische Datenschutzgesetz als Chance oder eher risikobehaftet bzw. sogar kritisch für Ihr Unternehmen?



GRAFIK 18

Quelle: Corporate Trust 2017

Ich denke viel an die Zukunft, weil das der Ort ist,
wo ich den Rest meines Lebens verbringen werde.

Woody Allen

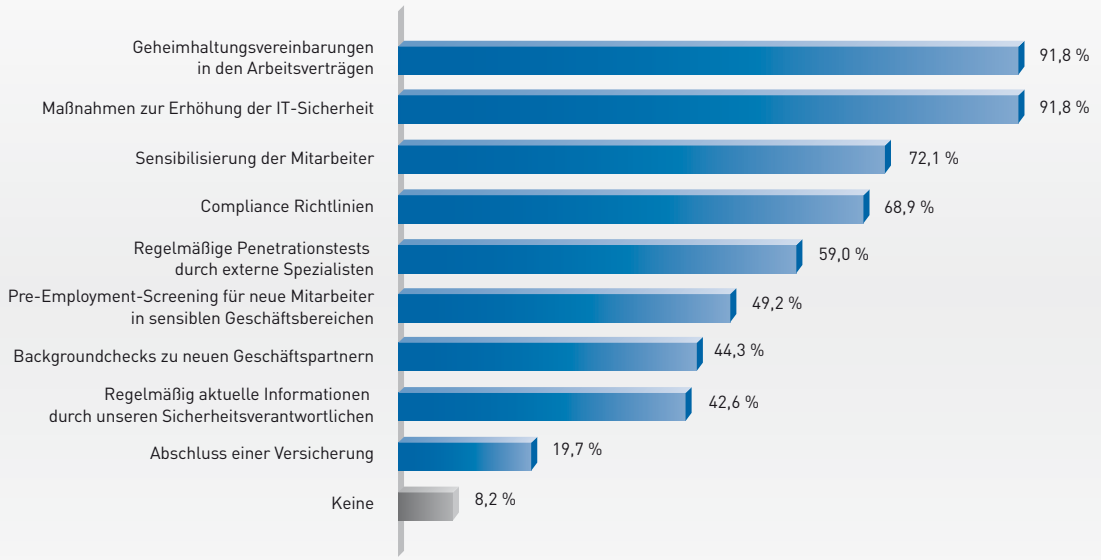
Kurzstudie

Präventive Massnahmen

Österreichische Unternehmen sind von vielerlei Sicherheitsrisiken bedroht. Sie haben bereits entsprechende Schäden und sehen auch ein deutlich steigendes Risiko für die Zukunft. Was tun sie eigentlich dagegen? Welche Sicherheitsmaßnahmen werden bereits getroffen, um Angriffe auf das Unternehmen abzuwehren? Um den Rahmen dieser Kurzstudie nicht zu sprengen, wurden nicht alle Maßnahmen abgefragt, sondern explizit zwei wesentliche Bereiche herausgegriffen und die Sicherheitsvorkehrungen für diese Bedrohungen erhoben. Dies war zum einen für das bereits sehr bekannte Risiko von Spionage bzw. Informationsabfluss und zum anderen für ein etwas neueres Thema, den Schutz gegen Propaganda in Form von öffentlichkeitswirksamen Falschmeldungen bzw. reputationsschädigenden Informationen.

Um gegen Industriespionage und Informationsabfluss geschützt zu sein, setzen fast alle Unternehmen auf Geheimhaltungsvereinbarungen in den Arbeitsverträgen (91,8 %) sowie eine Erhöhung der IT-Sicherheit (91,8 %). Immerhin noch die überwiegende Mehrheit schützt sich auch mit einer Sensibilisierung der Mitarbeiter (72,1 %) und entsprechenden Compliance Richtlinien im Unternehmen (68,9 %). Leider finden es bisher nur 19,7 Prozent der österreichischen Unternehmen wichtig, auch eine Versicherung für solche Vorfälle abzuschließen, zum Beispiel eine Cyber-Polizze für Hackerangriffe oder eine Vertrauensschadenversicherung für den Fall, dass eigene Mitarbeiter kriminell werden und die Daten verkaufen.

Welche Sicherheitsvorkehrungen hat Ihr Unternehmen zum Schutz vor Spionage oder Informationsabfluss getroffen?
(Mehrfachnennungen möglich)

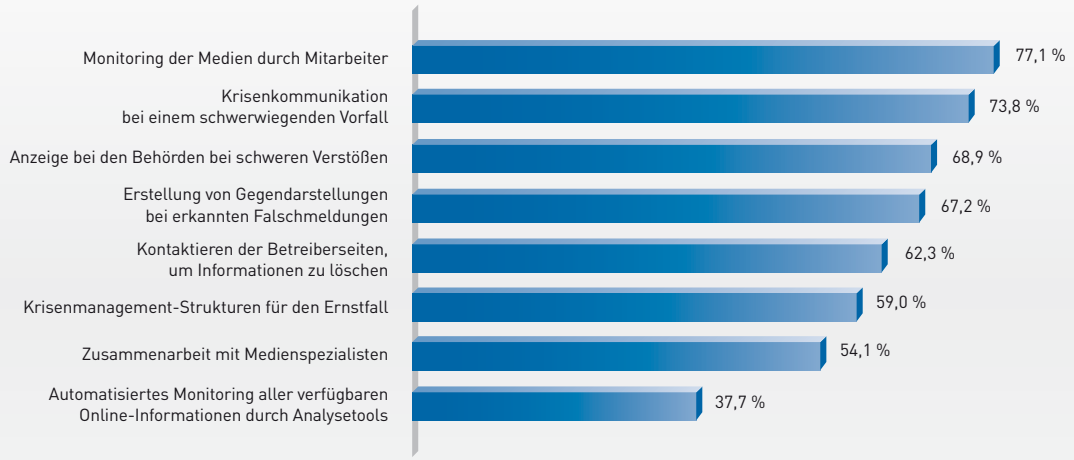


GRAFIK 19

Quelle: Corporate Trust 2017

Für das Risiko, durch Fake News oder reputationsschädigende Informationen einen Nachteil für das Unternehmen zu erleiden, ist die österreichische Wirtschaft anscheinend überraschend gut aufgestellt. 77,1 Prozent gaben an, bereits ein Monitoring der Medien durch eigene Mitarbeiter zu betreiben. Sollte es tatsächlich zu einem schweren Verstoß kommen, zeigen 68,9 Prozent diesen Vorfall an und 73,8 Prozent haben sich sogar bereits Gedanken dazu gemacht, wie bei einem schwerwiegenden Vorfall die Krisenkommunikation durchzuführen wäre. Dies macht Hoffnung, dass österreichische Unternehmen bei manipulierten Informationen nicht einfach tatenlos zusehen müssen, sondern bereits erkannt haben, was die Zukunft bringt und dementsprechend schnell mit präventiven Maßnahmen reagiert haben.

Mit welchen Maßnahmen schützen Sie Ihr Unternehmen gegen öffentlichkeitswirksame Falschmeldungen oder reputationsschädigende Informationen?
(Mehrfachnennungen möglich)



GRAFIK 20

Quelle: Corporate Trust 2017


-INTERNET
-LIVE CHAT
-MEDIA
-PHOTOS
-VIDEOS
-MUSIC
EUROPE
USA
-VIDEO
-FILMS
-SEARCH
-CONTACTS
-MESSAGES
-CREATIVE
-TUTORIALS
-INVESTMENT
-NETWORKING

Risk Maps 2017

Erklärung zur Herangehensweise

Corporate Trust gibt seit 2015 jedes Jahr Risk Maps zur aktuellen Sicherheitslage in der Welt heraus. Evaluiert werden dabei vier Hauptrisiken: Krisen & Konflikte, Informationsabfluss, Investitionssicherheit und Medizinische Risiken. Für die Erstellung der Risk Maps werten unsere Experten weltweit veröffentliche Datenbanken und Statistiken aus.

Anhand verschiedener Kriterien erfolgt dann die Einstufung der Länder für jedes Hauptrisiko in vier Risikostufen:

- Geringes Risiko
- Erhöhtes Risiko
- Hohes Risiko
- Sehr hohes Risiko

Bei der Einstufung geringes Risiko sind Geschäftstätigkeit und Reisen in das betreffende Land ohne besondere Schutzmaßnahmen möglich. Es sollten dennoch Strukturen und Prozesse für einen Notfall etabliert werden.

Gilt für das Land die Einstufung erhöhtes Risiko, sollten Reisende vor Antritt der Reise zumindest eine Schulung zum sicherheitsgerechten Verhalten im Ausland absolvieren.

Bei einem hohen Risiko sollten Reisen nur nach vorheriger Sicherheitsprüfung durchgeführt und besondere Schutzmaßnahmen festgelegt werden.

Gilt für ein Land ein sehr hohes Risiko, sollten Reisen auf das Nötigste beschränkt werden. Ist ein Aufenthalt in solchen Ländern unumgänglich, empfehlen wir, nur mit Unterstützung durch professionelle Sicherheitspartner dorthin zu reisen, zum Beispiel mit Personenschutz oder besonders ausgestatteten Fahrzeugen.

Für die Einstufung von Ländern in den Risk Maps werden zu den vier Hauptrisiken jeweils 3 bis 4 Variablen herangezogen (siehe unten). Die Bewertung der Gefährdung erfolgt anhand einer Risikoeinstufung der einzelnen Variablen von Grün (= kein oder nur geringes Risiko) bis Rot (= sehr hohes Risiko).

Hier eine Übersicht über die vier Hauptrisiken und die dazugehörigen Variablen:

Krisen & Konflikte
- Bewaffneter Konflikt[1]
- Zivile Unruhen[2]
- Terrorismus[3]
- Kriminalität[4]

Informationsabfluss
- Gefahr durch Verlust von IT-Geräten[5]
- IT-Risiko durch staatliche Spionage[6]
- IT-Risiko durch private Infobeschaffung[7]

Investitionssicherheit
- Rechtssicherheit[8]
- Korruption[9]
- Fraud[10]

Medizinische Risiken
- Infektionskrankheiten[11]
- Hygiene[12]
- Behandlungsstand[13]
- Medizinische Infrastruktur[14]

Dabei gilt für Krisen & Konflikte sowie Informationsschutz, dass der Maximalwert einer Variablen die Gesamteinstufung eines Landes bestimmt. Wenn ein Land also ein sehr hohes Terrorismus-Risiko aufweist, heißt das, dass die Gesamteinstufung für Krisen & Konflikte in dem Land bei Rot für sehr hohes Risiko liegen würde.

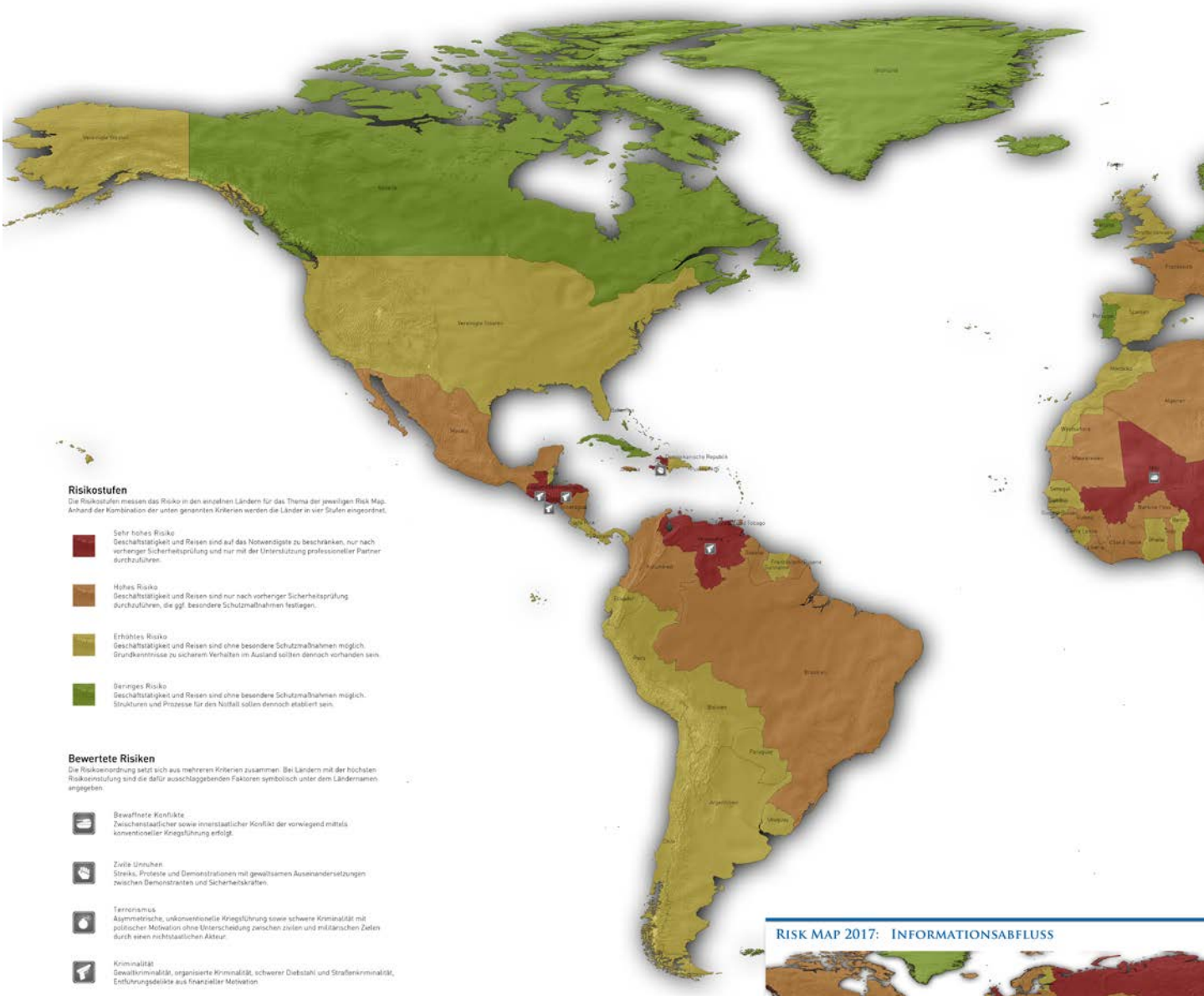
Für Investitionssicherheit und Medizinische Risiken gilt, dass der Durchschnittswert der Variablen die Gesamteinstufung eines Landes bestimmt. Wenn ein Land also ein geringes Risiko für Korruption, jedoch ein hohes Risiko bei der Rechtssicherheit hätte, wäre die Gesamteinstufung für Investitionssicherheit bei Gelb für erhöhtes Risiko.

Nähere Informationen zu den Risk Maps finden Sie auch unter: www.corporate-trust.de/de/portfolio/risk-map

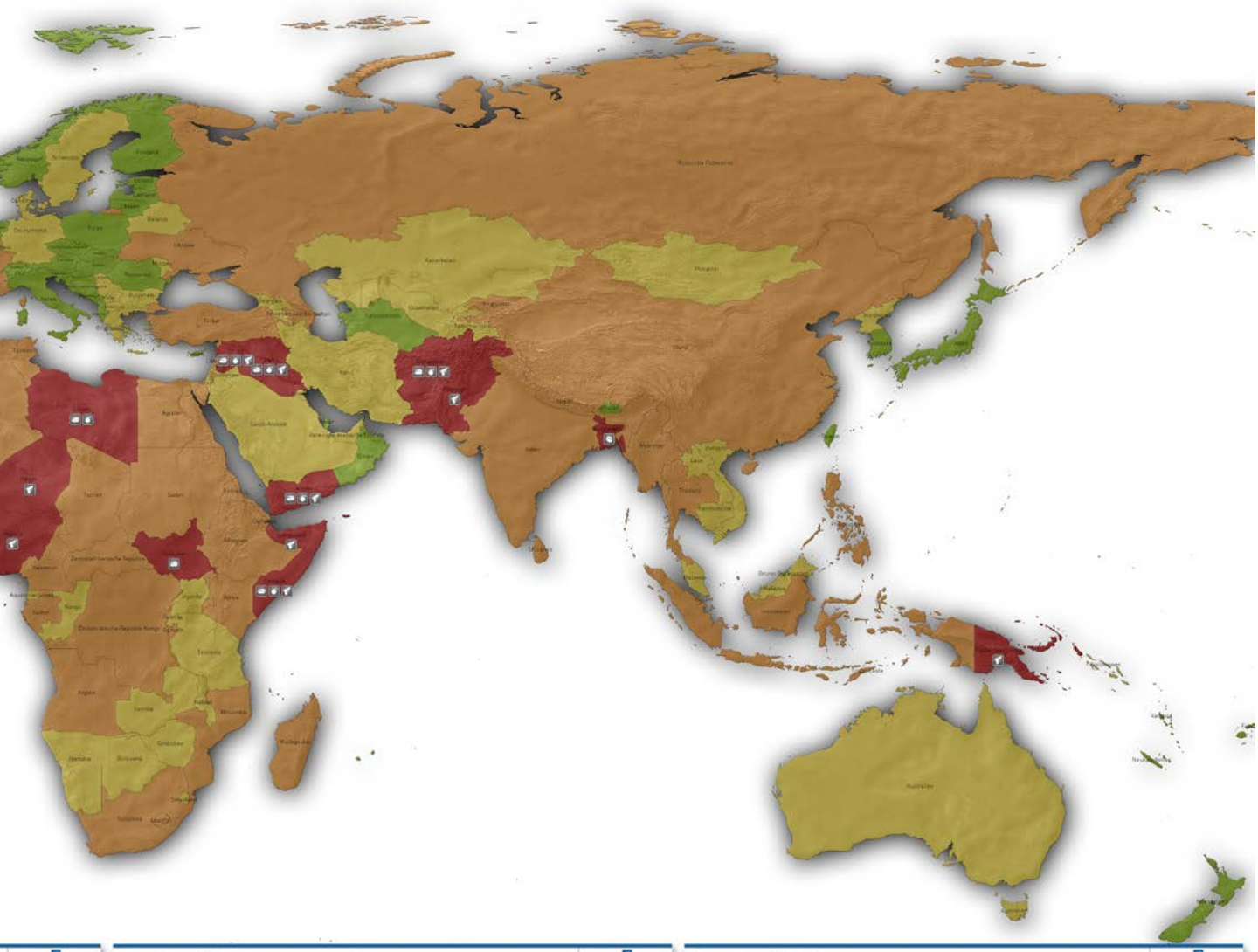
1) Zwischenstaatlicher oder innerstaatlicher Konflikt, der vorwiegend mittels konventioneller Kriegsführung erfolgt.
2) Streiks, Proteste und Demonstrationen mit gewaltsamen Auseinandersetzungen zwischen Demonstranten und Sicherheitskräften.
3) Asymmetrische, unkonventionelle Kriegsführung sowie schwere Kriminalität mit politischer Motivation durch einen nichtstaatlichen Akteur, ohne Unterscheidung zwischen zivilen und militärischen Zielen.
4) Gewaltkriminalität, organisierte Kriminalität, schwerer Diebstahl und Straßenkriminalität sowie Entführungsdelikte aus finanzieller Motivation.
5) Erpressung mit Daten von gestohlenen oder verlorenen IT-Geräten bzw. Datenträgern oder Weiterverkauf dieser Daten an Konkurrenten oder sonstige Drittverwerter.
6) Staatlich finanzierte Informationsbeschaffungsmaßnahmen, geheimdienstliche Wirtschaftsspionage, Überwachung von Internet, Mobilfunk und andere Kommunikation durch staatliche Stellen.
7) Industriespionage durch Konkurrenten, Ausspähung durch Detekteien und privatwirtschaftliche Auskunftsdienste sowie Informationsweitergabe an private Stellen durch Vetternwirtschaft und Korruption.
8) Unabhängigkeit der Gerichte und bestehende Grundrechte der Bürger.
9) Bestechung und Vorteilsnahme auf allen hierarchischen Ebenen in Politik, öffentlicher Verwaltung und Justiz.
10) Betrug, Untreue und Unterschlagung durch Mitarbeiter in privatwirtschaftlichen Unternehmen.
11) Infektionsgefahr durch bakterielle oder virale Erreger, Vorherrschen von Infektionskrankheiten wie Malaria, Dengue-Fieber, Japanische Enzephalitis, Durchfallerkrankungen und Cholera, Hepatitis A und B, Meningokokken, Typhus, Tollwut u.a.
12) Sauberkeit, Verwendung von Desinfektionsmitteln, Händedesinfektion sowie Sterilität in den Krankenhäusern.
13) Vergleich mit internationalen Behandlungsstandards, Ausbildungsstand von Ärzten und anderem medizinischem Personal.
14) Qualität und Verfügbarkeit apparativer Möglichkeiten zur Diagnostik und Therapie der üblichen Krankheiten, z.B. CT-Messplatz oder spezielle sterile Operationsutensilien.

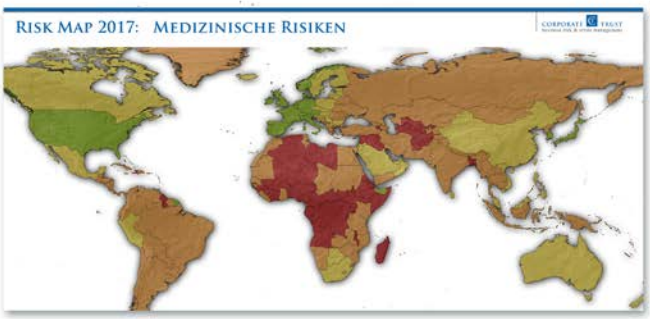
Risk Map 2017

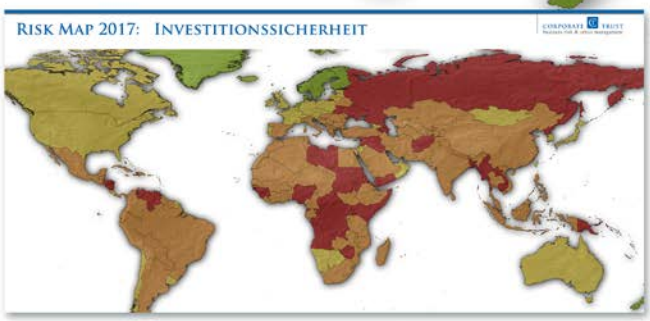
KRISEN & KONFLIKTE



Corporate Trust bietet mehr Sicherheit für Unternehmen im Ausland, von Risikoanalysen über Tracking-Lösungen, IT-Security, Due Diligence bis zur Unterstützung vor Ort. Dabei werden sämtliche Risiken betrachtet, die Reisende, Ihr Projekt und Ihr Unternehmen beeinträchtigten: Terrorismus, gesundheitliche Risiken, Korruption oder Industriespionage. Zudem bietet Corporate Trust mit „Global Business Security" eine Paketlösung für mittelständische Unternehmen im Bereich Auslands- bzw. Reisesicherheit "Made in Germany". Mehr unter: www.corporate-trust.de oder +49 89 599 88 75 80.

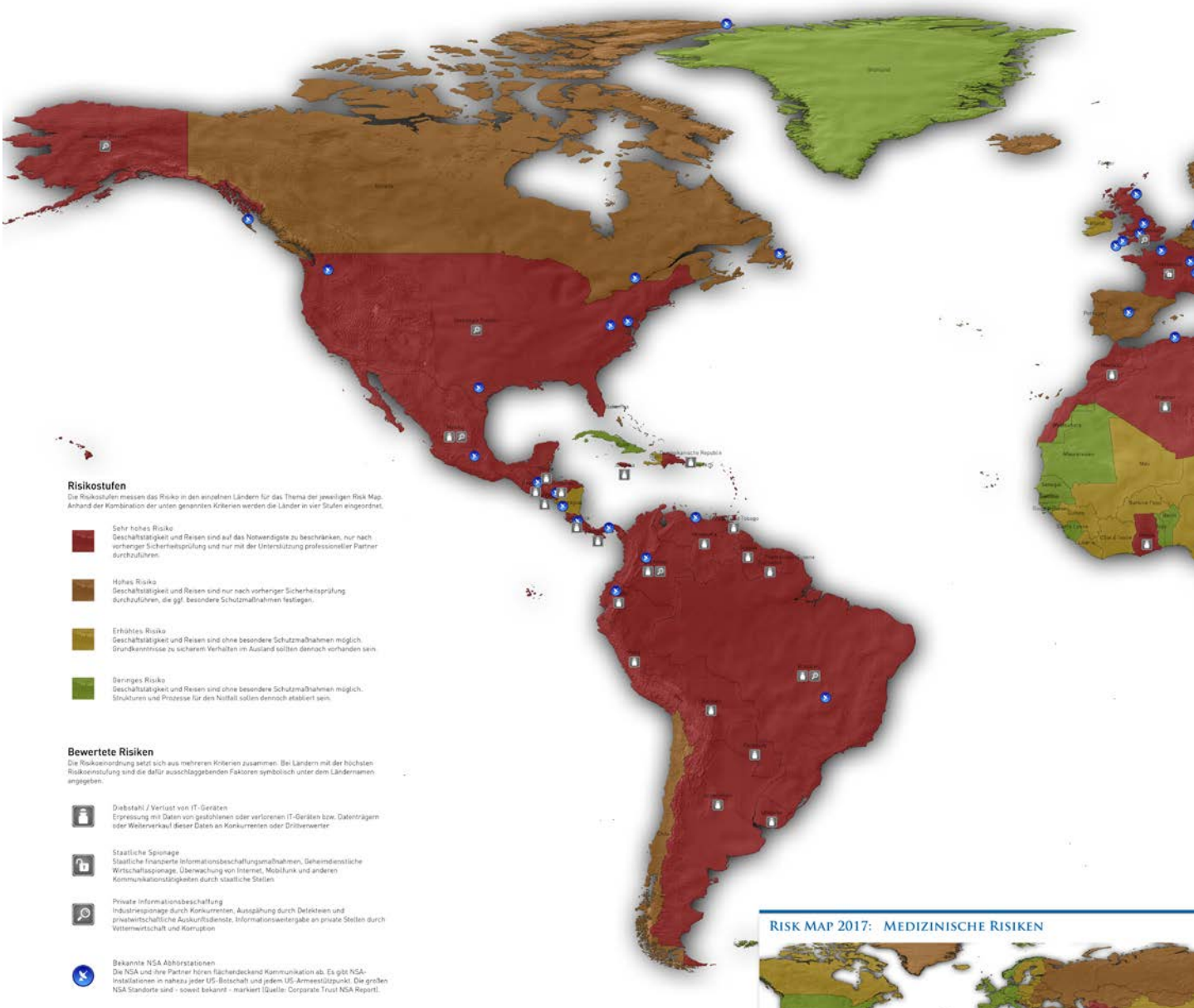



Risk Map 2017: Medizinische Risiken

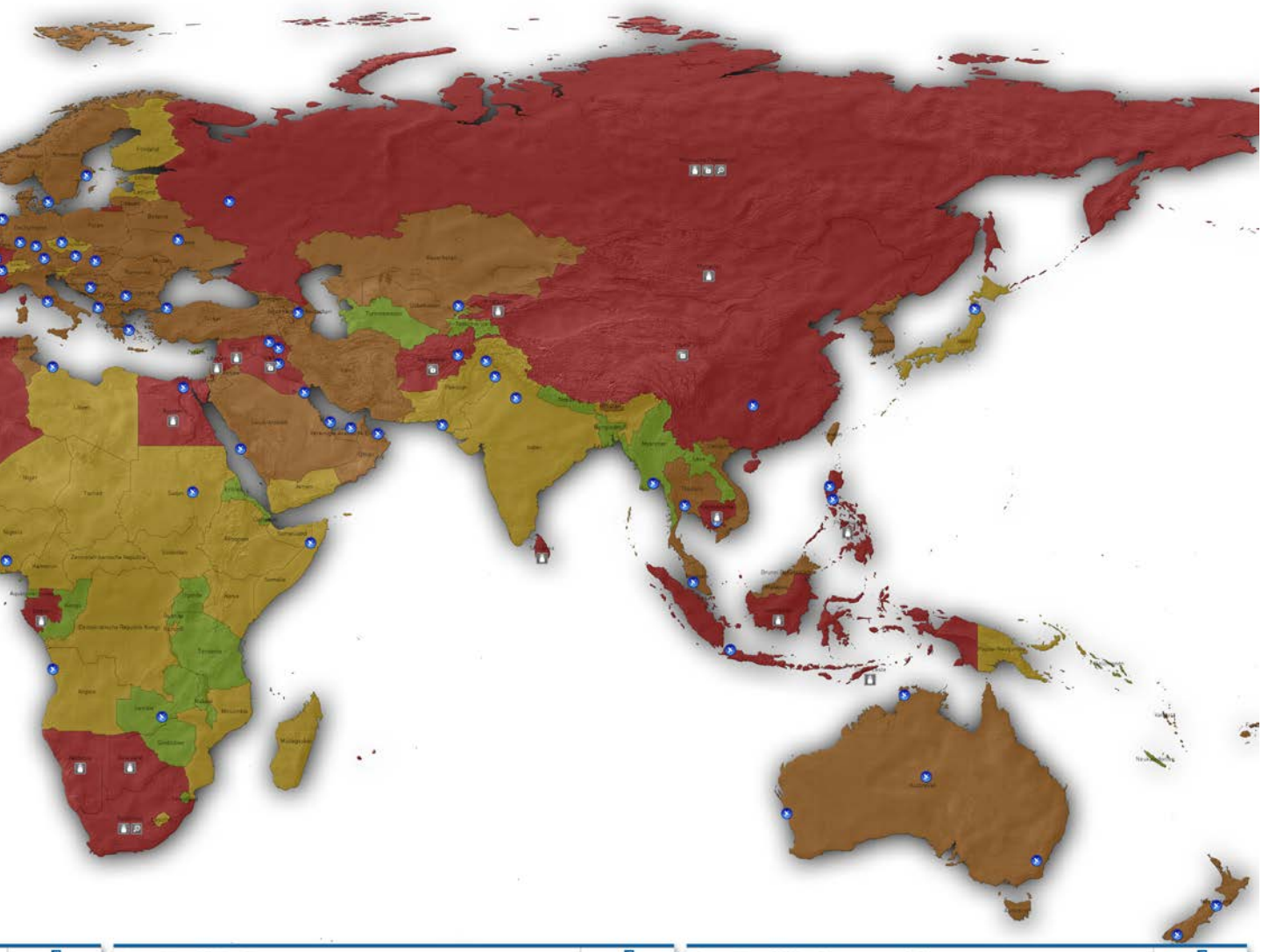

Risk Map 2017: Investitionssicherheit

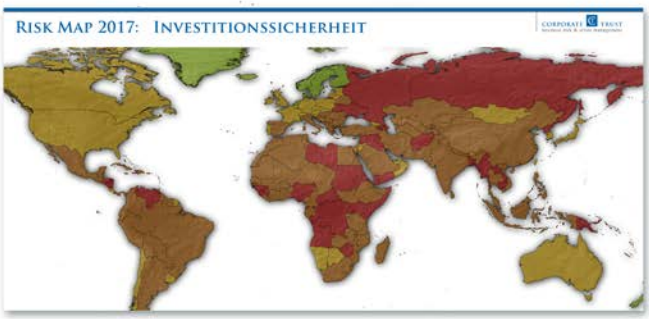
Risk Map 2017

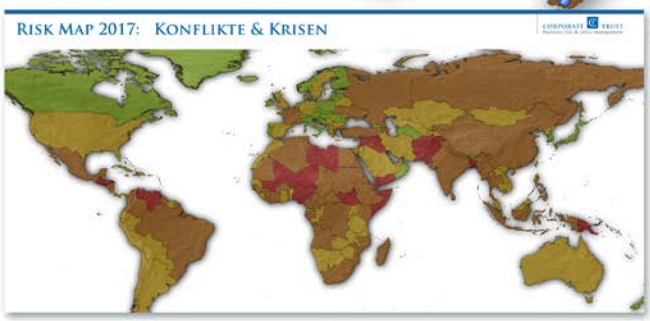
INFORMATIONSABFLUSS



Corporate Trust bietet mehr Sicherheit für Unternehmen im Ausland, von Risikoanalysen über Tracking-Lösungen, Cyber-Security, Due Diligence bis zur Unterstützung vor Ort. Dabei werden sämtliche Risiken betrachtet, die Reisende, Ihr Projekt und Ihr Unternehmen beeinträchtigten: Terrorismus, gesundheitliche Risiken, Korruption oder Industriespionage. Mit „Global Business Security" bietet Corporate Trust eine Paketlösung für Auslandsicherheit "Made in Germany" an, mit dem „Cyber Response Team" eine 24/7 Hotline für Cybersecurity. Mehr unter: www.corporate-trust.de oder +49 89 599 88 75 80.

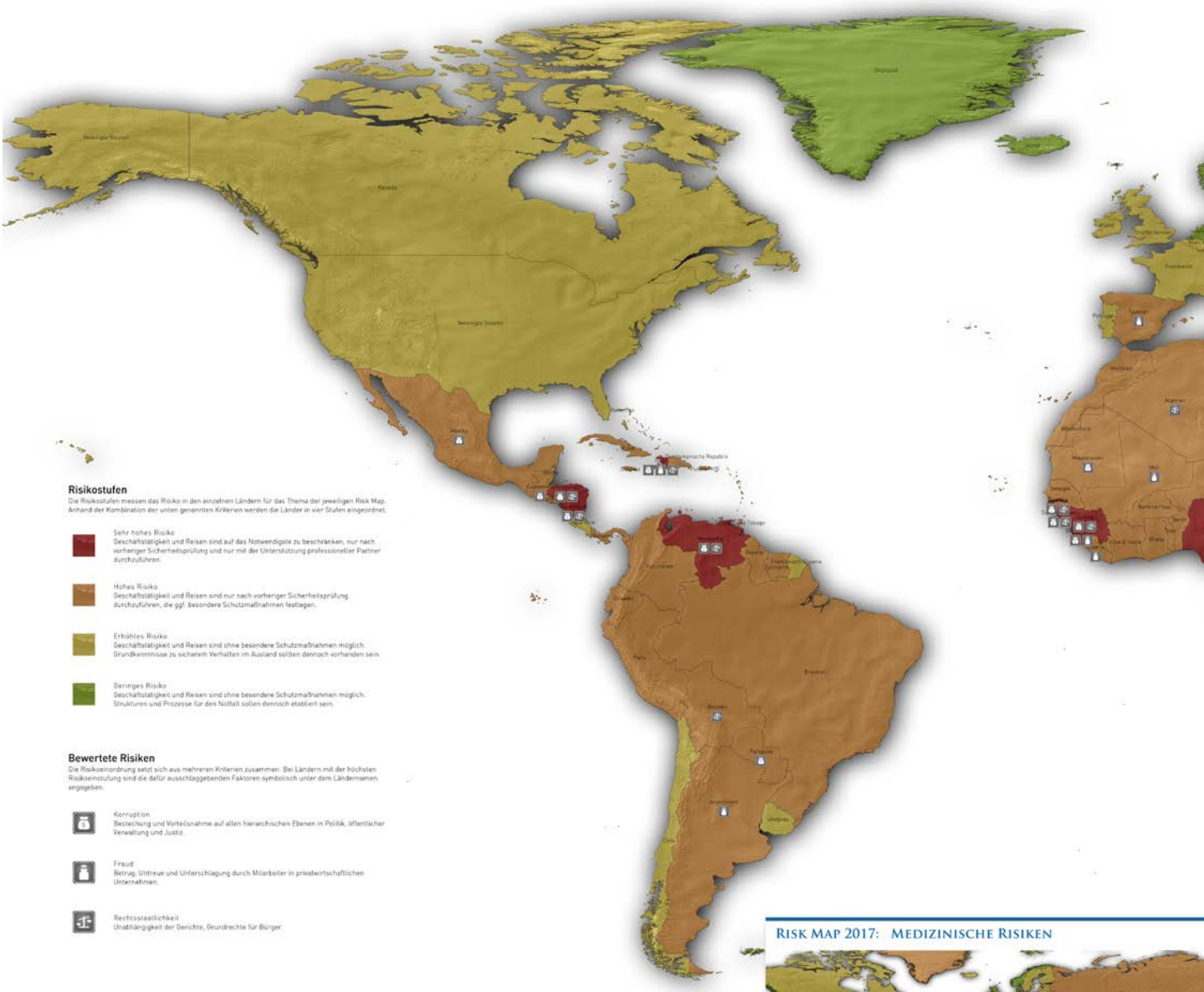


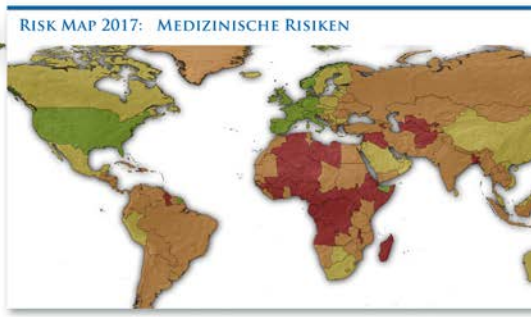

RISK MAP 2017: INVESTITIONSSICHERHEIT


RISK MAP 2017: KONFLIKTE & KRISEN

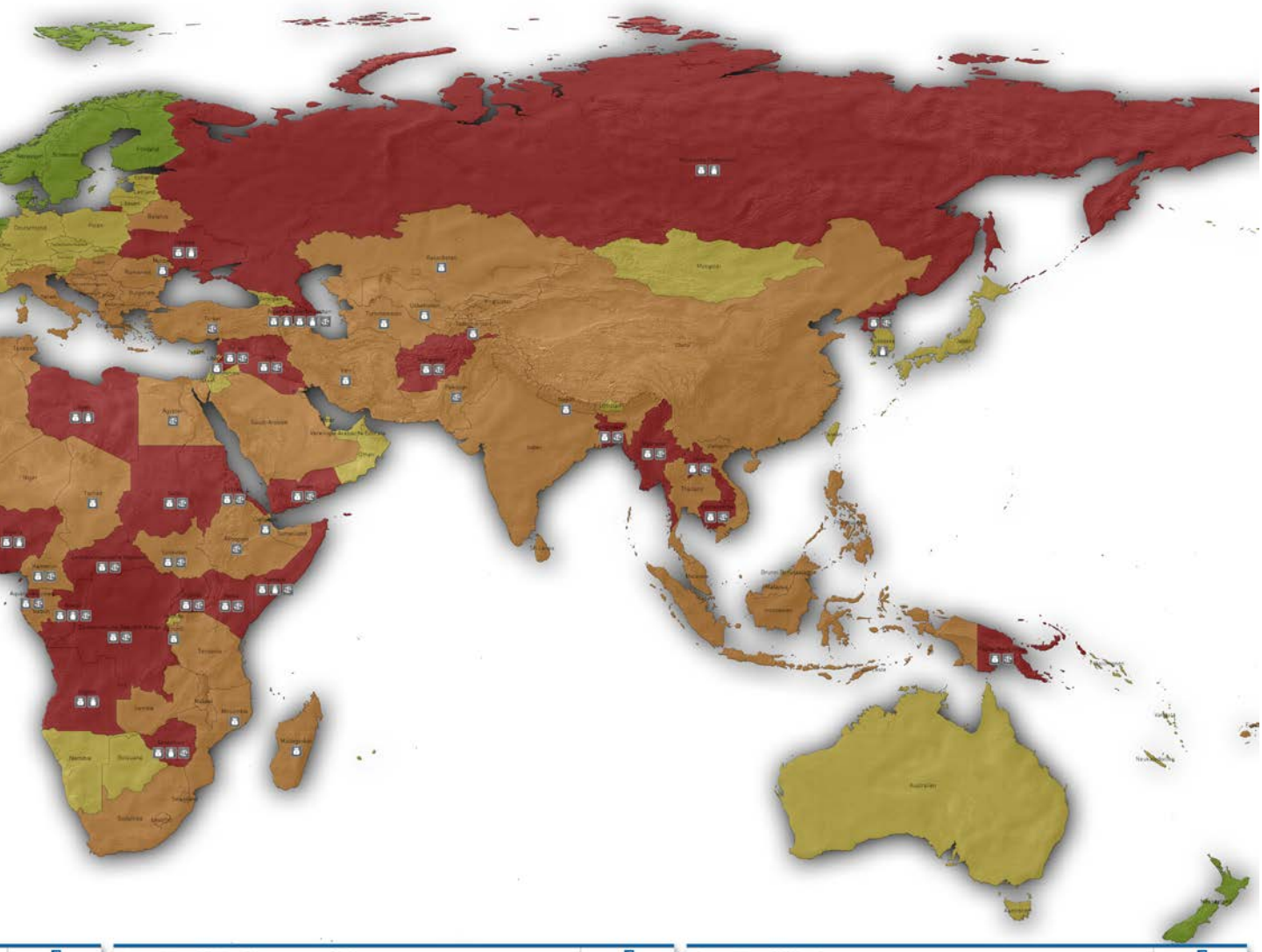
Risk Map 2017

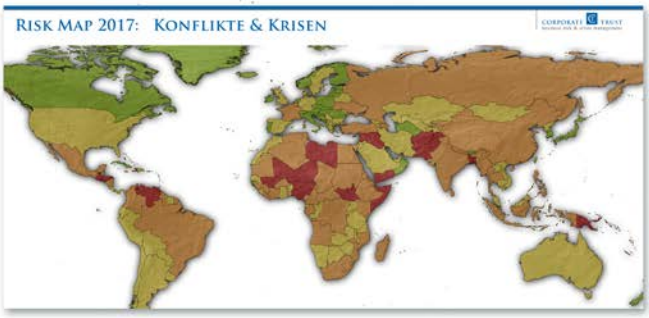
INVESTITIONSSICHERHEIT

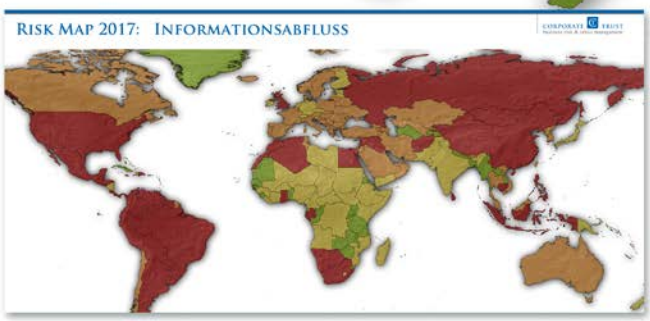




Corporate Trust bietet mehr Sicherheit für Unternehmen im Ausland, von Risikoanalysen und Tracking-Lösungen, über IT-Security und Due Diligence bis zur Unterstützung vor Ort. Dabei werden sämtliche Risiken betrachtet, die die Sicherheit Ihres Projektes und Ihres Unternehmens im Ausland gefährden können: Korruption, Wirtschaftskriminalität, Spionage, mangelnde Rechtstaatlichkeit, Gesundheitsrisiken und Terrorismus. Zudem bietet Corporate Trust mit „Business Risk Diligence" eine Paketlösung für Unternehmen im Bereich Risiko-Minimierung "Made in Germany" an. Mehr unter: www.corporate-trust.de oder +49 89 599 88 75 80.

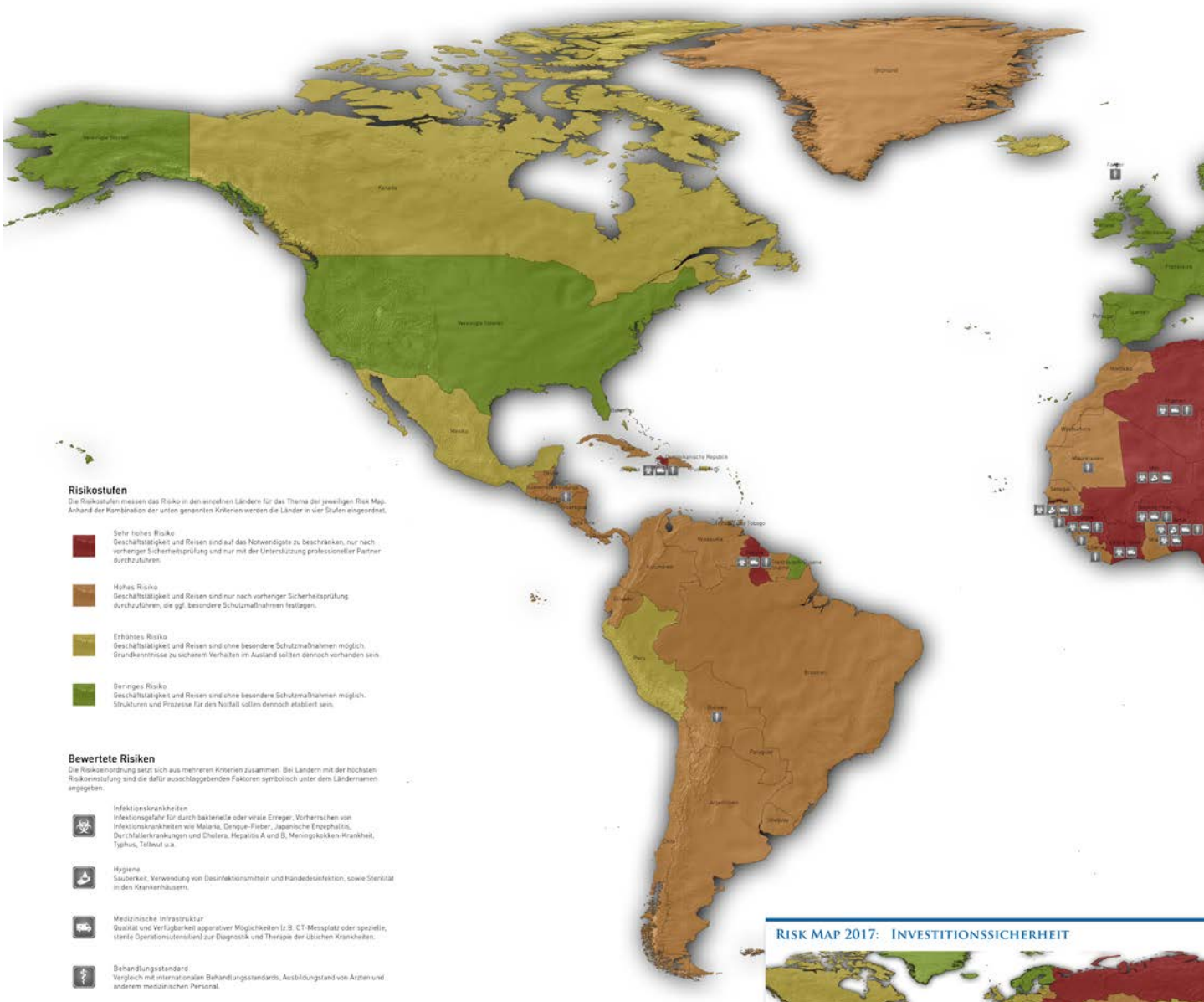



RISK MAP 2017: KONFLIKTE & KRISEN

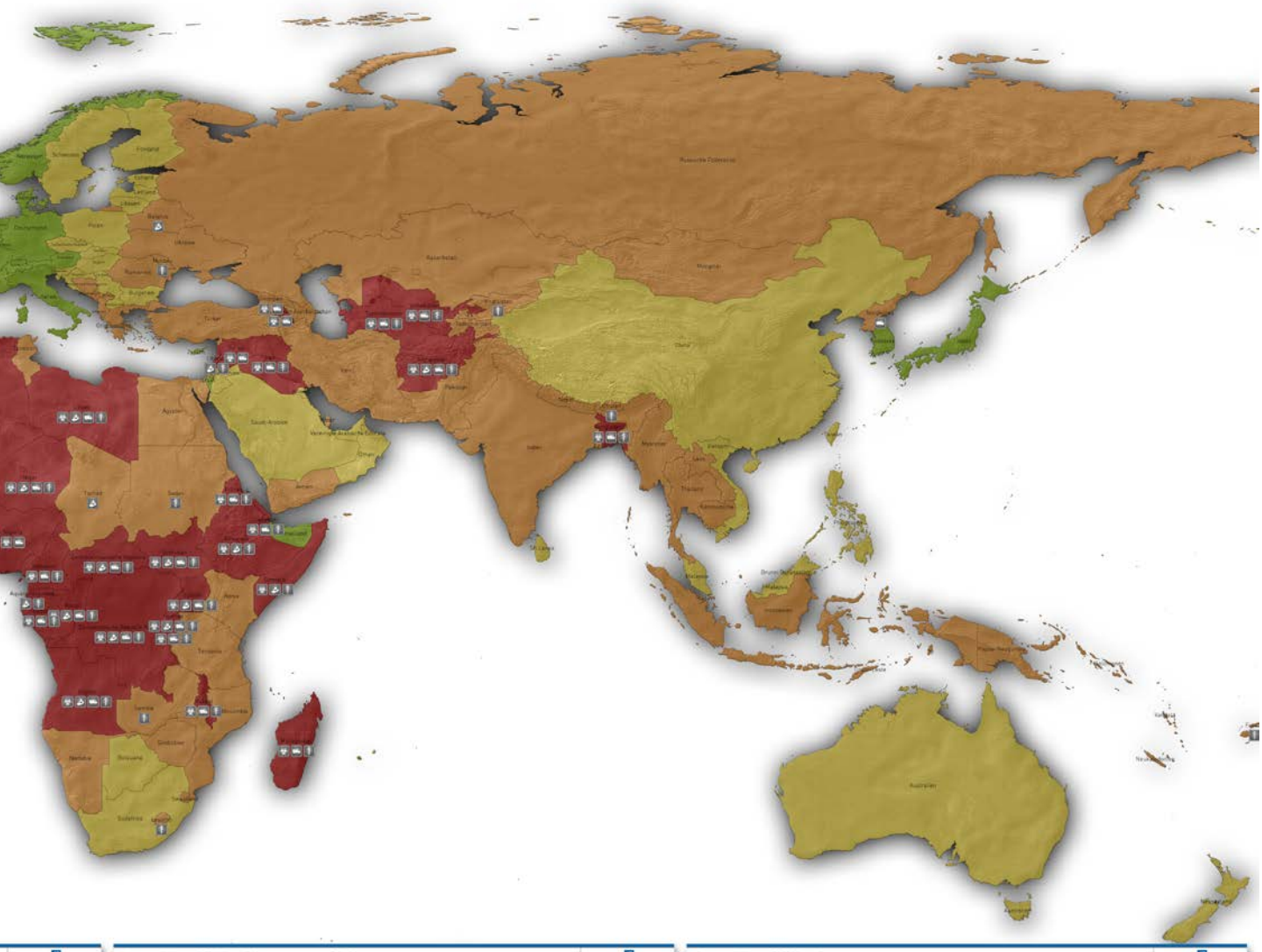

RISK MAP 2017: INFORMATIONSABFLUSS

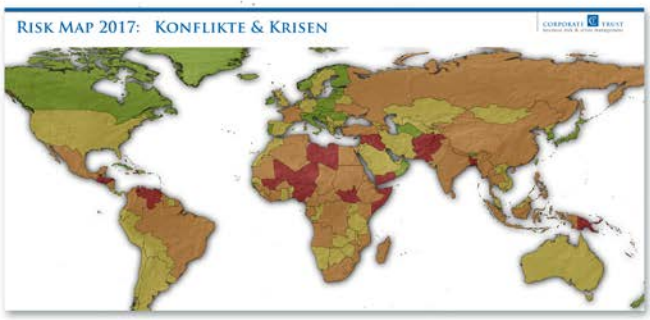
Risk Map 2017

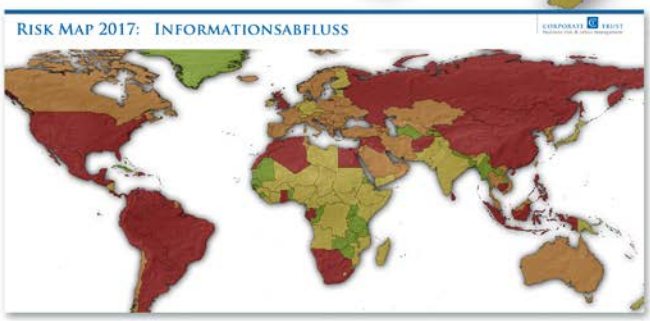
Medizinische Risiken



Corporate Trust bietet mehr Sicherheit für Unternehmen im Ausland, von Risikoanalysen über Tracking-Lösungen, IT-Security, Due Diligence bis zur Unterstützung vor Ort. Dabei werden sämtliche Risiken betrachtet, die Reisende, Ihr Projekt und Ihr Unternehmen beeinträchtigten: Terrorismus, gesundheitliche Risiken, Korruption oder Industriespionage. Zudem bietet Corporate Trust mit „Global Business Security" eine Paketlösung für mittelständische Unternehmen im Bereich Auslands- bzw. Reisesicherheit "Made in Germany". Mehr unter: www.corporate-trust.de oder +49 89 599 88 75 80.




RISK MAP 2017: KONFLIKTE & KRISEN


RISK MAP 2017: INFORMATIONSABFLUSS


INDUSTRIAL ESPIONAGE
INVESTMENT RISKS
WHISTLEBLOWER
FRAUD
SOCIAL ENGI
MEGACITIES
URBANISATION
GLOBALISATION
HOMELAND SECURITY
SPYWARE
NSA
DRONES
INDUSTRIAL ESPIONAGE
INVESTMENT RISKS
CRISIS MANAGEMENT
WHISTLEBLOWER
FRAUD
SOCIAL ENGINEERING
MIGRATION
REFUGEES
TERRORISM
BORDER CONTROL
//SCAN NETWORK
SPYWARE
NSA
DRONES
HACKER ATTACKS
INTERNET 4.0
BIG DATA
CLOUD
FUTURE
HOMELAND SECURITY
EMPT FAILED
MIGRATION
HACKER ATTACKS
INTERNET 4.0
REFUGEES
BORDER CONTROL
BIG DATA
CLOUD
USER SAFE
INTERNET OF THINGS
MEGACITIES
URBANISATION
CYBERWAR
TERRORISM
VIOLENT DEMONSTRATION
WAR
CONFLICTS
CORRUPTION
POLITICAL UNREST
MILITANT ACTS

Sicherheitstrends der Zukunft

Erklärung zur Herangehensweise

Die weltweite Sicherheitslage verändert sich. Um für künftige Herausforderungen gerüstet zu sein, empfiehlt es sich, regelmäßig einen Blick in die Zukunft zu wagen. Und zu fragen, auf welche Bedrohungen man sich schon heute einstellen muss. Natürlich kann niemand genau vorhersagen, welche Risiken uns in 5, 10 oder 15 Jahren tatsächlich erwarten. Aber eine Vorausschau ist in gewissen Grenzen möglich. Dabei hilft ein Blick auf die Bedrohungsfälle der Vergangenheit und die Bewertung der aktuellen Entwicklungen.

Um die wichtigsten Sicherheitstrends der Zukunft zu identifizieren, haben wir den umfassenden Risikobericht des World Economic Forum[1] herangezogen, den Global Risks Report 2017[2]. Dieser Report führt eine Reihe von Risikotrends für die kommenden Jahre an. Mehr noch: Er zeigt, in welcher Verbindung und Abhängigkeit sie voneinander stehen. Im Report finden sich so verschiedene Themen wie Soziale Instabilität, Urbanisierung, Klimawandel, Krieg und politische Unruhen, radikaler Islamismus oder Einkommensdisparität.

Corporate Trust hat gemeinsam mit dem Bayerischen Verband für Sicherheit in der Wirtschaft e.V. (BVSW) und der Brainloop AG, auf dieser Basis die zehn wichtigsten Sicherheitstrends der Zukunft für Österreich ermittelt.

Sicherheitstrends der Zukunft:

1. Die Zukunft der Organisierten Kriminalität
2. Terrorismus einer neuen Dimension
3. Propaganda im Zeitalter der Fake News
4. Politische und religiöse Agitation in Unternehmen
5. Urbanisierung: Bürger rüsten auf
6. Umverteilung von Wohlstand durch Spionage
7. Digitalisierung der Gesellschaft
8. Drohnen: Das Auge am Himmel
9. Privatsphäre im 21. Jahrhundert
10. Wettrüsten im Cyberraum

1) Das Weltwirtschaftsforum (World Economic Forum, kurz WEF) ist eine in Cologny im Schweizer Kanton Genf ansässige Stiftung, die in erster Linie für das von ihr veranstaltete Jahrestreffen gleichen Namens in Davos bekannt ist. Hierbei kommen international führende Wirtschaftsexperten, Politiker, Intellektuelle und Journalisten zusammen, um über aktuelle globale Fragen zu diskutieren. Diese umfassen neben der Wirtschafts- auch die Gesundheits- und Umweltpolitik. Neben den Jahrestreffen gibt das Forum auch Forschungsberichte heraus.

2) https://www.weforum.org/reports/the-global-risks-report-2017

Sicherheitstrends der Zukunft

Die Zukunft der Organisierten Kriminalität

Brain-Hacking, DNA-Erpressung und andere Bio Crimes: Die Zukunft der Organisierten Kriminalität sieht erschreckend aus. Kriminelle sind sehr gut darin, auf gesellschaftliche und technologische Trends aufzuspringen und sie in illegale Geschäftsmodelle zu verwandeln, erst recht wenn es sich um international aufgestellte und gut organisierte Banden handelt. Einer der verblüffendsten Zukunftstrends, die Fusion von IT-Technologie mit menschlicher Biologie, wird ein Tummelplatz für Verbrecher werden: Die Bio-Kriminalität wächst. Bürger, Staat und Wirtschaft werden sich rüsten müssen, um sich und unsere Gesellschaft vor diesen neuen Herausforderungen zu schützen.

Autor:

Sebastian Okada
Prokurist, Leiter Prävention &
Ermittlungen Wirtschaftskriminalität
Corporate Trust

„Denken Sie bitte jetzt an Ihr Passwort", fordert die Banking-App die Kundin an der Zapfsäule auf. Die Frau hat gerade getankt, jetzt will sie mit ihrem Smartphone 82 Euro fürs Benzin überweisen. Sie konzentriert sich... Toskana6788... der Gedanke an das Passwort wird drahtlos von ihrem Gehirn an das Brainwave-Headset übertragen, das sie wie ein Stirnband am Kopf trägt. Von dort wandert das Passwort weiter an ihr Smartphone. „Super bequem", denkt die Frau, „schneller geht's nicht." Ein Quittungston erklingt, Zahlung erledigt.

Sie bemerkt nicht den Mann, der an der Zapfsäule neben ihr steht. Verdeckt unter seiner Jacke trägt er ein Empfangsgerät für elektromagnetische Wellen, das gerade ihre Gedanken bei der Übertragung an das Headset aufgefangen und abgespeichert hat. Noch am Abend wird dieser Mann seinen Fang des Tages, 30 quasi aus der Luft gegriffene Passwörter von Tankstellenkunden, an seine Komplizen weiterleiten. Sie werden dann eine Reihe von Überweisungen auslösen, auf Offshore-Konten in Zypern, Malta und Singapur.

Nicht mal in den Köpfen sind PINs und Passwörter zukünftig mehr sicher.

Freilich: Schon heute kann ein Gehirn in gewissem Umfang gehackt werden. 2012 hat eine Studie von Forschern aus Oxford, Berkeley und Genf gezeigt, dass sensible Personendaten wie PINs, Passwörter und Kreditkarteninformationen schon dann aus Gehirnwellen ausgelesen werden können, wenn die Person nur ein handelsübliches EEG-Headset auf dem Kopf trägt. Die Treffergenauigkeit betrug in dem Experiment rund 30 Prozent. Doch was sind das für Geräte? Und wer trägt so etwas freiwillig?

Bio-Kriminalität: Die nächste große Welle des Organisierten Verbrechens

EEGs (oder Elektroenzephalogramme) kennt man aus dem Krankenhaus: Sie sind ein Werkzeug der neurologischen Diagnostik. Elektroden am Kopf, ein Bildschirm mit Wellen und zackigen Linien – so entstehen per EEG Diagnosen über Krankheiten wie Epilepsie und Schlafstörungen oder über die Tiefe eines Komas. Was dabei gemessen wird, ist die elektrische Aktivität im Gehirn. Diese nutzen zum Beispiel auch Psychologen für ihre Analysen, etwa wenn eine bestimmte Emotion wie Wut, Angst oder Zufriedenheit bei der Versuchsperson ausgelöst und im Gehirn gemessen wird.

Inzwischen sind EEG-Headsets für private Konsumenten der letzte Schrei der Elektronikindustrie. Die Kunststoff-Stirnbänder kosten 200 bis 400 Euro, tragen Namen wie InteraXon Muse und NeuroSky BrainLink und ermöglichen die Übertragung von Gedanken – zur Steuerung von

Computern, Smartphones und anderen Endgeräten. Die Gehirn-Computer-Schnittstelle ist somit Realität.

Immer mehr Menschen werden sich in den nächsten Jahren davon verabschieden, Daten über Tastatur einzugeben. Selbst Siri & Co. – also die Spracheingabe am Smartphone oder im Auto – sind nur ein Zwischenschritt.

Hier fließen zwei Entwicklungen zusammen. Zum einen macht die thought identification durch die Neurowissenschaft große Fortschritte, das heißt: Gedanken können durch EEGs inhaltlich viel genauer identifiziert, ja gelesen werden als früher. Zum anderen entwickelt die Elektronikindustrie immer mehr Wearables, also Geräte, die am Körper getragen werden und biologische Informationen „auslesen". Die Verbindung der beiden Trends macht aus der Biologie eine gewinnbringende – und von Kriminellen nutzbare – Informationsquelle. Denn: Wo neue Technologie verwendet wird, ist das Organisierte Verbrechen meist nicht weit.

Wearable

Biologie als Quelle für Personendaten

Innovative Technologien, vor allem wenn sie Sicherheitsprobleme lösen, werden oft zuerst von staatlichen Sicherheitsbehörden und Geheimdiensten eingesetzt, bevor sie Jahre später von der Organisierten Kriminalität aufgeschnappt und in Geschäftsmodelle verwandelt werden.
Die Zukunft könnte etwa so aussehen: Bio-Sensoren an internationalen Flughäfen sammeln im „Kampf gegen den Terror" unbemerkt Hautzellen von jedem Reisenden ein. Der Mensch verliert im Schnitt etwa zehn Gramm Hautschuppen pro Tag, und jede einzelne Hautzelle ist eine mögliche Quelle für Gen-Analysen. Die Datenbanken der Flughäfen, die sich an einer solchen Maßnahme beteiligen, würden so via Hautschuppen-DNA ein ziemlich erschreckendes Tracking eines großen Teils der Menschheit ermöglichen, wie im Buch „Future Crimes" von Marc Goodman anschaulich beschrieben. Dieselben Sensoren könnten auch am Eingang staatlicher Gebäude und an öffentlichen Plätzen zum Einsatz kommen. Ein (noch fiktiver) Datenschutz-Alptraum.

Und: Kriminelle könnten eines Tages die gleichen Methoden anwenden und mit Hilfe solcher Sensoren eine Genanalyse von Menschen veranlassen, die davon gar nichts wissen. Ihnen spielt in die Hände, dass die Kosten und der zeitliche Aufwand für einen DNA-Test in den vergangenen zwei Jahrzehnten drastisch gefallen sind. Während es früher noch Millionen von Euro kostete und Monate dauerte, eine DNA zu sequenzieren, geht das heute in wenigen Tagen und für etwas mehr als 100 Euro. Es ist mittlerweile so billig geworden, dass Menschen zum Spaß ihre DNA analysieren lassen, um festzustellen, welche Mischung von ethnischen Hintergründen sie haben (was mitunter böse Überraschungen gibt und die Familiengeschichte auf den Kopf stellt).

Sicherheitstrends der Zukunft

Die Zukunft der Organisierten Kriminalität

Kriminelle werden in Zukunft zweifellos die Möglichkeiten der DNA nutzen. Zum Beispiel für raffinierte Mordanschläge: Einem Opfer wird zunächst ein Haar aus einem Kamm oder die Zahnbürste entwendet. Ein Labor analysiert die Genprobe. Dabei kommt heraus, dass die Person eine Anfälligkeit für Herzschwäche, Lebensmittel-Allergie oder ähnliche Gesundheitsrisiken hat. Die Täter wählen dann gezielt ein passendes Mordwerkzeug – zum Beispiel das identifizierte Lebensmittel in konzentrierter und damit lebensgefährlicher Form. Oder einen blutdrucksteigernden und gefäßverengenden Stoff. Oder ein genetisch auf das Opfer zugeschnittenes Gift. Bei späteren Ermittlungen wird es dann außerordentlich schwer zu erkennen sein, dass es sich nicht um einen Unfall oder eine Krankheit gehandelt hat.

Die Gentechnik beschert der Organisierten Kriminalität auch noch eine Idee zum Geldverdienen: Erpressung mit DNA-Erkenntnissen. Das könnte etwa nach diesem Muster ablaufen: „Wir wissen, dass Sie an schizophrenen Episoden leiden. Bisher haben Sie das ziemlich gut vor Ihrem Umfeld geheim gehalten. Aber weiß eigentlich Ihr Arbeitgeber davon? Oder Ihre Ehefrau? Ihre Lebensversicherung? Gegen Zahlung von 10.000 Euro stellen wir sicher, dass keiner davon je erfahren wird…“

Solche Szenarien wirken vielleicht heute noch ziemlich weit weg. Aber wenn man nur an die Möglichkeiten denkt, die zum Beispiel Umkleidekabinen von Fitnessclubs und benutzte Handtücher in Hotels angesichts von erschwinglicher Genanalyse und freiem Zugang zu DNA-Quellen bieten, kann einem schwindelig werden.

Kriminelle am Puls der Zeit

Eine Vielzahl gesellschaftlicher Trends und technischer Innovationen wird irgendwann von Gruppen der Organisierten Kriminalität als Geschäftsmodelle genutzt. Das war schon in der Antike so: Kaum waren Leuchttürme erfunden, nutzten Piraten falsche Leuchttürme und Strandfeuer, um Handelsschiffe auf Sandbänke oder Felsen zu locken und auszurauben.

Drogenschmuggler in Südamerika nutzen seit den 1990er-Jahren selbstgebaute U-Boote in allen denkbaren Größen für den Transport von Kokain in die USA. In der Regel fassen die Unterseeboote, von denen manche sogar mit radar- und sonarabweisender Stealth-Technik ausgestattet sind, von ein paar hundert Kilo bis zu 10 Tonnen Drogen, in Einzelfällen auch 200 Tonnen.

Aber die Organisierte Kriminalität nutzt nicht nur moderne Technik, sondern auch wirtschaftlich-gesellschaftliche Trends. Das „Crowd Sourcing“ etwa, also die Auslagerung von Tätigkeiten an eine Vielzahl von Freelancern, ist bereits verbreitet. Wirtschaftskonzerne oder auch die Wissenschaft nutzen Crowd Sourcing etwa dafür, um die Kosten für Entwicklung ausgereifter Produkte zu verringern, indem sie gleich die Kunden selbst die Produktqualität kritisch hinterfragen lassen. Oder sie beschleunigen arbeitsintensive Mikrotätigkeiten durch eine große Menge an Kollaborateuren, etwa bei der Ahnenforschung oder der Suche nach Signalen außerirdischen Lebens im Weltraum.

Zwei Täter, die in New York Automaten entleerten, posierten mit einem Teil ihrer Beute für Selfies. (Quelle: US Justizministerium)

Mit Hilfe von Crowd Sourcing gelang Kriminellen vor wenigen Jahren einer der größten Geldautomaten-Raubzüge der Geschichte. Programmierer und Ingenieure der Organisierten Kriminalität hatten 2013 bei zwei Unternehmen in Indien und den Vereinigten Arabischen Emiraten die Server geknackt, die Kreditkartendaten für Mastercard und Visa verarbeiten. Die Täter hackten sich in die internen Computersysteme der Firmen, stahlen massenweise Kreditkartennummern und setzten gleichzeitig die Abhebungslimits auf „unbegrenzt".

Dann kam der Geniestreich, das Crowd Sourcing: Die Kartennummern wurden digital an Gruppen von Cyberkriminellen in mehr als zwei Dutzend Ländern verteilt, die mit Kartenrohlingen und professionellen Kreditkarten-Druckern unzählige Visa- und Mastercards – ohne Limit – herstellten. Beim vereinbarten Signal schlugen dann hunderte der kriminellen Freiberufler zu: Sie lösten an Geldautomaten in 27 Ländern gleichzeitig 36.000 Bar-Abhebungen aus und sammelten auf diese Weise mehr als 55 Millionen Dollar ein.

Da die Drahtzieher der Operation noch immer Zugriff auf die Kreditkartenserver hatten, konnten sie live verfolgen, wie viel Geld jeder Täter abhob und somit auch, wie viel an Kickbacks sie zu erwarten hatten – nach Abzug der jeweiligen „Bearbeitungsgebühr" der Free-Lancer.

Die Polizei fasste in mehreren Ländern einen Teil der Geldautomaten-Ausräumer, von denen manche sogar auf Facebook mit Ihrem Raub prahlten. Von den führenden Köpfen hinter der Aktion wurde ein Mitglied gefasst, ein 35-jähriger Türke, der Anfang 2017 von einem Gericht in den USA, einem der Tatländer, zu acht Jahren Haft verurteilt wurde. Man darf gespannt sein, welchen Geniestreich die übrigen Drahtzieher, die entkommen konnten, sich als nächstes einfallen lassen.

Das Erstaunliche an dem Coup war, dass er mit der Professionalität und Effizienz eines multinationalen Konzerns ablief und aus dem Lehrbuch für erfolgreiche Betriebswirtschaft hätte stammen können: Globalisierungsvorteile wurden effizient genutzt (Streuung der Überfälle auf eine Vielzahl von Ländern und damit Multiplikation der Erträge), Risiken wurden konsequent an Dritte ausgelagert (die Free-Lancer setzten sich der mit Abstand größten Gefahr aus) und nicht zuletzt Personalkosten durch den Einsatz der „Crowd" gespart.

Fragt sich nur, was passiert, wenn kriminelle Drahtzieher, die derart kreativ und IT-bewandert sind, auch noch anfangen, mit Gehirnwellen und DNA-Analysen zu experimentieren.

Sicherheitstrends der Zukunft

Terrorismus einer neuen Dimension

Terroranschläge werden sich in den nächsten Jahren häufen, sowohl konventionelle als auch Cyberangriffe. Sie werden unser Sicherheitsgefühl verändern – und sie drohen zerstörerischer zu werden denn je. Deshalb müssen sich Unternehmen wappnen. Damit sie schnellstmöglich reagieren können, wenn sie und ihre Mitarbeiter betroffen sind.

Autor:

Christian Schaaf
Geschäftsführer
Corporate Trust

Es ist eine kalte Februarnacht, als in Europa das Licht ausgeht. Erst breitet sich die Dunkelheit in Italien aus, dann über den ganzen Kontinent. Schnell ist klar: Cyber-Terroristen sind am Werk. Sie haben die Software von Stromzählern manipuliert. Alle Stromnetze sind gelähmt. Europa steuert auf eine Katastrophe zu.

Was der Autor Marc Elsberg in seinem Thriller „Blackout" beschreibt, ist Fiktion. Der Realität kommt er aber erschreckend nahe. Schon im Frühjahr 2007, als ein Hackerangriff die Rechner von Strom- und Wasserversorgern der baltischen Republik Estland für zehn Tage lahmlegte, wurde deutlich, dass solche Szenarien möglich sind. Für kurze Zeit war Estland sogar komplett vom Internet getrennt. Kein Einzelfall: Erst im Dezember 2015 führte ein Hackerangriff zu mehrstündigen Blackouts in der Westukraine.

Hat der Terrorismus damit eine neue Dimension erreicht? In Fällen wie diesen zielt er jedenfalls darauf ab, ganze Staaten außer Gefecht zu setzen. Gewöhnlich verbreitet Terrorismus Angst und Schrecken mittels Gewalt gegen Menschen oder Sachen. Politische, wirtschaftliche oder religiöse Ziele sollen erreicht werden. Was aber, wenn sich die klaren Ziele auflösen? Und der einzige Zweck blankes Chaos ist? Wie wirkt sich das auf unseren Alltag, auf unser Gefühl von Sicherheit aus?

Terroranschläge, auch herkömmliche, werden gefühlt immer mehr Teil unseres Lebens. Die Anschläge am 11. September 2001 auf das World Trade Center in New York, am 13. November 2015 auf das Bataclan-Theater in Paris und am 19. Dezember 2016 auf den Weihnachtsmarkt am Berliner Breitscheidplatz haben bei vielen Menschen ein Gefühl von Ohnmacht entstehen lassen. Sind wir überhaupt noch sicher?

Klar ist: Der islamistische Terrorismus ist keinesfalls die einzige Bedrohung. Anschläge durch Rechtsradikale und linke Extremisten haben heute ebenso ein wachsendes Risikopotenzial wie eben Hackerangriffe durch Cyberaktivisten. Wenn man sich über die Zukunft von Terrorismus Gedanken macht, sollte man bedenken: Auch Terroristen werden die Möglichkeiten des Cyberraums künftig verstärkt nutzen.

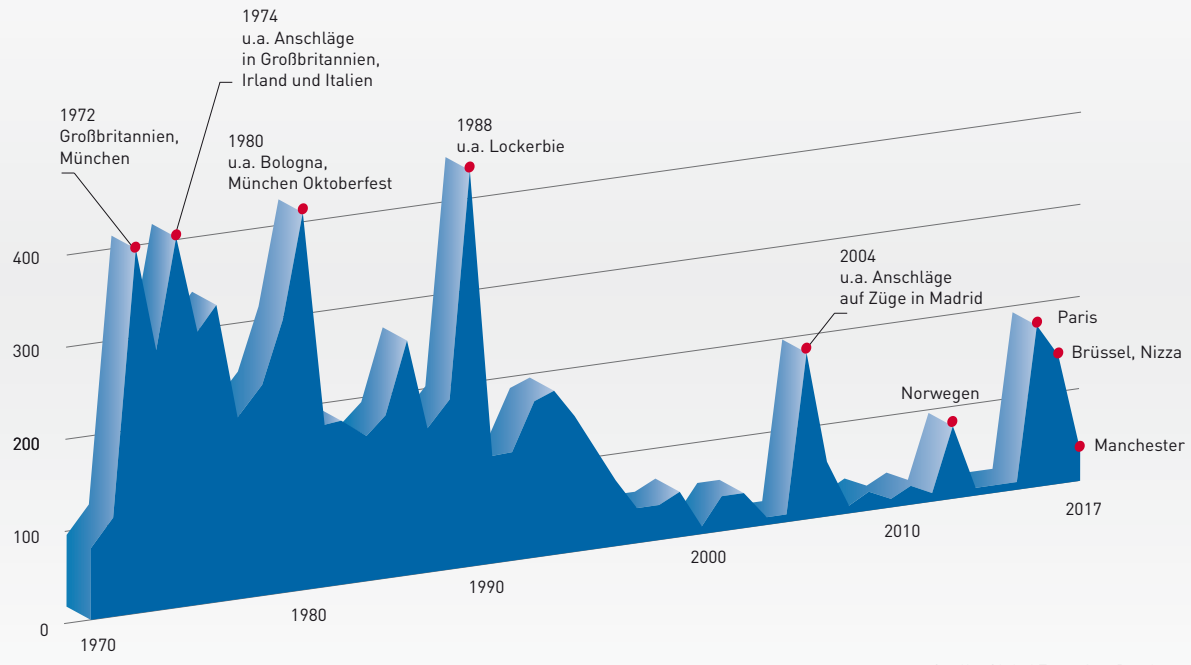
Zudem können aber auch die Schäden durch einen analogen Angriff immense Ausmaße annehmen – zum Beispiel, wenn ein Biokampfstoff dazu verwendet würde, die Trinkwasserversorgung einer Großstadt zu kontaminieren. Gerade bei hoch entwickelten Biokampfstoffen oder genveränderten Substanzen genügen oft kleinste Mengen, um eine riesige Wirkung zu erzielen. Verheerend wäre auch der Einsatz von schmutzigen Bomben (englisch: dirty bombs oder radiological dispersion devices). Dies sind Waffen, die aus einem konventionellen Sprengsatz bestehen, der bei seiner Explosion radioaktives Material in der Umgebung verteilt.

Immer häufiger wird es aber auch das geben: staatlichen Terror. Die Machtspiele einiger Diktatoren führen schon heute in manchen Ländern zu großer Unsicherheit, nicht nur für die betroffene Gesellschaft, sondern auch für Reisende und Investoren. Wo Korruption und Rechtsunsicherheit herrschen, spricht man häufig von failed states. Die politischen Entscheidungen und vor allem die Gerichtsverfahren sind nicht mehr von Rechtsstaatlichkeit geprägt. Die Bürger leiden. Der Staat versagt.

Davon ist man in Österreich zwar weit entfernt. Dennoch: Auch hier reagiert die Wirtschaft sensibel auf das Thema Terror. Die aktuelle Umfrage in diesem Future Report zeigt, dass 27,9 Prozent aller befragten Unternehmen bereits einen Schaden durch einen Terroranschlag erlitten haben (siehe Seite 20). Betroffene Unternehmen klagten zwar vor allem über Projektverzögerungen bzw. Ausfälle beim Öffentlichen Personennahverkehr (ÖPNV), 57,4 Prozent der Unternehmen sehen den Terrorismus aber als künftiges Risiko für sich.

Betrachtet man die Terrorgefahr nüchtern, muss man allerdings feststellen, dass die Zahl der Anschläge in Westeuropa und vor allem das Risiko, Opfer eines Terroranschlags zu werden, seit den 1970er-Jahren laut der Global Terrorism Database[1] gesunken sind (siehe folgende Grafik).

Opfer von Terroranschlägen in Westeuropa



Quelle: Global Terrorism Database

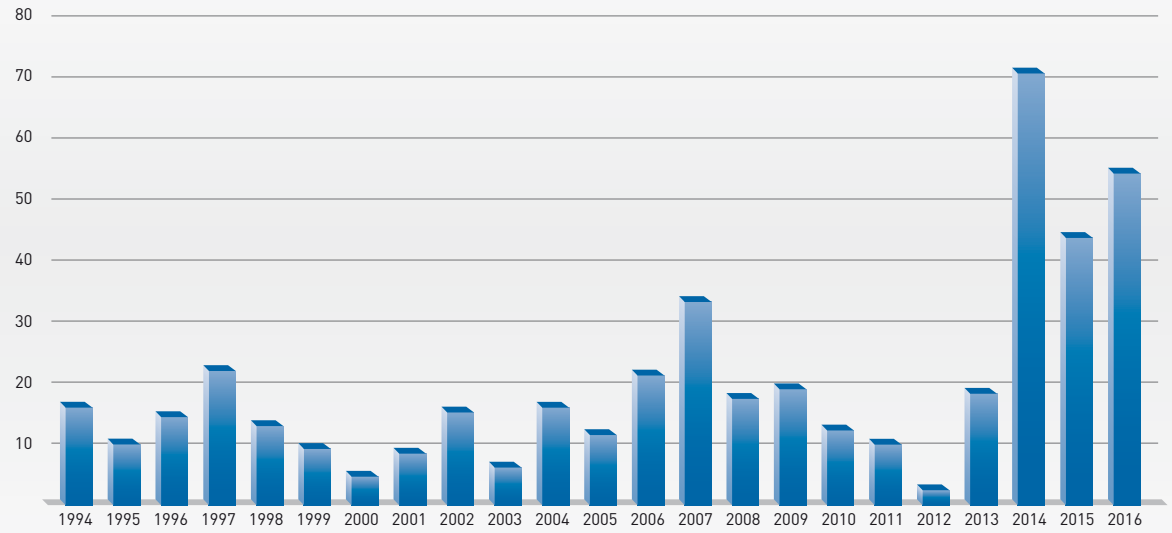
1) https://www.watson.ch/Wissen/Schweiz/982459207-Die-vergessenen-Jahre-des-Terrors--In-den-70ern-und-80ern-zogen-Terroristen-eine-Blutspur-durch-Europa

Sicherheitstrends der Zukunft

Terrorismus einer neuen Dimension

Aber: Es gibt einen erschreckenden neuen Trend. Die Anzahl der schweren Anschläge, mit mindestens 50 Toten, ist in den Jahren 2014, 2015 und 2016 deutlich gestiegen. Das belegt die Global Terrorism Database[1] des National Consortium for the Study of Terrorism and Response to Terrorism (University of Maryland, USA, Grafik unten). Womöglich verschärft sich dieser Trend in den kommenden Jahren noch. Anschläge könnten immer häufiger eine große Zahl von Opfern treffen.

Anzahl schwerer Anschläge mit mindestens 50 Toten



Quelle: Global Terrorism Database

Spätestens seit den Anschlägen vom 11. September ist klar, was der islamistische Terrorismus anrichten kann. Unabhängig davon, ob die Bedrohung von Al-Qaida, den Taliban, Al-Shabaab, Boko Haram oder heute verstärkt durch den IS (sog. Islamischer Staat) ausgeht: Ihnen allen liegt ein fanatischer religiöser Glaube zugrunde. Nach Einschätzung des Bundesamts für Verfassungsschutz wird islamistischer Extremismus auch in Zukunft ein wachsendes Problem darstellen. Denn die Radikalisierung vorzugsweise junger Muslime und die Bereitschaft zum Gewalteinsatz sowie zur Beteiligung an terroristischen Anschlägen nehmen rapide zu. Die Rekrutierung junger Kämpfer für den Dschihad[2] fällt nicht zuletzt durch moderne Kommunikationsmittel zunehmend leichter.

Im Juli 2016 griff ein minderjähriger Flüchtling in einer Regionalbahn bei Würzburg mit Beil und Messer fünf Menschen an. Im selben Monat wurde ein Sprengstoffanschlag auf ein Musikfestival in Ansbach verübt. Ein halbes Jahr später steuerte dann der Tunesier Anis Amri einen Lastwagen in die Menschenmenge am Weihnachtsmarkt auf dem Berliner Breitscheidplatz. Dies wäre jederzeit auch in Österreich denkbar. Auch hier zeigte sich: Bei der Bereitschaft, Schaden anzurichten, scheint es kein Maß mehr zu geben. Immer öfter sind einfache Menschen, Zufallspassanten, sogar Kinder betroffen. Die Frage ist: Gibt es noch Grenzen für Terroristen?

1) Die Global Terrorism Database (GTD) ist eine Datenbank, die Terroranschläge ab 1970 enthält. Betrieben wird die Datenbank durch das National Consortium for the Study of Terrorism and Responses to Terrorism (START) an der University of Maryland, College Park, USA. Sie ist auch die Basis für andere Maßnahmen zum Thema Terrorismus, wie z.B. den Global Terrorism Index (GTI), der vom Institute for Economics and Peace veröffentlicht wird.

2) Der Begriff Dschihad (arabisch für Anstrengung, Kampf, Bemühung, Einsatz; auch Djihad oder in der englischen Schreibweise Jihad) bezeichnet ein wichtiges Konzept der islamischen Religion: die Anstrengung bzw. den Kampf auf dem Weg Gottes.

Offenkundig ist: Aufsehenerregende Anschläge können auch mit konventionellen Mitteln verübt werden, mit Bomben, Schusswaffen sowie Fahrzeugen oder Flugzeugen. Eine Gefährdung besteht besonders bei Großveranstaltungen, Menschenansammlungen oder an symbolischen Orten.

Darüber hinaus wird es vermehrt terroristische Attacken über das Internet geben. Zwar ist nach allgemeiner Auffassung der Sicherheitsexperten der IS derzeit noch nicht in der Lage, einen großangelegten Blackout durch einen Cyberangriff auf die Stromversorgung eines Landes durchzuführen. Dies könnte sich in naher Zukunft aber ändern.

Denn der Wettlauf zwischen Staaten und Kriminellen um die Vorherrschaft im Cyberraum hat längst begonnen. Wie wir seit den Veröffentlichungen von Edward Snowden wissen, setzt der amerikanische Geheimdienst NSA viele verschiedene Technologien zum Angriff auf weltweite IT-Systeme ein. Dieses Wissen um die Angriffstechniken und eine genaue Beschreibung der Vorgehensweise ist seit Snowden öffentlich. Ausgenutzt wurden oft Schwachstellen in einem Computersystem oder -programm, die noch nicht öffentlich bekannt waren, sogenannte Zero-Day-Lücken. Nicht nur, dass jetzt weltweit Staaten versuchen, ihre eigenen Mini-NSAs aufzubauen. Auch jeder Kriminelle oder Terrorist kann sich dieses Wissen nun aneignen. Mittlerweile gibt es sogar einen Schwarzmarkt für Zero-Day-Lücken. Es ist nur eine Frage der Zeit, bis ein Geheimdienst eines nicht demokratisch geführten Landes oder Cyberterroristen eine solche Schwachstelle nutzen, um einen großen Cyberangriff auf ein Unternehmen, eine Branche oder ein ganzes Land zu starten.

Durch so einen Angriff könnte für eine längere Zeit das Internet nicht erreichbar sein. Angesichts unserer immer stärker vernetzten Industrie und der privaten Wohnhäuser, bei denen die Haustechnik, Multimediaanwendungen und Sicherheitsfunktionen zunehmend über das Internet gesteuert werden (Smart Home), hätte das weitreichende Folgen. Maschinen könnten nicht mehr produzieren, die Lieferketten wären unterbrochen und in privaten Küchen würde es nicht einmal mehr den morgendlichen Kaffee geben.

Wenn solche Bedrohungsszenarien in der breiten Bevölkerungsschicht als immer realistischer eingestuft werden, wird dies zwangsläufig zu mehr präventiven Vorkehrungen führen, sowohl im privaten als auch im geschäftlichen Bereich. Menschen werden sich für ihr Zuhause Stromgeneratoren und Vorräte zulegen, etwa haltbare Lebensmittel oder Trinkwasser. Und sie werden die Haussteuerungen stärker gegen fremden Zugriff aus dem Internet schützen müssen. Beim Zugriffsschutz stellt sich allerdings die Frage, wie gut dies in Zeiten von immer mehr Digitalisierung, egal ob in unseren Fahrzeugen oder sog. Wearables[3], überhaupt möglich ist. Die wenigsten wissen etwas über die Schnittstellen ihres Fitnessarmbands oder darüber, wie die Automobilhersteller den Internetzugang zu ihrem Fahrzeug gegen Fremdzugriffe schützen. Auch unser soziales Leben und manche Verhaltensweisen werden sich ändern. Menschen werden bei Zunahme von terroristischen Anschlägen immer häufiger Großveranstaltungen meiden und manchen Menschgruppen immer vorsichtiger bzw. feindlicher gegenüberstehen. Dies könnte unsere offene Lebenskultur verändern.

Im Geschäftsbereich wird man von den Unternehmen erwarten, dass sie Vorkehrungen für ein professionelles Krisenmanagement treffen. Dazu zählt auch, neben Maßnahmen zur Stärkung der IT-Sicherheit, dass Niederlassungen in betroffenen Regionen auch dann noch kommunizieren können, wenn normale E-Mail- und Telefonleitungen unterbrochen sind. Betroffene Mitarbeiter sollten bei einem Anschlag schnell aus Gebäuden gebracht werden können und die Versorgung mit Energie und Notfall-Equipment aus der Zentrale gewährleistet sein, wenn sonst nichts mehr geht.

Klar ist: Der Terrorismus verändert unser Sicherheitsgefühl. Die weltpolitische Lage lässt vermuten, dass dieses Thema in den nächsten Jahren akut bleiben wird. Auch wenn viele Offizielle und Politiker stets beteuern, dass man sich vom Terrorismus nicht einschüchtern lasse und wir unser freiheitliches Leben in gewohnter Weise weiterleben sollten, bleibt ein Gefühl des Unwohlseins – etwa, wenn wir auf eine Großveranstaltung gehen. Schließlich könnte gerade diese als nächstes Ziel auserkoren worden sein. Der Terrorismus, egal ob von rechts, von links, aus dem Cyberraum, fanatisch religiös bedingt oder sonst wie geartet, wird unser Begleiter bleiben. Daher müssen wir uns schon heute auf die Risiken von morgen vorbereiten.

3) Wearables sind tragbare Computersysteme, die während der Anwendung am Körper des Benutzers befestigt sind. Wearable Computing unterscheidet sich von der Verwendung anderer mobiler Computersysteme dadurch, dass die hauptsächliche Tätigkeit des Benutzers nicht die Benutzung des Computers selbst, sondern eine durch den Computer unterstützte Tätigkeit in der realen Welt ist.

Sicherheitstrends der Zukunft

Propaganda im Zeitalter der Fake News

Fake News, Social Bots, Echokammern: Die moderne Medienwelt bringt seltsame Phänomene hervor. Das Problem: Sie alle begünstigen Manipulation. Das gefährdet nicht nur die öffentliche Meinungsbildung. Auch der Wirtschaft droht Unheil. Szenen aus der digitalen Zukunft.

Autoren:

Ingmar Heinrich
Leiter Intelligence
Corporate Trust

Sebastian Schramm
Intelligence
Corporate Trust

„Die Raumtemperatur beträgt 14,2 Grad", tönt es aus dem Lautsprecher der Smart-Home-Anlage. Auf der kalten Leder-Couch rückt Familie Meyer, in Decken gehüllt, enger zusammen. Trotz der unzähligen Kerzen, die Frau Meyer übers Wohnzimmer verteilt hat, will keine rechte Weihnachtsstimmung aufkommen. Dass ausgerechnet über die Feiertage Millionen von Haushalten in Deutschland kein Erdgas zum Heizen haben, wer hätte das im Jahr 2025 für möglich gehalten?

Schuld ist ein plötzlicher Lieferausfall. Seit ein paar Tagen strömt kein russisches Erdgas mehr durch die Ostsee-Pipeline North Stream 2 nach Westen. Der EU platzt deshalb der Kragen: Nach einer Krisensitzung am 27. Dezember unter Leitung des Energiekommissars kündigt sie die Lieferverträge mit Russland wegen nicht ordnungsgemäßer Vertragserfüllung. Katars Stunde ist gekommen. Das kleine Emirat verspricht, die Versorgungslücke mit Flüssiggas (LNG) sofort zu schließen. Katar hat nicht nur die drittgrößten Erdgasreserven der Welt, sondern auch die größte Tankerflotte. So kann der Golfstaat schnell auf Veränderungen am globalen Gasmarkt reagieren. Seit es möglich geworden ist, Erdgas abzukühlen und in verflüssigter Form auf dem Seeweg zu transportieren, hatte Katar um die Gunst der Europäer gebuhlt. Diese waren jedoch wegen langfristiger Abnehmerverträge an russisches Pipeline-Gas gebunden. Damit war jetzt Schluss.

Auffallend war schon, wie rapide sich das Verhältnis zwischen EU und Russland zuletzt verschlechtert hatte. Und wie sehr sich das Russland-Bild in den Medien verfinsterte. Ständig las man auf den Titelseiten in Deutschland, Frankreich und Belgien alarmierende Meldungen über Fremdenhass in den russischen sozialen Netzwerken. Auch von antieuropäischer Stimmung war die Rede. Wie eine Bombe schlug die Nachricht über die Vergewaltigung einer deutschen Kunststudentin an der Lomonossow-Universität in Moskau durch russische Neonazis ein: Bei Facebook und Twitter wurde sie millionenfach geteilt. In Berlin gab es daraufhin eine riesige Demonstration vor der russischen Botschaft: Mehr als 24.000 Personen beteiligten sich und forderten eine rasche Aufklärung durch die Moskauer Ermittler. Als sich wenige Tage später herausstellte, dass sowohl die Austauschstudentin als auch die mutmaßliche Vergewaltigung frei erfunden waren, fand diese Nachricht kaum Beachtung im Netz.

Auch sonst waren merkwürdige Dinge passiert: Mehrfach hatten Hacker in den vergangenen Monaten den Pipeline-Knotenpunkt im russischen Wyborg angegriffen, an dem die North Stream Pipelines beginnen. Anfangs kam es nur zu stundenweisen Ausfällen. Vor Weihnachten wurde die Pumpstation dann durch absichtliche Fehlsteuerungen auch physisch so stark beschädigt, dass sie abge-

schaltet werden musste: Die Gaslieferungen kamen zum Erliegen. Weil die russisch-europäischen Beziehungen ohnehin angespannt waren, hatte Moskau den Hacker-Angriff verschwiegen: Man wollte keine Schwäche zeigen. In Brüssel verstärkte genau das die bestehenden Vorurteile gegenüber Russland noch weiter. Es war ein Teufelskreis. Alles Zufall?

Fake News, Social Bots, Echokammern: Begriffe wie diese bestimmen die Medienwelt im Jahr 2017. Informationen breiten sich rasend schnell über die sozialen Netzwerke aus. Traditionelle Nachrichtenquellen wie Zeitungen und Fernsehen verlieren an Bedeutung. Offensichtliche Tatsachen werden durch „alternative Fakten" in Frage gestellt, gegensätzliche Meinungen im Netz mit Hass-Kommentaren unterdrückt. Negativbeispiele waren die Brexit-Abstimmung in Großbritannien und die US-Präsidentschaftswahl 2016. Nachweislich waren fast 20 Prozent der Tweets während des US-Wahlkampfs von Social Bots erstellt worden. Solche Computerprogramme täuschen eine menschliche Identität vor, ja sie kommunizieren im Internet wie Menschen. Und sie werden zu manipulativen Zwecken eingesetzt: Staatliche und nichtstaatliche Akteure versuchen, durch sie Einfluss auf die öffentliche Meinungsbildung zu nehmen.

Social Bots verbreiten massenweise Fake News. Sie tragen so zur Veränderung der politischen Debattenkultur im Internet bei, bewirken Desinformation und Klimavergiftung im öffentlichen Diskurs. Sie nutzen zudem aus, dass viele Menschen gerne Nachrichten konsumieren, die ihre eigenen Überzeugungen bestätigen; andere Perspektiven lassen sie oft nicht gelten. Dieses Prinzip der „Echokammer" – also die permanente Bestätigung zwischen Gleichgesinnten – macht es außerordentlich schwer, alternative Ideen zu vermitteln.

Zurück zu unserem fiktiven Erdgas-Szenario. Dort führten einige wenige gezielte Aktionen zu einer drastischen Verschlechterung der Beziehung zwischen Russland und der EU. Und das schon lange vor dem kalten Weihnachten:

Es ist Oktober, als DGB-Chef Dieter Sömmerling die „menschenverachtenden Arbeitsbedingungen" der russischen Stahlwerker anprangert, die die Röhrensegmente für den Bau der Offshore-Pipeline hergestellt haben. Der Gewerkschaftsboss bezieht sich dabei auf ein „geleaktes" Video, das bei Youtube aufgetaucht ist. Die Aufnahmen zeigen das Innere eines Stahlwerkes im 1.400 km östlich von Moskau gelegenen Jekaterinburg, heißt es. Ohne jegliche Schutzkleidung stehen die Arbeiter um die gigantischen Hochöfen, die Temperaturen von bis zu 3.500°C erreichen. Bei den Stahlkochern handelt es sich dem Video zufolge um Baschkiren, also Angehörige einer am Ural beheimateten, ethnischen Minderheit. In einer anderen Einstellung sind die Baracken zu sehen, die den Arbeitern als Unterkünfte dienen: schmutzige Holzverschläge, in denen sich bis zu 50 Arbeiter drängen; die Pritschen stapeln sich bis unter die Decke. Erinnerungen an Konzentrationslager und die Gulags werden wach. Eingestellt wurde das Video über den Account von „Human Rights Watchers", laut dazugehöriger Webseite eine Menschenrechtsorganisation mit Sitz in Doha. Deren Aktivisten seien unter Lebensgefahr auf das Werksgelände gelangt und hätten die schockierenden Bildbeweise gesammelt, so steht es in den Kommentaren unter dem Clip. Das Video hatte europaweit für Empörung gesorgt. Doha, Hauptstadt von Katar – das Land, das 2025 ein hohes Interesse an schlechter Publicity für Russland hat...

Dass die sozialen Netzwerke und darin verbreiteten Inhalte starken Einfluss auf die öffentliche Meinungsbildung nehmen, ist bekannt. Hinzu kommt, dass in der digitalen Öffentlichkeit jeder Mediennutzer selbst zum Medien- und damit zum Meinungsmacher werden kann. Das birgt aber die Gefahr des Missbrauchs. Das Konsumverhalten vieler Nutzer, gepaart mit der Schnelllebigkeit der modernen Medienwelt, macht es immer schwieriger, aus der Fülle verfügbarer Informationen qualitativ hochwertige auszuwählen. Oder seriöse Beiträge von solchen zu unterscheiden, die absichtlich zum Zweck der gezielten Desinformation verbreitet werden.

In der öffentlichen Debatte ist dieses Problem längst angekommen. Diskutiert werden aktuell unterschiedliche Lösungsansätze:

1. Neue Algorithmen sollen Fake News oder Social Bots in den sozialen Netzwerken erkennen und markieren, so dass der Konsument weiß, wie hoch der Wahrheitsgehalt der Nachricht ist.

2. Betreiberunternehmen wie Facebook und Twitter sollen unangebrachte Nachrichten wie Hassreden oder Fake News innerhalb einer bestimmten Frist löschen. Bei Verstoß drohen Strafen.

3. Die Medienkompetenz der Nutzer soll gestärkt werden, damit diese ein besseres Verständnis für die Entstehung von Nachrichten und deren Quellen entwickeln.

4. Das Hinterfragen von Fakten, das sog. Fact Checking, durch Journalisten und spezielle Stiftungen soll mehr in den Vordergrund gerückt werden, um gezielt Falschmeldungen zu enttarnen.

Sicherheitstrends der Zukunft

Propaganda im Zeitalter der Fake News

Am Ende wird es eine Kombination dieser Maßnahmen sein, die die Wirkung von Fake News & Co. verringern könnte. So viel ist schon jetzt klar, vollkommen eindämmen lassen wird sich der Missbrauch aber nicht. Dazu verändert sich die Informationsgesellschaft zu schnell und bietet den Nutzern nebenbei auch viele, oft bequeme Vorteile. Zu viel Kontrolle der Medien durch staatliche Organe wird wahrscheinlich nicht erfolgreich sein, weil dies eine Einschränkung des Rechts auf freie Meinungsäußerung bedeutet. Und Freiheit zählt in Europa viel. Zumindest solange keine wirtschaftlichen Interessen auf dem Spiel stehen.

Mit der Inbetriebnahme der Ostsee-Pipeline North Stream 2 und 3 im Frühjahr 2022 hatte sich Europa endgültig von russischem Erdgas abhängig gemacht. Angesichts der Aussicht auf eine gesicherte Energieversorgung bei zugleich niedrigen Kosten hatten die Bürokraten in Brüssel alle Warnungen ignoriert.

Katar, einer der größten Konkurrenten Russlands auf dem globalen Gasmarkt, hatte im Vorfeld – durch intensive Lobbyarbeit in Brüssel, in Verbindung mit gezielten Social Media-Kampagnen – vergeblich versucht, sich als alternativer Erdgaslieferant ins Spiel zu bringen. Der Versuch der USA im Jahr 2017, den Bau weiterer Ostsee-Pipelines durch Sanktionen gegen Russland zu verhindern, scheiterte am energischen Widerstand der Europäer. Die EU drohte mit der Errichtung von Schutzzöllen auf amerikanische Produkte, die der US-Exportwirtschaft enormen Schaden zugefügt hätten. Washington lenkte daraufhin ein, Sanktionen wurden nicht verhängt und die North Stream-Pipelines gebaut.

Da die Herstellung und der Transport von verflüssigtem Erdgas teuer waren, konnte Katar nicht mit Russland auf dem europäischen Markt konkurrieren. Man griff deshalb zu unorthodoxen Mitteln. Mit finanziellen Anreizen lockte der Golfstaat Hacker, IT-Spezialisten und Social Media-Experten aus der ganzen Welt nach Doha. Mittels einer sorgfältig geplanten, mehrstufigen Cyber-Operation schufen die Emiratis die Voraussetzung für den Einstieg in den europäischen Gasmarkt. Europa konnte mithilfe Katars zwar die russischen Lieferausfälle kompensieren, musste aber den höheren Preis für Flüssiggas akzeptieren.

Erst im Nachhinein konnten die verschiedenen Ereignisse der vergangenen drei Jahre miteinander in Verbindung gebracht und Katar als deren Urheber identifiziert werden. Der volkswirtschaftliche Schaden für den Wirtschaftsstandort Europa, der durch den Anstieg der Energiepreise entstand, wirkte sich bis hin zum Endverbraucher aus. Am Ende profitierte nur Doha.

Schon heute könnte ein solches Szenario, ob durch Katar oder ein vergleichbares Land, jederzeit Wirklichkeit werden. Staatliche oder nichtstaatliche Akteure, auch Kriminelle, nutzen längst das Internet, um politische und wirtschaftliche Interessen durchzusetzen. Fake News und Social Bots gefährden nicht nur die politische Meinungsbildung, sondern können auch gezielt eingesetzt werden, um wirtschaftlichen Schaden anzurichten.

Dabei müssen die Urheber derartiger Desinformationskampagnen nicht immer nur auf bestimmte Industriezweige oder eine Volkswirtschaft als Ganzes abzielen. Auch Einzelunternehmen können ins Visier geraten, um etwa strategische Entscheidungen (M&A, Joint Ventures, feindliche Übernahmen etc.) in eine gewünschte Richtung zu lenken. Schon heute sind die technischen Voraussetzungen für den großflächigen Einsatz von Social Bots in Form von ganzen Bot-Armeen vorhanden, was auf ihr Gefahrenpotenzial schließen lässt.

Desinformationskampagnen dürften in Zukunft immer subtiler werden und damit schwieriger zu erkennen sein. Denn nach den ersten öffentlich gewordenen Fällen (z.B. Brexit, US-Wahl, Frankreich-Wahl) steigt die Sensibilität für im Netz verbreitete Falschinformationen. Zudem werden derzeit Mechanismen zur Identifizierung und angemessenen Reaktion geschaffen. Darüber hinaus entwickelt sich gerade ein Bewusstsein dafür, dass Medienkompetenz gezielt vermittelt werden muss – also die Fähigkeit, zwischen seriösen und unseriösen Inhalten zu unterscheiden.

In Zukunft werden die Kommunikationsgeschwindigkeit und die Zeit, die wir im Internet verbringen, weiter steigen. Damit sind wir permanent einer Informationsflut ausgesetzt, die das menschliche Gehirn kaum verarbeiten kann. Das macht uns so verwundbar!

Man muss das Wahre immer wiederholen,
weil auch der Irrtum um uns herum immer wieder gepredigt wird
und zwar nicht von einzelnen, sondern von der Masse,
in Zeitungen und Enzyklopädien, auf Schulen und Universitäten.

Überall ist der Irrtum obenauf, und es ist ihm wohl und behaglich
im Gefühl der Majorität, die auf seiner Seite ist.

Johann Wolfgang von Goethe

Sicherheitstrends der Zukunft

Politische und religiöse Agitation in Unternehmen

Österreichische Unternehmen werden zusehends mit einem ungewohnten und verunsichernden Phänomen konfrontiert. Probleme entstehen zunehmend in den eigenen Reihen: Politische und religiöse Agitation am Arbeitsplatz. Auch wenn nicht viel darüber gesprochen wird, scheinen sich die Vorfälle zu häufen. Derartige befremdliche Aktivitäten sind dazu geeignet das Arbeitsklima negativ zu beeinflussen und gefährden die Sicherheit im Betrieb. Ein vielschichtiges und komplexes Problem. Wegschauen ist dabei keine Lösung. Auch wenn es sich um ein sensibles Thema handelt, sind Unternehmen gefordert auf solche Probleme zu reagieren. Und zwar schon heute.

Autoren:

Uwe Knebelsberger
Geschäftsführer
Corporate Trust

Sabina Slominska
Krisenmanagement
Corporate Trust

Zum Einstieg einige Praxisbeispiele: Als der Kollege nach dem Türkeiurlaub an seinem Arbeitsplatz zurückkehrt, scheint er sich verändert zu haben. Auffällig verändert. Er ist distanziert, streitlustig, geht auf Distanz. Auf tagesaktuelle Gespräche unter Kollegen, die sich auf die politische Situation in Syrien, im Irak oder in der Türkei beziehen, reagiert er aggressiv. Kritik an islamistischen Vorfällen treibt ihn zur Weißglut. Er verstrickt Mitarbeiter in Diskussionen, wobei er Kolleginnen ausgrenzt, und will sie von seiner neuen Weltsicht überzeugen. Als ein Bekannter die Facebook-Seite des Mannes besucht, traut er seinen Augen nicht: Vor ein paar Tagen hat dieser eine schwarze Flagge mit arabischen Schriftzeichen gepostet. Es ist das Banner des „Islamischen Staates"[1].

In der Produktion eines anderen Unternehmens arbeitet ein Schichtleiter, der seine politische Ideologie den Mitarbeitern mit körperlicher Aggression aufzwingen will. Der Mann ist ein glühender Anhänger totalitärer Politik. Aufnahmen von Überwachungskameras zeigen, wie er sich seine vor allem türkischstämmigen Opfer greift, sie an die Wand drängt und dabei klarstellt, welche politische Ausrichtung erwünscht ist - und welche nicht. Viele fügen sich aus Angst um ihren Job.

Fälle wie diese sind bedauerlicher Weise keine Ausnahmen. Vermehrt kommt es in Betrieben und Unternehmen zu politischer und religiöser Agitation. Manchmal hetzen Einzelpersonen in den Betrieben selbst, mitunter versuchen einschlägige Vereinigungen, vielfach vom Ausland finanziert und gesteuert, über die von der wenig integrierten Community besuchten Veranstaltungen, anderen ihre Überzeugungen aufzuzwingen. Solche Aktivitäten gefährden mitunter, wenn sie nicht frühzeitig unterbunden werden, die Sicherheit im Unternehmen. Sie beeinflussen nachhaltig das Arbeitsklima – und zwar negativ. Dabei entsteht ein ernst zu nehmendes Risiko: Wenn Verantwortliche von Unternehmen und Organisationen wegschauen, schwindet möglicherweise die Loyalität der Mitarbeiter. Sie fühlen sich im Stich gelassen.

Die Auswirkungen solcher Agitationen, die sich künftig womöglich häufen werden, sind durchaus dazu geeignet, durch die Verbreitung über öffentlichkeitswirksame Kanäle wie beispielsweise Social Medias für betroffene Unternehmen einen erheblichen Reputationsschaden zu verursachen.

Politische Agitation ist selbstverständlich auch aus den rechts- oder linksextremen Ecken möglich. Ein islamisch oder islamistisch gefärbter Nationalismus, wie ihn Teile der türkischen Politik seit einer Weile vermehrt propagieren,

1) Der Islamische Staat (IS) ist eine seit 2003 aktive terroristisch agierende sunnitische Miliz mit zehntausenden Mitgliedern, die derzeit Teile des Irak und Syriens kontrolliert, wo sie seit Juni 2014 ein als „Kalifat" deklariertes dschihadistisches „Staatsbildungsprojekt" unterhält. Die Organisation ist auch in anderen Staaten aktiv und wirbt um Mitglieder für Bürgerkriege sowie Terroranschläge. Sie wird des Völkermords, der Zerstörung von kulturellem Erbe der Menschheit wie auch anderer Kriegsverbrechen beschuldigt.

birgt jedoch ein enormes Risikopotenzial, da es sich hierbei um ein Problem mit importierter und damit für Mitarbeiter ohne Migrationshintergrund weitgehend unbekannter Weltanschauung handelt. Das daraus resultierende Konfliktpotenzial könnte demnach in Zukunft für Spannung in heimischen Betrieben sorgen.

Die größte Gruppe muslimischer Migranten in Österreich sind Türken, Bosnier und Albaner. 247.500 Menschen mit türkischem Migrationshintergrund (d.h. Eltern stammen aus der Türkei) leben in Österreich, 112.000 Einwohner Österreichs haben die türkische Staatsbürgerschaft (Quellen: Statistik Austria). Wie sich im Verlauf des Verfassungsreferendums im April 2017 herausgestellt hat, unterstützen viele von ihnen Erdogan und seine AKP. Radikalisierungstendenzen haben auch in Österreich Fuß gefasst und breiten sich weiter aus. Unbemerkt kann sich an manchen Orten ein explosiver islamistisch-nationalistischer Mix entwickeln.

Fundamentalistische, gewaltbereite, salafistische Prediger und Netzwerke bereiten mit ihrer Propaganda den Nährboden für Extremismus. In den entsprechenden Milieus finden militante Einzelpersonen Gleichgesinnte. Dieses Radikalisierungspotenzial wird Entscheidungsträger in österreichischen Unternehmen vor wachsende Herausforderungen stellen.

Gründe für eine Identifikation mit radikalen Gruppierungen gibt es viele. Fehlende Perspektiven, eine gescheiterte Integration oder auch das Gefühl, unerwünscht zu sein, sind nur einige davon. Gerade bei männlichen, aus der Türkei (oder aus arabischen Ländern) stammenden Personen ist das Phänomen der Re-Ethnisierung zu erkennen: eine Rückbesinnung auf die kulturellen Traditionen des Herkunftslandes. Dies geht oft einher mit einer starken Bindung an die jeweilige Ethnie und einer schwachen Bindung an das österreichische Normen- und Wertesystem.

Türkeistämmige sind ein attraktives Humankapital für türkische nationalistische Parteien. Sie geraten im schlimmsten Fall in deren ideologischen Griff, werden instrumentalisiert, sollen extremistische politische oder fanatisch religiöse Ziele propagieren.Die türkisch-nationalextremistischen Organisationen, das zeichnet sich deutlich ab, werden von ihren Anhängern aktive und bedingungslose Unterstützung für ihre Ziele fordern. Und sie werden die Reduzierung von Kontakten und Bindungen zu Personen und Institutionen verlangen, die sich außerhalb dieses Kreises befinden. All das trägt zur Spaltung von Belegschaften bei, führt zu Konflikten und letztlich zur Radikalisierung am Arbeitsplatz.

Der islamistisch motivierte Extremismus in Europa stellt vielfach Türkeistämmige als „verlorene Generation" dar und fördert damit deren Selbstwahrnehmung als Benachteiligte oder gar Opfer. Daraus resultierend fühlen sie sich häufiger als andere Migranten von der Aufnahmegesellschaft diskriminiert, was wiederum ihre Bereitschaft zur Eingliederung in die österreichische Gesellschaft senkt. Die Identität der Beteiligten bestimmt sich dann mehr und mehr durch die Feindschaft gegenüber der Aufnahmegesellschaft.

In der Türkei lernt jedes türkische Kind den Satz: „Glücklich ist, wer sich Türke nennt" und spricht ihn unzählige Male nach, wenn vor Unterrichtsbeginn die Nationalhymne gesungen wird. Mit diesem türkischen Nationalbewusstsein ausgestattet gelangen viele Türken nach Österreich. Solche Prägungen lassen sich kaum durch Maßnahmen seitens der einheimischen Aufnahmegesellschaft beeinflussen. Die ethnische Zugehörigkeit wird als wichtiger angesehen als die umgebende Aufnahmegesellschaft. In der Zukunft kann Ethnizität dadurch verstärkt zur Ressource politischer Mobilisierung werden. Gewaltneigungen, die bereits in der Familie entstanden und akzeptiert sind, können im türkisch-nationalistischen Extremismus zusätzlich eine ideologische Legitimation finden. Die Türkeistämmigen können sich dann in der Rolle der Vollstrecker des türkisch-nationalen Volkswillens sehen, egal ob privat oder in der Arbeit.

Was ist zu tun? Die Bekämpfung extremistischer Einstellungen und Aktivitäten ist zum einen eine gesamtgesellschaftliche Aufgabe. Das Thema muss präsenter werden: in der Arbeit, in der politischen Bildung, in den Kommunen, in Moscheen, bei der Polizeiarbeit. Höhere Investitionen im Bildungsbereich sind erforderlich, sie verbessern die Integrationschancen von Kindern und Jugendlichen aus Migrantenfamilien.

All das dauert allerdings. Doch die Zeit drängt. Deshalb müssen die Unternehmen schon heute aktiv werden. Am wichtigsten dabei ist offen und bereit zum Dialog auf das Phänomen zu reagieren. Ausgrenzung von islamischen oder türkischstämmigen Kollegen und Kolleginnen ist zu verhindern. Auf der anderen Seite können islamistische oder islamistisch-nationalistische Agitation nicht toleriert werden. Unternehmen müssen Führungskräfte, Personalisten und Mitarbeiternnen sind zu sensibilisieren und mit Lösungsansätzen und –vorschlägen auszustatten. Frühzeitige Aufklärungsarbeit ist dringend nötig, mit Workshops und Informationsveranstaltungen für die ganze Belegschaft. Externe spezialisierte Beratung ist dabei sinnvoll. Wenn Hinweise auf Agitationen in Blackboxes deponiert werden, müssen Unternehmen darauf reagieren. Proaktives, offenes, dialogbereites Vorgehen stabilisiert Sicherheit und Wohlfühlen im Unternehmen dauerhaft. Wer dagegen die Augen verschließt, trägt unter Umständen dazu bei, dass in den Betrieben ungewollt und unbemerkt Extremismus heranwächst.

Sicherheitstrends der Zukunft

Urbanisierung: Bürger rüsten auf

Die Sicherheitslage ändert sich – auch in Österreich. Der soziale Unfriede in der Bevölkerung wächst, das subjektive Sicherheitsgefühl verschlechtert sich. Angesichts dieser Entwicklung sind künftig die Bürger gefordert: Sie müssen vermehrt selbst für ihre Sicherheit sorgen. Möglichkeiten stehen ihnen dabei genügend zur Verfügung.

Autor:

Marie Jungk
Sicherheitsmanagement
Corporate Trust

Emma, 21, öffnet ihre App. Sie bestellt sich ein Taxi und gibt an, dass sie vom Büro nach Hause will. Beide Adressen sind in der App gespeichert. Emma bestätigt ihre Identität per Fingerabdruck – als Beweis, dass sich kein Unbefugter mit ihrem Account angemeldet hat. Das Taxi ist kein herkömmliches, sondern eines mit hohen Sicherheitsstandards. Spezialverglasung, geschützte Registrierung und Buchung, sogar die Türen des Fahrzeugs lassen sich nur mit einem individuellen Code öffnen. Denn: Es gibt auch keinen Fahrer mehr. Die meisten Taxen fahren im Jahr 2040 autonom.

Aber warum nutzt Emma nicht einfach die U-Bahn? Ganz einfach: Es ist zu gefährlich geworden.

Zurück in die Gegenwart: Im Jahr 2017 lebt man in Österreich und den meisten Ländern Europas in Frieden. Das heißt nicht nur, dass es dort keine Kriege gibt. Das bedeutet auch: Während man in vielen Ländern Afrikas oder Südamerikas schon am helllichten Tag Angst haben muss, Opfer einer Straftat zu werden, kann man sich in den Straßen Europas heute relativ frei bewegen – meistens auch nachts. Nur: Wir können uns nicht darauf verlassen, dass das so bleibt.

Urbanisierung birgt sozialen Sprengstoff

Sicher ist: In den Städten werden künftig immer mehr Menschen auf engstem Raum zusammenleben. Sie kommen schon heute aus den ländlichen Regionen dieses Landes und anderen Staaten, sie finden als Wirtschafts- und Kriegsflüchtlinge Zuflucht. Die globalen Entwicklungen werden diese Trends eher verschärfen. Die Experten gehen zwar nicht davon aus, dass Wien oder Berlin zu Mega-Städten oder Ballungsräumen mit 40 Millionen Einwohnern werden. Aber es ist durchaus möglich, dass zum Beispiel Wien von derzeit knapp 1,9 Millionen auf 4 Millionen Einwohner anwächst. Die Stadtbevölkerung hätte sich damit verdoppelt – so etwas birgt sozialen Sprengstoff.

Die Folgen spüren dann alle Bürger: Die Versorgung der Einwohner wird schwieriger, die Infrastruktur gerät unter Druck. Auch die kommunalen Verwaltungen stoßen ans Limit. Das bedeutet nicht nur längere Wartezeiten bei Ämtern, sondern auch Überlastung der Sicherheitsbehörden. Bereits jetzt suchen die Polizeibehörden händeringend nach neuem Personal – mit geringem Erfolg.

Schon heute lässt sich in Europa beobachten, dass die Polizei mitunter an ihre Grenzen stößt. Dies zeigte sich zum Beispiel in Deutschland bei den sexuellen Übergriffen auf Frauen in Köln in der Silvesternacht 2015/16 und während der Ausschreitungen beim G20-Gipfel in Hamburg im Juli 2017. Da die Zeichen derzeit eher auf eine Verschlechterung der Situation hindeuten (mehr Einwohner in den

URBANISIERUNG: BÜRGER RÜSTEN AUF

Städten, geringere Anzahl von Gesetzeshütern), könnte dies dramatische Auswirkungen auf die Sicherheit haben. Denn eine überlastete, überforderte und unterbesetzte Staatsgewalt wird ihre Aufgaben nicht mehr erfüllen und die Sicherheit der Bürger nicht gewährleisten können. Die Folge: Die Bürger werden künftig stärker für ihre eigene Sicherheit sorgen müssen.

Unzufriedenheit und soziale Spannungen

Sie werden das umso mehr tun müssen, als sich das subjektive Sicherheitsgefühl der Bevölkerung verschlechtert. Der mediale Überfluss mit Nachrichten zur Kriminalität trägt einen großen Teil dazu bei. Zudem öffnet sich die Schere zwischen Arm und Reich weiter. Viele Menschen werden wegen unerfüllter Träume frustriert sein, andere ums Überleben kämpfen. Neid und der Kampf gegen die Armut waren schon immer ein Nährboden für soziale Spannungen.

Soziale Ungleichheit und Urbanisierung fördern auch situationsbedingte Kriminalitätsphänomene. So wurde nach dem Zweiten Weltkrieg manche Hausfrau und Mutter zur Diebin, um ihre Familie in der Stadt irgendwie ernähren zu können.

In den vergangenen Jahren ist auch die Zahl der Haus- und Wohnungseinbrüche stark gestiegen. Geringe Aufklärungsquoten der Polizei und eine immer noch geringe Bereitschaft selbst Vorsorge zu treffen, sorgen dafür, dass die Einbruchszahlen schwer in den Griff zu bekommen sind. Im Vergleich zu den USA oder anderen europäischen Ländern sind in österreichischen Haushalten z.B. immer noch deutlich weniger Einbruchmeldeanlagen installiert, obwohl dies heute für jedermann einfach umzusetzen wäre.

Den Tätern einen Schritt voraus sein

Wie sich die Sicherheit in den Städten entwickeln wird, lässt sich natürlich nicht exakt vorhersagen. Fest steht aber: Wer schon heute an die Gefahren von morgen denkt, der wird nicht nur besser vorbereitet sein. Er wird manches sogar verhindern können. Indem man sich mit künftigen Formen der Kriminalität auseinandersetzt, schafft man das, was wichtig ist für die Prävention von Straftaten: den Tätern einen Schritt voraus zu sein.

Am Anfang sollte die Erkenntnis stehen, dass die Wahrscheinlichkeit, in Europa Opfer einer Straftat zu werden, steigen wird. Daraus folgt das Gebot, Maßnahmen zu ergreifen. Dazu gehört, sich nicht unnötigen Gefahren auszusetzen und das eigene Gefährdungspotential zu kennen. Der Großteil der Möglichkeiten zum Schutz vor künftigen Straftaten besteht bereits heute. Klar ist: Sicherheitstechnik hilft. Je länger ein Täter erfolglos versucht, in das Zuhause anderer einzudringen, desto höher ist die Wahrscheinlichkeit, dass er von seinem Vorhaben ablässt. Das Nachrüsten der Häuser und Wohnungen mit Einbruchmeldeanlagen oder Videoüberwachung ist durchaus sinnvoll. Auch Notrufsender, die man verdeckt am Körper trägt, geben dem Träger ein Gefühl von Sicherheit, die man dann nach außen hin ausstrahlt. Und, auch das ist Fakt: Täter suchen sich eher ein Opfer aus, das Unsicherheit ausstrahlt.

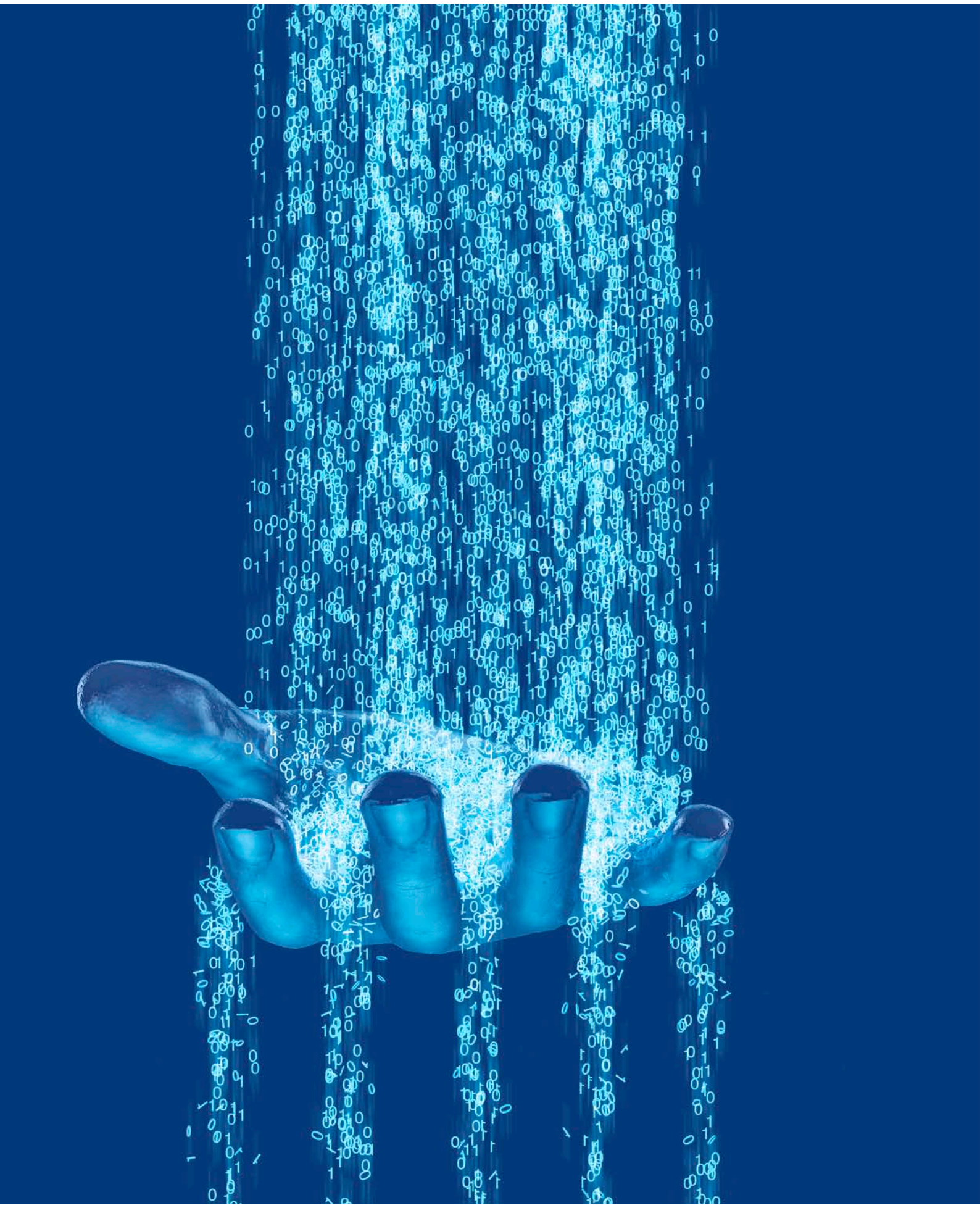
Autonomes Fahren soll die Sicherheit auf den Straßen erhöhen. Damit ist gemeint: Die neue Technik weckt Hoffnungen auf weniger Unfälle und damit weniger Verletzte sowie Tote im Straßenverkehr. Verkehrssicherheit könnte aber, wenn die Kriminalität steigt, noch eine weitere Facette bekommen: Menschen müssen künftig auch vermehrt vor Straftaten im Verkehr geschützt werden. Wer heute mit seinem Fahrzeug an einer Ampel in Johannesburg steht und einen verdächtigen Mann sieht, der sich seinem Wagen nähert, wird unbewusst abwägen: Welche Gefahr ist größer – die, wenn ich eine rote Ampel überfahre, oder die, die von der Person ausgehen könnte? Womöglich kalkuliert in der Zukunft der Bordcomputer solche Risiken.

Längst können aber auch spezielle Vorkehrungen an Fahrzeugen solche Probleme minimieren, gar aushebeln. Sicherheitsverglasung schützt vor dem Zerschlagen der Fenster, die Authentifizierung beim Einstieg ins Fahrzeug versperrt Unbefugten den Zutritt – um nur einige Möglichkeiten zu nennen. Den Menschen stehen mit der Anatomie ihrer Ohren, Fingerkuppen, Venenmuster und Stimmen genügend einzigartige Identifizierungsmerkmale zur Verfügung. Und nebenbei sorgen Panzerglas-Fenster für zusätzliche Sicherheit der Insassen, sollte es doch zu einem Unfall kommen.

Zurück in die Zukunft 2040: Emma ist inzwischen daheim angekommen. Sie öffnet ihre Tür, die durch ein dreistufiges System gesichert ist. Emma hat einen Hausschlüssel, der ein Signal an die Türe sendet. Daraufhin wird sie aufgefordert, ihren Code einzugeben. Während ihre Finger über die Tasten fliegen, scannt ein Programm im Hintergrund das Venenmuster ihrer Hand. Die Tür schwingt auf und Emma tritt ein. Sobald die Tür ins Schloss fällt, verriegelt sie sich. Emma fühlt sich sicher – ein unbezahlbares Gefühl. Auch wenn sie ein bisschen in dieses Gefühl investieren musste.

Die Freiheit besteht in erster Linie nicht aus Privilegien, sondern aus Pflichten.

Albert Camus,
(französischer Schriftsteller und Philosoph, 1913 - 1960)



Sicherheitstrends der Zukunft

Umverteilung von Wohlstand durch Spionage

Es ist kein Geheimnis: Fremde Nachrichtendienste spionieren die österreichische Wirtschaft aus. Damit verschaffen sie der ausländischen Konkurrenz illegal massive Vorteile. Und sie tragen dazu bei, den Wohlstand Österreichs, der häufig auf Forschung und Entwicklung basiert, in ihre Heimatländer umzuverteilen – modernes Raubrittertum. Unsere Firmen müssen ihre Sicherheit stärken, sowohl in technischer Hinsicht als auch im Bewusstsein ihrer Mitarbeiter – nichts Geringeres als die Zukunft unserer Wirtschaft hängt davon ab.

Autor:

Sebastian Okada
Prokurist, Leiter Prävention &
Ermittlungen Wirtschaftskriminalität
Corporate Trust

Die Warnmeldung traf die IT-Abteilung des Technologie-Unternehmens wie ein Fausthieb. Die Detektoren, erst kürzlich von einer Sicherheitsfirma installiert, hatten angeschlagen. Sie brachten eine alarmierende Botschaft: Das hausinterne „Active Directory" – also das Verzeichnis aller Passwörter und Mitarbeiter-Zugangsberechtigungen – war in Kopie aus dem Unternehmen abgeflossen. Die Reaktion war zunächst Schock, dann Unglaube, dann Depression. Konnte das überhaupt stimmen?

Es kam noch dicker. Weitere Tests ergaben, dass die Täter sich ein „Golden Ticket" beschafft hatten. Damit hatten sie Kontrolle über das gesamte Unternehmensnetzwerk. Solche Tickets brauchen Netzwerke, damit ihre Steuerungsinstanzen, die „Domain Controllers", sich vertrauen und miteinander kommunizieren können. Ein „Golden Ticket" zu besitzen ist, wie wenn man den Schlüssel zu jedem einzelnen Haus in der Stadt hat. Und im Moment, wenn man ihn benutzt, aussieht wie der jeweilige Hauseigentümer. Eine Katastrophe.

Spätestens jetzt war klar: Hier war Spionage im Gange. Gewöhnliche Kriminelle würden versuchen, ihren Einbruch ins IT-Netz und den Diebstahl wertvoller Daten schnell zu Geld zu machen, etwa durch Erpressung. Nicht jedoch diese Täter. Die Ermittlungen ergaben, dass sie sich seit Jahren in dem Firmennetzwerk eingenistet hatten und sich in aller Ruhe umsahen. Diese Täter „wohnten" regelrecht in ihrem Opfer, wie ein Parasit, und hatten langfristige Absichten, so viel war klar. Es konnte also nur ein Geheimdienst sein.

Der Fall ist real, das Opfer existiert wirklich: Es ist ein weltweit präsentes Technologie-Unternehmen. Die Geschichte ist nur so weit anonymisiert, dass keine Rückschlüsse auf das betroffene Unternehmen möglich sind. Fakt ist: Es hat mächtige Wettbewerber, die ein hohes Interesse daran haben, technologisch selbst die Nase vorn zu haben. Mit manchen dieser Wettbewerber im Ausland gibt es sogar Joint Ventures, trotz der Gefahr, dass kostbares Know-how abfließen könnte. Ohne solche Partnerschaften geht es oft nicht, sonst muss man auf ganze Märkte verzichten – ein Dilemma für jedes Unternehmen, das global Geschäft machen will.

Wie sich in dem Fall zeigte, war die Infektion mit dem „Golden Ticket" zu umfassend, als dass man sie hätte kurieren können. Es blieb nur eines: ein völlig neues IT-Netz aufzubauen, von Null an. Ein Prozess, der Jahre dauert und weh tut.

Sicherheitstrends der Zukunft

Umverteilung von Wohlstand durch Spionage

Bloß nicht publik

Unternehmen, die durch solche Spionageangriffe heimgesucht werden, wollen nicht, dass die Öffentlichkeit davon erfährt. Um keinen Preis. Die Angst ist begründet: Würden der Angriff und sein Ausmaß publik, würden die Aktienkurse des Unternehmens vermutlich in den Keller rauschen, könnten Anleger das Unternehmen mit Klagen überziehen und dessen Vermögenswerte in massive Gefahr geraten.

Unternehmen müssen sich darauf einstellen, dass sie solche Krisen in Zukunft öfter treffen und sie für das Unternehmen äußerst bedrohlich sein können. In so einem Fall gilt, sich auf das Wesentliche zu konzentrieren: die Verteidigung der eigenen Infrastruktur.

Wirtschaftsspionage, das wird oft unterschätzt, kann eine enorme Tragweite haben: Unser Wohlstand und unsere Arbeitsplätze in Österreich sind mit jedem solchen hochprofessionellen Spionageangriff gefährdet: Schon alleine durch das mögliche Bekanntwerden können massive Schäden entstehen, aber noch mehr durch die Weitergabe der Daten an Konkurrenten.

Innerhalb kürzester Zeit werden zig Millionen oder sogar Milliarden von Euro an Forschungs- und Entwicklungskosten neutralisiert, die heimische Unternehmen über lange Zeit aufbringen müssen und die der Konkurrent einspart – ein gigantischer Wettbewerbsvorteil auf Kosten unserer Wirtschaft. Ein großer Teil des Wissens und Könnens, das in jahrelanger Arbeit mühsam von Mitarbeitern eines Unternehmens aufgebaut wurde, verschwindet so beinahe über Nacht.

Wer jetzt denkt: Alles halb so schlimm, Österreichs Wirtschaft wird immer innovativer bleiben als die anderen, der irrt.

Zwei neue Phänomene haben sich im digitalen Zeitalter zusammengebraut und ergeben kombiniert den perfekten Sturm:

1. Informationen sind bares Geld wert („Information is the new oil", sagen manche). Einige sind so wertvoll wie das Bruttosozialprodukt eines kleinen Landes.

2. Informationen können heute in riesigen Mengen und in kürzester Zeit kopiert werden.

Der Mix ist hochgefährlich – oder hochinteressant, je nachdem, ob man Opfer oder Angreifer ist. Man kann daran jedenfalls sehen, weshalb Länder wie die USA, Großbritannien, Russland und China, um nur einige Beispiele zu nennen, atemberaubende Summen in ihre Geheimdienste investieren, vor allem in die technischen Abteilungen. Das Geld ist gut angelegt, wenn man mit Informationsbeschaffung im großen Stil auch Einnahmen generiert – so wird ein Geschäftsmodell daraus.

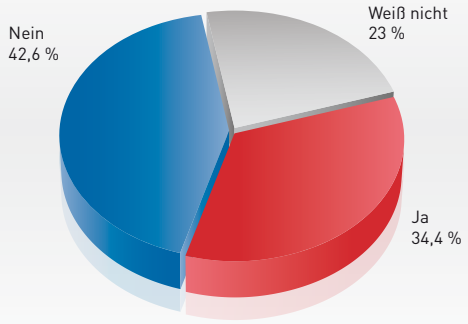
Die Lage ist ernst, aber nicht aussichtslos

Die Gefahr für Österreich wächst. Denn die ernstzunehmenden Angriffe, die wir in der österreichischen Wirtschaft beobachten, häufen sich. Ein paar Fälle im Jahr kann unser Land sicher verkraften – aber was, wenn es deutlich mehr werden?

Genau genommen, sind es schon jetzt deutlich mehr.

Wie die aktuelle Befragung in diesem Future Report ergab, hatten 34,4 Prozent der Unternehmen in den letzten drei Jahren einen Spionageangriff oder Informationsabfluss (siehe Seite 21). Weitere 23,0 Prozent der Unternehmen wussten nicht, ob es ihnen schon passiert ist. Nur 42,6 Prozent konnten definitiv bestätigen, dass sie keinen Vorfall hatten. Dies zeigt, Know-how-Abfluss stellt ein Problem für österreichische Unternehmen dar.

Wurde Ihr Unternehmen in den letzten drei Jahren Opfer von Spionage oder Informationsabfluss?



GRAFIK 7

Quelle: Corporate Trust 2017

Wahrscheinlich sind nicht alle der Spionagefälle auf Angriffe fremder Nachrichtendienste zurückzuführen; manche mögen einfach Spionage durch Wettbewerber gewesen sein. Aber der Unterschied ist für die betroffenen Firmen oft kaum erkennbar.

Klar ist: Österreich hat seit Jahrzehnten von der Globalisierung und seinen Joint Ventures profitiert. Die Kehrseite der Medaille: Auch andere Länder wollen nun ihr Stück vom Kuchen abhaben. Manchen ist dafür jedes Mittel recht. So sind viele Partnerunternehmen de facto sehr nah an der Technologie-Expertise der österreichischen (und anderer westlichen) Unternehmen dran. Ein kleiner Schubs genügt, um den einen oder anderen auf Augenhöhe mit unseren Besten zu bringen. Und dieser Schubs kann auch durch Spionage erfolgen.

Das passierte zum Beispiel im Fall eines Maschinenbau-Konzerns, der jahrelang die privaten und staatlichen Ermittler beschäftigte. Einer seiner Mitarbeiter hatte sich von einem ausländischen Nachrichtendienst bestechen lassen, was ihm half, seine privaten Finanzprobleme zu lindern. Er sorgte im Gegenzug dafür, dass der Nachrichtendienst Zugang zu den IT-Systemen seines Arbeitgebers erhielt. Der wiederum bekam davon zunächst nichts mit.

Eines Tages jedoch rief bei einer ausländischen Niederlassung des Konzerns eine örtliche Ermittlungsbehörde an. Im nüchternen Ton der Fakten schilderte ein staatlicher Ermittler der Geschäftsführung, dass man beobachtet habe, wie der gesamte Firmenserver in Kopie an ein Drittland abgeflossen sei, das bekannt ist für seine aggressiven und kompetenten Spionagebemühungen.

Der gesamte Server?

Ja, lautete die Antwort, man könne sich ja anhand einiger Kopien sensibler technischer Dokumente, die Teil der Beute waren, davon überzeugen. Das war der erste Tag einer neuen Ära im Unternehmen. Es folgten: eine Festnahme, jahrelange private und staatliche Ermittlungen und Sicherungs- und Säuberungsarbeiten in der technischen Infrastruktur der Firma.

Sicherheitstrends der Zukunft

Umverteilung von Wohlstand durch Spionage

Spionagestrategien und Ziele

Es gibt eigentlich kaum noch Länder, deren Geheimdienste ausschließlich im Dienst ihrer nationalen Außen- und Sicherheitspolitik spionieren. Dazu sind die Möglichkeiten, mit Informationsbeschaffung auch Geld zu verdienen, einfach zu verlockend. Österreich und Deutschland haben sich entschieden, ihren Nachrichtendiensten nur das Mandat zur Verteidigung der eigenen Wirtschaft zu geben, nicht zum Angriff anderer. Ob das so klug war, wird sich in den nächsten Jahrzehnten zeigen.

Andere haben da weniger Hemmungen. Die USA zum Beispiel betreiben Wirtschaftsspionage in einer Reihe von Industrien, die das Land als strategisch relevant betrachtet – auch spezifisch gegen Deutschland gerichtet, wie die Snowden-Dokumente belegen. Die Liste der ausspionierten Branchen reicht von sehr spezifisch bis sehr allgemein, ein äußerst breites Spektrum.

Spezifisch: Hoch- und Niedrigenergie-Laser, Waffen mit gerichteter Energie, Tarnungs- und Tarnungsentdeckungstechnik, Raumfahrt- und Fernsensoren, Nanotechnologie, Elektro-Optik.

Allgemein: Datenverarbeitung und Informationstechnik, Elektronische Kriegsführung und energetische Materialien (alles, was Energie enthält).

Damit kein Missverständnis aufkommt: Die „Kunden" der staatlichen Spione, also die Empfänger der Informationen, sind beileibe nicht nur Sicherheitsbehörden und das Weiße Haus, sondern auch die geschäftsmäßig orientierten Zweige der US-Regierung: die drei Ministerien für Landwirtschaft, Handel und Finanzen.

China hat im Unterschied dazu gleich die Entwicklung seiner gesamten Wirtschaft zum strategischen Ziel erhoben – und einen entsprechend umfassenden Spionageauftrag an seine Nachrichtendienste erteilt. Das Land hat schon lange erkannt, dass wirtschaftliche und finanzielle Dominanz der Schlüssel zu geostrategischer Sicherheit ist. Wer selber alles herstellen kann, braucht nicht viel zu importieren. Wer zudem die Schulden der anderen kontrolliert, hat sie beim Schopf.

Österreichs Wirtschaft muss sich also warm anziehen.

Was wir tun können

Erkenntnis ist der erste Schritt zur Besserung. Konkret heißt das: Österreichische Unternehmen müssen wissen, wie empfänglich sowohl ihre technische Infrastruktur, das heißt ihre IT und baulichen Sicherheitsmerkmale, als auch ihre Mitarbeiter für Angriffe sind.

Denn ein erfolgreicher Spionageangriff funktioniert fast nie allein auf technischer Ebene. Vielmehr geht er Hand in Hand mit Social Engineering[1], also der Manipulation von Menschen im Unternehmen, die dazu verleitet werden, den Angreifern Informationen zu liefern, die ihnen letztlich Zugang zu Systemen bescheren.

Social Engineering gehört zu den drei häufigsten Angriffsmethoden, wenn es darum geht, österreichische Unternehmen auszuspionieren, wie die befragten Unternehmen 2014 in unserer Studie zu Industriespionage[2] angaben. Rund 18 Prozent der Unternehmen, die von Spionage betroffen waren, haben Social Engineering bei sich festgestellt. Weitere Methoden, die oft auch mit der Manipulation von Menschen kombiniert wird, sind das Hacking von Computern und Netzwerken (rund 42 Prozent) und das Abfangen elektronischer Kommunikation (rund 40 Prozent).

Ein Mitarbeiter, der zum Beispiel nicht bemerkt, dass ein Anrufer nur vortäuscht, bei seinem Unternehmen zu arbeiten, oder dass der „neue Freund" aus dem Fitness-Studio in Wahrheit einen finsteren Plan verfolgt, ist ein ernstes Risiko für jedes Unternehmen. Ziel muss es sein, Mitarbeiter durch Trainings in die Lage zu versetzen, die Warnzeichen zu erkennen und einen Verdacht an die zentralen Sicherheitsstellen im Haus zu melden, damit diese tätig werden können.

Eines ist klar: Wenn in den nächsten Jahren nicht spürbar mehr Abwehrmechanismen gegen Spionage in unserer Wirtschaft aufgebaut werden, wird Österreich über kurz oder lang Arbeitsplätze und Wohlstand einbüßen. Und das wird fix gehen, denn die Welt dreht sich auch dank der Technologie immer schneller.

1) Als Social Engineering bezeichnet man das Ausspionieren des persönlichen Umfelds, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität bzw. unter Verwendung einer Legende. Social Engineering hat zum Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

2) https://www.corporate-trust.de/de/portfolio-items/studie-industriespionage-2014?portfolioCats=5%2C12

Illegal is always faster.

Eoin Colfer
(Irischer Autor, geb. 1965)

Sicherheitstrends der Zukunft

Digitalisierung der Gesellschaft

Durch die zunehmende Digitalisierung der Gesellschaft geben immer mehr Menschen die Verantwortung über ihre persönlichen Daten und kritischen Prozesse aus der Hand.

Autoren:

Christian Schaaf
Geschäftsführer
Corporate Trust

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit
& Computerkriminalität
Corporate Trust

Der 42-jährige Versicherungsangestellte wollte wie jeden Morgen um acht Uhr in sein Auto steigen, um zur Arbeit zu fahren. Bereits am Frühstückstisch, als er über die App auf seinem Smartphone den Batteriezustand seines Elektrofahrzeugs prüfen wollte, bekam er keine Verbindung. Als er zum Auto ging, ließ sich der Wagen zwar noch öffnen aber nicht starten. Irgendetwas lief schief an diesem Morgen. Dann kam die E-Mail: Hacker hatten seinen Wagen gekapert und verlangten ein Lösegeld von 1 Bitcoin[1], aktuell mehr als 3.500 Euro, um ihn wieder freizugeben.

Im Moment zwar noch Fiktion, könnten solche Vorfälle jedoch schon bald Wirklichkeit werden. Denn auf ähnliche Weise wurden in den vergangenen Jahren Unternehmen, Krankenhäuser und Behörden weltweit erpresst, nachdem Hacker ihre Daten verschlüsselt hatten und so ihren Betrieb zum Erliegen brachten.

Durch die zunehmende Digitalisierung der Gesellschaft geben immer mehr Menschen die Verantwortung über ihre persönlichen Daten und kritischen Prozesse aus der Hand. Weil die Dienstleister in diesem Bereich oft nur schwer einem Land zuzuordnen sind, werden Daten in Zukunft vermutlich immer häufiger in Ländern verarbeitet, deren Rechtsvorschriften wir nicht kennen. Ob diese Daten bei solchen Anbietern sicher sind, wissen wir häufig nicht. Um nicht ausgeliefert zu sein und den Überblick über die eigenen digitalen Spuren zu behalten, werden wir immer mehr gezwungen sein, uns mit den genutzten Geräten, den technischen Möglichkeiten, Prozessen und Auswirkungen auseinander zu setzen. Die meisten Menschen sind damit jedoch völlig überfordert.

Die Industrialisierung Anfang des 19. Jahrhunderts stellte die Menschen bereits vor eine große Herausforderung. Der Wandel von überwiegend handwerklicher Herstellung zur industriellen Produktion mit maschineller Erzeugung von Gütern und Dienstleistungen, war eine Revolution. Erst nach einigen schweren Unfällen mit explodierenden Dampfmaschinen wurde 1866 in Mannheim die Gesellschaft zur Überwachung und Versicherung von Dampfkesseln gegründet, der Vorläufer des heutigen TÜV in Deutschland. Heute ist der Einsatz von Maschinen bei allen Arten von Produktion ebenso eine Selbstverständlichkeit wie das Fahren mit Autos oder das Fliegen mit einem Flugzeug.

1) Bitcoin (englisch sinngemäß für „digitale Münze") ist eine digitale Geld¬einheit eines weltweit verwendbaren dezentralen Zahlungssystems. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet mithilfe einer speziellen Peer-to-Peer-Anwendung abgewickelt, sodass anders als im herkömmlichen Bankverkehr keine zentrale Abwicklungsstelle benötigt wird. Eigentumsnachweise an Bitcoin können in einer persönlichen digitalen Brieftasche gespeichert werden.

Bei der Industrialisierung hatten die Menschen einen Zeitraum von ca. 200 Jahren, um sich an die neuen Technologien zu gewöhnen. Das Internet gibt es seit knapp über 50 Jahren und die Nutzung durch Jedermann seit nicht mal ganz 30 Jahren. Und obwohl diese Technologie damit eigentlich noch sehr jung ist, gibt es bereits jetzt den ganz großen nächsten Schritt: die Digitalisierung der Gesellschaft.

Wenn in Häuser zunehmend Steuerungen für die Heizung, Beleuchtung, Multimediaanwendungen, Türöffnung, Alarmanlagen oder Videokameras zur Überwachung eingebaut werden, die aus dem Internet erreichbar sind (Stichwort: Smart Home), dann hilft uns dieses Internet of Things (IoT) beim täglichen Leben und steigert den Komfort. Allerdings führt es auch dazu, dass wir eine Menge privater Daten und Informationen preisgeben und angreifbarer werden.

Definitionen:

Internet of Things (IoT):

Der Begriff Internet of Things beschreibt, dass der Computer in der digitalen Welt zunehmend in Maschinen und Alltagsgegenstände eingebaut wird und von intelligenten Gegenständen bis hin zu künstlicher Intelligenz oder Sensoren ergänzt wird. Die immer kleineren eingebetteten Computer sollen Menschen unterstützen, ohne abzulenken oder überhaupt aufzufallen.

Industrie 4.0:

Die industrielle Produktion wird zunehmend mit moderner Informations- und Kommunikationstechnik vernetzt. Der Begriff Industrie 4.0 stammt ursprünglich aus der Hightech-Strategie der Bundesregierung und ihrer Forschungsunion. Technische Grundlage hierfür sind intelligente und digital vernetzte Systeme, mit deren Hilfe eine weitestgehend selbstorganisierte Produktion möglich werden soll.

Nur die wenigsten Hersteller machen sich aktuell ausreichend Gedanken zur Sicherheit ihrer Geräte und Anwendungen. Eine Lackiermaschine, ein Auto, eine Waschmaschine und eine Heizung sollen 10, 15 oder gar 20 Jahre lang halten. In solche Wirtschaftsgüter wird aktuell IT-Technik eingebaut, um die Geräte digital zu bedienen, über das Internet auszulesen oder vom Smartphone aus zu steuern.

Leider ist Software in der Regel nur kurzlebig. In der IT-Branche sind Zeiträume von 10 Jahren im wahrsten Sinne des Wortes unvorstellbar. Vorhersagen, wie die Technologie in einem Jahrzehnt aussehen wird, traut sich niemand zu. Und für viele Softwareprogramme, die vor 20 Jahren programmiert wurden, bräuchte man einen Uralt-Computer mit Diskettenlaufwerk, um noch Veränderungen vornehmen zu können. Solche Veränderungen sind aber manchmal notwendig: egal ob auf dem PC, Laptop, Tablet oder Smartphone, wir alle bekommen regelmäßig Updates. Dies bedeutet nichts anderes, als dass der jeweilige Hersteller erkannt hat, dass es einen Fehler in seiner Software gibt, einen sogenannten „Bug"[2], der behoben werden muss.

Beim Einbau kurzlebiger IT-Technik in langlebige Wirtschaftsgüter muss es daher die Möglichkeit für Updates der Software geben. Gleichzeitig muss auch die Hardwareversorgung über die gesamte Lebensspanne gesichert werden. Dabei findet dies unter erschwerten Bedingungen statt: die Hacker lernen ständig dazu und die Angriffe werden immer ausgefeilter. Ein 10 Jahre alter PC würde heute keinem Hacker mehr standhalten. Es muss also auch eine Möglichkeit geben, die IT-Funktionen in den Geräten wieder abzuschalten, wenn sie nicht mehr nachgesichert werden können.

Ein weiteres Problemfeld ist die Versorgung mit neuer Software, die in der Regel über den Zugang aus dem Internet erfolgt. Darüber können die Geräte selbstverständlich auch angegriffen und gekapert werden, wenn sie ungenügend gesichert sind. Über ein gehacktes Gerät, das im heimischen WLAN eingebunden ist, können dann evtl. auch die Netzwerkdaten ausgelesen werden, wodurch weitere am WLAN angebundene Geräte wie Fernseher, PC, Tablet oder Smartphone angreifbar werden.

2) Ein Programmfehler, Softwarefehler oder Software-Anomalie, häufig auch Bug (englisch) genannt, bezeichnet im Allgemeinen ein Fehlverhalten von Computerprogrammen. Dies tritt auf, wenn der Programmierer eine bestimmte Festlegung der Spezifikation nicht oder falsch umgesetzt hat, oder wenn die Laufzeitumgebung fehlerhaft bzw. anders als erwartet arbeitet.

Sicherheitstrends der Zukunft

Digitalisierung der Gesellschaft

Hier bedarf es also viel IT-Sicherheits-Know-how, um die Hard- und Software in den Geräten so zu „härten"[3], dass nicht jedermann einfach darauf zugreifen kann. Viele Firmen haben dieses Know-how jedoch nicht. Sie sind mit ihrem ursprünglichen Know-how, z.B. Ingenieursleistungen, groß geworden. Das Thema IT war bisher nur für die eigenen Office-Anwendungen oder zur Erleichterung der Buchhaltung nötig. Jetzt plötzlich muss man auch für die Erstellung der eigenen Produkte alle IT-Register beherrschen und sich am Markt um die besten Köpfe in der IT-Entwicklung und -Sicherheit bemühen. Kein leichtes Unterfangen, wenn man von der Historie her gar nicht in diesem Bereich tätig war und plötzlich bei Null anfangen muss.

Aber auch die IT-Sicherheitsexperten selbst haben in diesem Bereich noch viel zu lernen. Es ist ja nicht zu bestreiten, dass bei PCs auch nach Jahren der Beschäftigung mit IT-Sicherheit die Sicherheitsprobleme nicht verschwunden sind. Genau betrachtet, ist die IT-Sicherheit an sich eine recht junge Branche. Und wie die klassische Sicherheit im Mittelalter, wo hohe und dicke Mauern das Maß der Dinge waren, setzen die Cyber-Sicherheitsexperten häufig allein auf eine einzige, möglichst stabile Verteidigung. Themen wie die ständige Betreuung der Systeme aus Sicherheitssicht, hintereinander gestaffelte Verteidigungssysteme, Software zur Angriffserkennung sowie die professionelle Aufklärung und Behandlung von Vorfällen sind oft eher die Stiefkinder der IT-Sicherheit.

Für die Hersteller ist dies eine Zwickmühle. Einerseits können sie ihre Produkte in naher Zukunft nicht mehr ohne digitale Steuerungen anbieten. Andererseits sind sie oftmals mit ihrer eigenen Organisationstruktur noch nicht in der Lage, die digitalen Prozesse und das Entwicklungs-Know-how in diesem Bereich in der gleichen Güte abzuliefern, wie bei ihren eigentlichen Produkten. Weil damit unter Umständen gewohnte Player am Markt, die vor allem aufgrund der Qualität ihrer Produkte geschätzt wurden, ebenfalls Lücken oder Softwareschwächen haben, wird die Erwartungshaltung an Qualität und Zuverlässigkeit schwinden. Produkte von weltweiten Anbietern werden ebenso akzeptiert werden, wie die der österreichischen „Platzhirsche".

Die Digitalisierung betrifft aber auch unsere tägliche Versorgung. Der Handel steuert seine komplexen Logistikketten, die uns mit allen möglichen Gütern versorgen, mit IT. Unser Fahrzeuge werden automatisch fahren, unsere Fabriken automatisiert produzieren. Computer steuern unsere Stromversorgung und die Verwaltung der Infrastrukturen unserer Städte. Neue digitale Währungen breiten sich in unserem Banksystem aus, das schon seit längerer Zeit computergesteuert Milliardentransaktionen in Millisekunden durchführt. Alle diese Entwicklungen führen zu einer steigenden Verwundbarkeit unserer Gesellschaft aus dem Cyberraum.

Die Nutzer der neuen Technologien sind aber eher fasziniert von den neuen Möglichkeiten und rufen nach immer größerer Funktionsvielfalt. So lange sich aber das Produkt mit den meisten Funktionen am besten verkauft, werden Sicherheitsüberlegungen bei der Entwicklung neuer Technologien weiterhin nachrangig behandelt werden. Der Ruf danach, die Sicherheit der Produkte gleich bei ihrer Entwicklung zu berücksichtigen („Security by Design"), verhallen in den meisten Firmen ungehört, da der Wettbewerber gerade wieder eine neue Funktion eingebaut hat, die nun sofort nachgebaut werden muss. Die Entwicklung von IT-Systemen unter Zeitdruck ist aber von jeher das Sicherheitsrisiko Nummer Eins.

So lange also die Konsumenten das Thema Sicherheit nicht in ihre Kaufentscheidung mit einbeziehen, werden wir weiter ungebremst auf das erste große „9/11" der Digitalisierung zurasen. Wir können nur hoffen, dass auf dem Weg dahin einige kleinere Vorfälle die Aufmerksamkeit der Öffentlichkeit erregen und uns dann das Umsteuern hin zu einer sicheren Digitalisierung unserer Gesellschaft noch gelingt.

3) Unter Härten versteht man in der Computertechnik, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist und deren korrekter Ablauf unter Sicherheitsaspekten garantiert werden kann. Das System soll dadurch besser vor externen Angriffen geschützt sein. Ziel ist es, ein System zu schaffen, das von vielen, auch weniger vertrauenswürdigen Personen benutzt werden kann.

Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren.

Benjamin Franklin (1706 - 1790)

SICHERHEITSTRENDS DER ZUKUNFT

DROHNEN: DAS AUGE AM HIMMEL

Privatleute, Journalisten, Logistiker und Sicherheitskräfte haben eines gemeinsam, sie alle interessieren sich für unbemannte Fluggeräte.

Autoren:

Alfred Czech
Geschäftsführer Österreich
Corporate Trust

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit
& Computerkriminalität
Corporate Trust

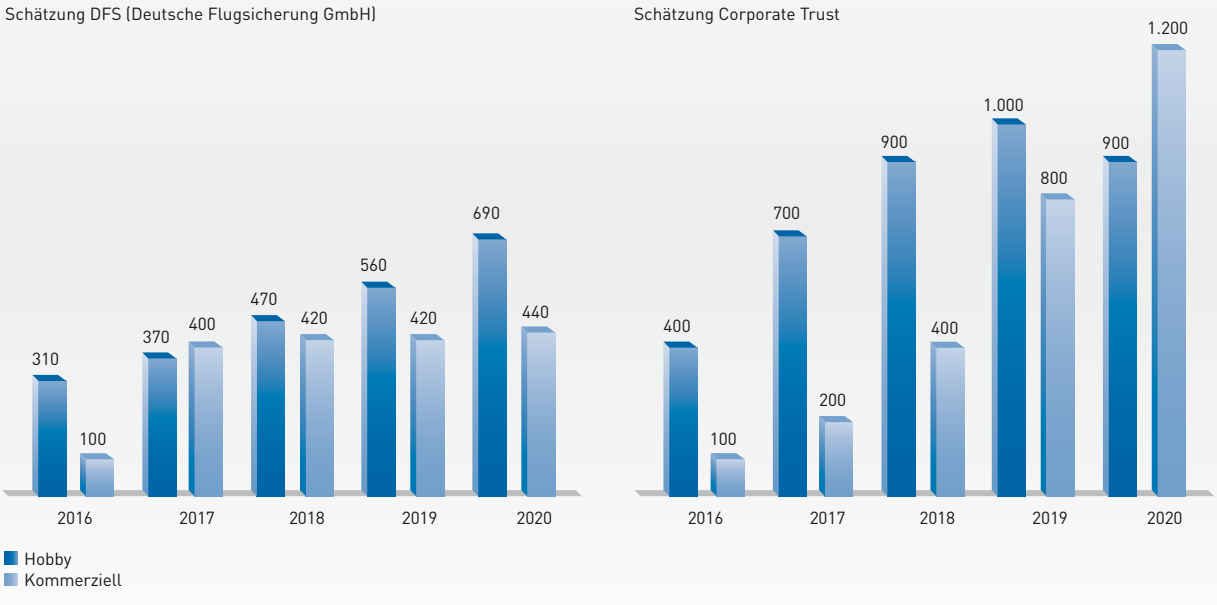
Auftakt zum portugiesischen Fußball-Pokalfinale 2017 zwischen Benfica Lissabon und Vitoria Guimaraes: Ein Surren am Himmel erregt die Aufmerksamkeit der Zuschauer, die auf den Anpfiff warten. Das Geräusch kommt von einer umgerüsteten Drohne, auf der – wie ein Surfer – ein Mann steht. Sein fliegendes Gefährt – eine Kreuzung aus Drohne und Hoverboard – hat er perfekt im Griff. Zur Überraschung der Zuschauer ist es der Schiedsrichterassistent, der wie ein Superheld mit dem Fußball ins Stadion schwebt.

Der Show-Effekt war ein Hit. Sicherheitsfachleute denken in so einem Moment aber auch an ein anderes Szenario: Dass mit einer solchen Drohne schlimmstenfalls auch eine Bombe in ein vollbesetztes Stadion fliegen könnte – ein erschreckender Gedanke.

Privatleute, Journalisten, Logistiker und Sicherheitskräfte haben eines gemeinsam, sie alle interessieren sich für unbemannte Fluggeräte. Bei so viel Interesse wundert es nicht, dass die Anzahl der Drohnen in Deutschland Jahr für Jahr wächst. Gleichzeitig steckt die Drohnenabwehr in den Kinderschuhen.

Während einige Unternehmen eine halbwegs zuverlässige Drohnendetektion im Nahbereich im Angebot haben, bleibt die Ferndetektion, und erst Recht die eigentliche Abwehr, faktisch unmöglich. Insofern werden wir uns mit den Folgen des zunehmenden Drohnenverkehrs am Himmel auseinandersetzen müssen.

Geschätzte Anzahl von Drohnen im deutschen Luftraum (in Tausend)



Quelle: DFS Flugsicherung GmbH & Corporate Trust 2017

Sicherheitstrends der Zukunft

Drohnen: das Auge im Himmel

Die Einsatzmöglichkeiten von Drohnen sind vielfältig: Sicherheitskräfte setzen Drohnen ein, um Veranstaltungen, Demonstrationen, kritische Infrastrukturen aber auch Justizvollzugsanstalten zu überwachen.

Typischerweise erfolgen solche Patrouillenflüge durch eine Kommandodrohne, die bei Detektion von Angreifern oder Sondersituationen automatisch programmierte Prozesse in Gang setzt. Das kann die Aktivierung einer Verbindung zur Leitstelle sein, die über die eingebaute Kamera die Lage erkennen und handeln kann. Das kann aber auch die Nutzung von technischen Funktionen der Drohne sein, zum Beispiel die Aktivierung einer Gesichtserkennung, die Ansprache von Tätern über eingebaute Lautsprecher oder die Nutzung einer Bewaffnung.

Die Diskussion über die Bewaffnung von Drohnen ist dabei ein besonderes heikles Thema. Im Sicherheitsbereich kann der Einsatz einer bewaffneten Drohne dann erfolgen, wenn die Abwehr durch menschliche Kräfte zu gefährlich ist.

In Dallas etwa hat sich 2016 ein Mann in einem Parkhaus verschanzt und sich mit der Polizei einen Schusswechsel geliefert. Dann setzten die Beamten einen ferngesteuerten Roboter ein, um einen Sprengsatz in die Nähe des Mannes zu bringen und dort detonieren zu lassen. Der Schritt, solche Situationen mit Drohnen zu lösen, ist nicht mehr weit; bereits heute können Drohnen (teilweise im Eigenbau) mit Schusswaffen, Sprengmitteln, Flammenwerfern oder Kettensägen bestückt werden.

Die Diskussion, in wie weit der Einsatz von Drohnen für das Aufspüren und Abwehren von kriminellen oder terroristischen Angreifern im Inland zulässig ist, wird in den nächsten Jahren geführt werden. Besonders interessant wird die Diskussion, wenn Sicherheitsbehörden die Tötung von Gefährdern mittels Drohnen bzw. Robotern andenken.

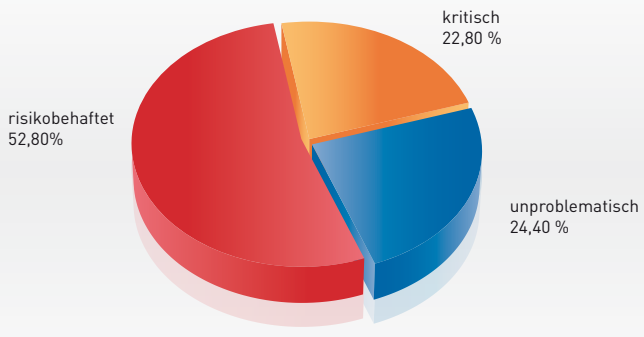
Gleichzeitig besteht die Gefahr, dass Kriminelle Drohnen nutzen. Die Steuerung von Drohnen ist kinderleicht. Der Operator kann meilenweit von seinem Ziel entfernt sein und damit sehr anonym agieren. Das Entdeckungsrisiko für einen Drohnenpiloten ist gering, das Bedrohungspotential hingegen riesig. Drohnen, die über Massenveranstaltungen Krankheitserreger verteilen, politische Attentate mit Drohnen – der Fantasie sind hier kaum Grenzen gesetzt.

Auch können Drohnen als Spionagemittel zur Auskundschaftung von Liegenschaften eingesetzt werden. Paparazzi, Detekteien und Diebesbanden haben die fliegenden Roboter längst zu ihren Lieblingswerkzeugen erkoren. Dass selbst billige Spielzeug- und Kameradrohnen aus dem Elektronikmarkt heute gute Bildqualität und lange Flugzeiten liefern, spielt den Benutzern in die Hände.

Die steigende Anzahl der Hobby-Drohnenpiloten stört mittlerweile den Flugverkehr deutlich. Die Deutsche Flugsicherung hat 2016 über 60 Störfälle registriert, in 2015 waren es noch 12. Drohnen können aber natürlich auch absichtlich als Angriffsmittel gegen landende oder startende Flugzeuge eingesetzt werden und bestimmte Maschinen beschädigen oder im Schwarm den Flugbetrieb eines Großflughafens lahmlegen.

Der Gesetzgeber ist bereits aktiv geworden und hat für Drohnen größer als 0,25 kg eine Kennzeichnungspflicht eingeführt. Ab 2 kg fordert das Gesetz einen Kenntnisnachweis des Piloten und ab 5 kg gar eine Flugerlaubnis. Da der Kauf einer Drohne jedoch frei bleibt und Kriminelle sicher das Risiko, eine Drohne illegal zu steuern, nicht scheuen, sind solche Maßnahmen zur Abwehr von Straftaten kaum ausreichend.

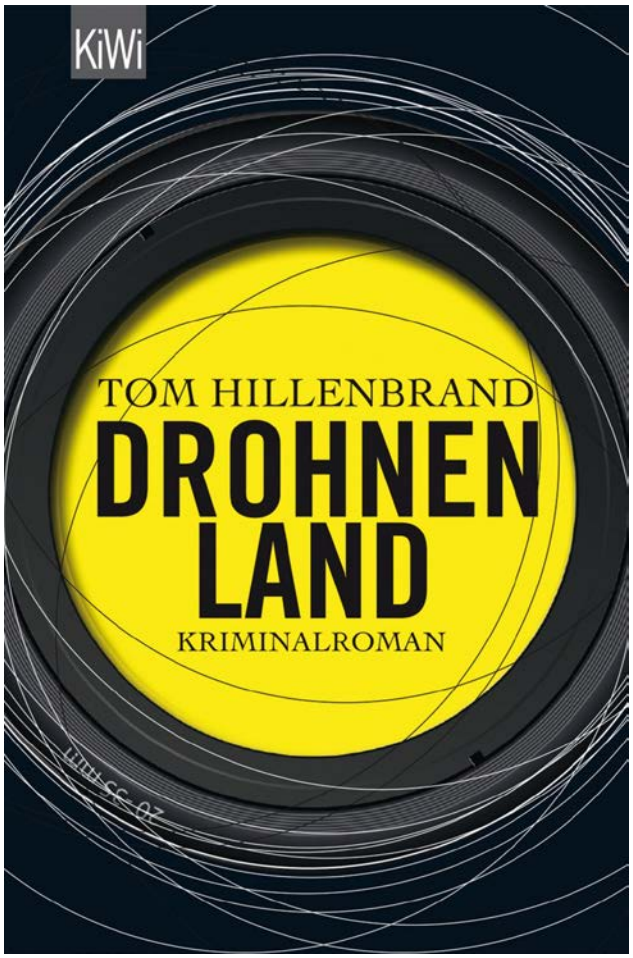
Bewertung der Drohnentechnologie für das eigene Unternehmen



Quelle: Corporate Trust 2017

Mehr und mehr setzen auch Wirtschaftsunternehmen Drohnen ein, um z.B. die „letzte Meile" in der Lieferlogistik zum Kunden oder für exponierte Adressaten zu überwinden. Hier werden dann neue Angriffsarten denkbar: das Kapern von Sendungen durch Luftpiraten (die z.B. mit GPS-Störsendern oder Piratendrohnen arbeiten), gezielte Angriffe auf die Logistikketten von Unternehmen oder Massenangriffe mittels Ransomware[1].

Besonders interessant sind Drohnen, die ein Ziel weitgehend autonom ansteuern. Solche Drohnen, die mit intelligenten Algorithmen oder künstlicher Intelligenz ausgestattet sind, werfen ganz neue Fragen auf, wie Sie auch im Zusammenhang mit selbstfahrenden Autos diskutiert werden. Wer trägt Schuld für einen Unfall? Wie muss sich eine Drohne verhalten, wenn Menschenleben in Gefahr sind?



Lesenswert: ein Kriminalroman rund um das Thema Drohnen

Der Ausblick in die Zukunft ist vielfältig. Hybriddrohnen, die fliegen, schwimmen und auf Rädern fahren können, sind bereits im Anmarsch. Minidrohnen werden kleiner und kleiner, während große Lastdrohnen mittlerweile ganze Schiffscontainer befördern können. Spezialdrohnen für die Feuerwehr, die Luftaufklärung, die Identifizierung von Menschen in Massenveranstaltungen mittels Gesichtserkennung, die Erkennung von auffälligem menschlichem Verhalten oder den bewaffneten Kriegseinsatz – der Fantasie scheinen kaum Grenzen gesetzt.

Und während die Drohnendetektion mittlerweile zumindest im Nahbereich gut gelingt, ist die Abwehr, wie bereits erwähnt, noch nicht sauber gelöst. Die Unterbrechung von Funksignalen bzw. die Übernahme der Steuerung funktioniert bei autonomen oder teilautonomen Drohnen systembedingt nicht.

Der Einsatz von speziell ausgebildeten Greifvögeln, z.B. Adlern, die gefährliche Drohnen vom Himmel holen, wurde zwar schon erfolgreich beim französischen Militär und Polizei etabliert. Anders als technische Lösungen skaliert die Vorgehensweise mit den Abwehr-Adlern jedoch nicht, weil die Zahl der Greifvögel wegen ihres langwierigen Trainings nicht beliebig erhöht werden kann.

Auch die Nutzung von Abfangdrohnen ist komplex und fehleranfällig. Der Abschuss einer „feindlichen" Drohne ist häufig nicht legal und die Frage nach den Kollateralschäden bei einem Drohnenabschuss ungeklärt. Eine schnelle technische Entwicklung, gepaart mit schlechten Abwehrmöglichkeiten, zeigt uns auf, dass wir, was die Auswirkungen der Drohnentechnologie angeht, noch ganz am Anfang stehen.

Bei all den Gefahren und Risiken, die von Drohnen und Menschen (Drohnenoperatoren) ausgehen können, darf nicht vergessen werden, dass Roboter und Drohnen eine Vielzahl an industriellen Einsatzmöglichkeiten bieten. Das reicht, oftmals in Kombination mit entsprechenden Hochleistungssensoren, von hochpräziser Vermessung und Zustandserfassung mittels UAV-Laserscanner, der Ableitung genauester 3D-Modelle und 3D-Visualisierungen, teilautomatisierter Detektion, exakter Verortung und Dokumentation bis hin zur Analyse von Schäden und Gefahrenpotentialen an Objekten.

1) Ransomware (von englisch „ransom" für Lösegeld) sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf seine Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Die Daten auf dem Computer werden dabei meist verschlüsselt, um für die Entschlüsselung ein Lösegeld zu fordern.

Sicherheitstrends der Zukunft

Drohnen: Das Auge im Himmel

„Digitalisierung und autonome Zustandserfassung mittels unbemannter Luftfahrzeuge", wie es bspw. die österreichische Firma Bladescape Airborne Services in ihrem Leistungsspektrum zusammenfasst, kann im industriellen Segment wesentlich zur Erhöhung der Sicherheit von Objekten, deren Umfeld und involvierten Personen beitragen. Durchdachte, komplexe Sicherheitskonzepte (Security 4.0) können den Einsatz von Drohnen zur Steigerung der Effizienz und als Lösungsansatz zur Drohnenabwehr zielführend kombinieren. Drohnen könnten ja nicht nur als Angriffsmittel verwendet, sondern beispielsweise auch als Aufklärer im weiteren Vorfeld eingesetzt werden.

Wollte man einen Katalog an Einsatzmöglichkeiten erstellen, würde man bald zur Kenntnis nehmen müssen, dass sich solche Kataloge schwer erstellen lassen, da die Einsatzmöglichkeiten sehr vielfältig sind und sich permanent erweitern.

Das bedeutet aber, dass es in naher Zukunft vor allem im verbauten urbanen Bereich zu einem ziemlichen Gedränge am Himmel kommen könnte. Wie erwähnt, bieten sich Transportdrohnen vor allem für das letzte Stück des Zustellungsweges als individueller Lieferservice an. Um diesem Gedränge vorzubeugen, sollten Verkehrsplaner schon jetzt daran denken, ob die Einrichtung von „Drohnen-Highways" in der Luft sinnvoll sein könnte.

Das führt wieder zu der Frage: Und was passiert, wenn Drohnen sich nicht an die vorgegebenen Highways halten? Nun, da könnte man über eine Art Geo-Fencing nachdenken, um die Drohnen auf die Highways zu zwingen. Das würde aber bedeuten, dass die Hersteller solche „hoheitlichen" Eingriffsmöglichkeiten schon vorprogrammieren müssen, da die direkte Intervention bei autonomen, vorprogrammierten Systemen noch nicht zufriedenstellend funktioniert.

Der oben begonnene Gedankengang führt unweigerlich zu einer weiteren relevanten Sicherheitsfrage: Wie wird man eines Systems Herr, das sich verselbständigt? Diese Frage bezieht sich nicht nur auf die fliegende oder hybride Robotervariante, sondern auf alle – vor allem auf intelligente, selbstlernende Systeme, deren gedankliche, sich selbst programmierende Entwicklung (Stichwort: Künstliche Intelligenz) ja nicht immer vorhersagbar sein kann. Wie wir wissen, tun wir uns bereits bei der Abwehr von herkömmlichen Drohnen relativ schwer.

Wie werden die öffentlichen und privaten Sicherheitsorgane etwa auf amoklaufende, sich verselbstständigende Drohnen reagieren? Wird es eigene Polizeispezialkräfte für diesen Job geben – wie die „Blade Runner" im gleichnamigen Science-Fiction-Film von 1982 – die außer Kontrolle geratene Robotersysteme eliminieren? Diese Themen werden uns wahrscheinlich schon in naher Zukunft intensiv beschäftigen.

Alles, was digitalisierbar ist, wird digitalisiert werden. Alles.

Peter Glaser, Ehrenmitglied des Chaos Computer Club (CCC),
Autor u.a. des deutschen Technology Review

Sicherheitstrends der Zukunft

Privatsphäre im 21. Jahrhundert

Die IT-Branche bewegt sich so rasend schnell, dass sie das Datenschutzrecht mit jeder neuen Entwicklung vor Herausforderungen stellt.

Autor:

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit
& Computerkriminalität
Corporate Trust

Stellen Sie sich die Google-Homepage vor. Oberhalb und rechts von den Suchergebnissen gibt es dort einen freien Platz. Wenn Google Ihnen nun anbieten würde, zehn zufällig ausgewählten Google-Besuchern weltweit dort Ihre Werbung zu zeigen: Wie viel wäre Ihnen das wert? Wahrscheinlich sehr wenig. Wie aber wäre es, wenn Google Ihnen anbiete würde, Ihre Werbung zehn Uni-Absolventen zu zeigen, die laut ihren Profilen perfekt zu Ihrem Unternehmen passen – z.B. mit Auslandserfahrung in China, Einser-Examen und gerade in Ihrer Region auf Jobsuche? Der gleiche Werbeplatz auf der Google-Seite ist umso mehr Geld für Google wert, je besser das Unternehmen seine Besucher kennt.

Dieses sogenannte Profiling, das Sammeln von Daten über Benutzer, ist in Verruf geraten und wird von den meisten Benutzern prinzipiell abgelehnt. Aber Alternativen haben es schwer: Stellen Sie sich vor, ein Jungunternehmer käme zu Ihnen und würde Ihnen eine neue Geschäftsidee vorstellen. Er wird eine Suchmaschine aufbauen, die genauso gut ist wie Google, aber kein Profiling macht, und die statt auf Werbeeinahmen ausschließlich auf ein Abo-Modell für 3,99 EUR pro Monat setzt. Würden Sie Geld in seine Firma investieren? Die meisten Investoren würden das nicht. Die Wahrheit ist nämlich, dass die meisten Internetnutzer es durchaus schätzen, dass Google seine Dienstleistungen kostenlos anbietet – auch wenn sie dafür persönliche Daten herausrücken müssen.

Internetnutzer sind in der Regel schizophren: Im Prinzip lehnen sie Profiling à la Big Brother ab. Aber wenn ein nützliches Online- oder App-Angebot um die Ecke kommt, das ihnen gefällt, geben sie gerne auch sensible Daten heraus. Wir alle ticken so.

Google liefert eine hochwertige und komplexe Dienstleistung, die nicht billig herzustellen ist. Das Unternehmen benötigt viel Geld, um eine Suchmaschine im Internet anbieten zu können. Geld kann Google aber nur über noch besseres und detaillierteres Profiling verdienen. Und das betrifft nicht nur Google, sondern faktisch auch jeden anderen Dienst, der auf ein werbebasiertes Geschäftsmodell setzt. Gesetzliche Regelungen zur Datensparsamkeit oder gegen Profiling greifen hier ins Leere: die Benutzer schätzen das Geschäftsmodell – vor allem wegen der scheinbar geringen Kosten, aber durchaus auch, weil gute, passende Werbung durchaus interessant sein kann.

Zugleich teilen Nutzer massenhaft intime Daten – freiwillig – in sozialen Netzwerken, Kontaktbörsen, Messengern, Film- und Fotoportalen. Auch hier sind die meisten Dienste kostenlos und werbefinanziert und nutzen diese Daten im Gegenzug für Profiling.

Nehmen wir die „smarte" Haustechnik: Ob Kühlschrank, Heizungssystem oder Videoüberwachung – heute wird für alle Arten von Haushaltsgeräten die Vernetzung mit dem Internet angeboten. Der Kühlschrank meldet dann per SMS, dass die Milch alle ist; das Heizungssystem fährt hoch, bevor man zuhause eintrifft und lässt sich fernsteuern; und die Innenraum-Überwachungskamera springt an, wenn daheim eingebrochen wird. Da bleibt es nicht aus, dass Daten über unser Leben aus unserem trauten Heim abfließen.

Oder beim Thema Gesundheit: Gewicht, Puls, Blutwerte, Schlafgewohnheiten und Bewegungspensum werden durch Fitnessarmbänder gesammelt – Teil des neuen Megatrends „Quantified Self", die quantitative Auswertung des eigenen Lebensalltags. Dazu gehören auch Computer, die in Brille, Kleidung oder Schmuckstücke integriert sind, und die versteckte Mikrofone und Kameras enthalten. Und alle so erlangten Daten werden gesammelt und sowohl dem Benutzer als auch – mehr oder weniger offensichtlich – Drittabnehmern zur Verfügung gestellt.

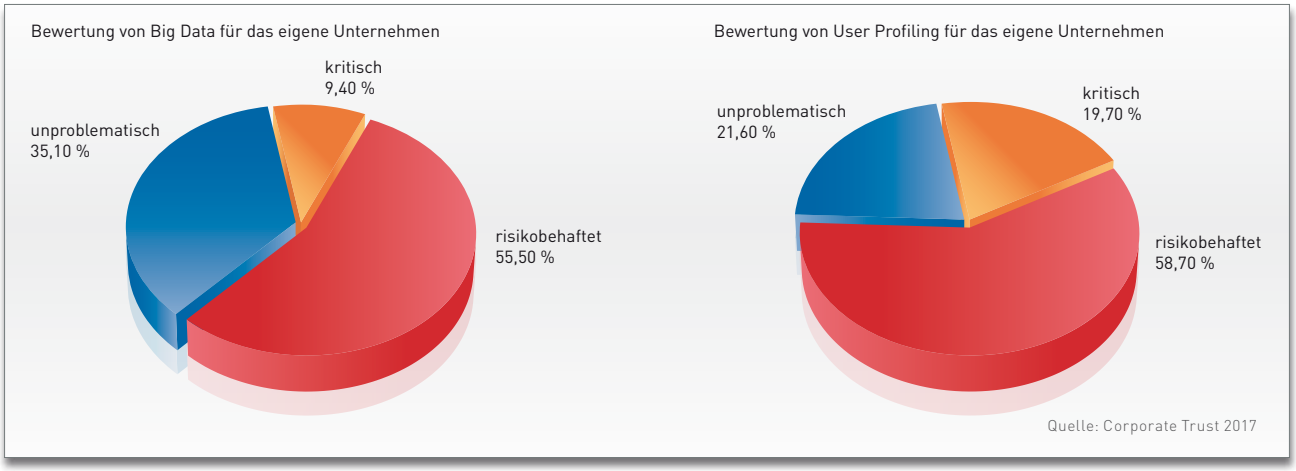
Ein Hersteller von Roboterstaubsaugern etwa hat jüngst angekündigt, sein Wissen über die Grundrisse der Kundenwohnungen an Dritte, z.B. Möbelhersteller und Online-Händler, verkaufen zu wollen (anonymisiert, versteht sich). Um möglichst viele Daten zu sammeln, werden durch die Verkaufserlöse der Informationen häufig die Geräte subventioniert, so dass wir heute den Preis eines Haushaltsgeräts zum Teil auch mit den eigenen Daten bezahlen.

Das ist alles schon Realität. Die uneingeschränkte Privatsphäre ist also faktisch bereits tot. Und wir selbst haben den Abzug gedrückt.

Die intelligente Auswertung all dieser nutzerbezogenen Daten – das ist nun Big Data – bietet die nächste Zündstufe unserer technologiedurchsetzten Zukunft. Als logische Folge all unserer Aktivitäten füllen sich weltweit riesige Datenbanken, die Nutzerinformationen sammeln und in der Lage sind, trotz großer und unübersichtlicher Datenmengen, komplexe Anfragen in kurzer Zeit zu beantworten. Zum Beispiel, wie erwähnt, welche zehn Uni-Absolventen Auslandserfahrung in China haben, ein Einser-Examen vorweisen und gerade in einer bestimmten Region auf Jobsuche sind, siehe unser Beispiel oben.

Mit Big Data können Vorhersagen aus der Nutzerhistorie abgeleitet werden (sog. Predictive Analytics). Und mit Echtzeitauswertungen kann schnell und automatisiert auf neue Chancen reagiert werden (sog. Complex Event Processing). Solche System werden in immer mehr kritischen gesellschaftlichen Prozessen eingesetzt: bei Börsenhandel, polizeilicher Gefahrenabwehr, Kredit-Scoring, Versicherungen etc.

Dennoch ist Big Data gesellschaftlich durchaus umstritten, was sich auch in unserer diesjährigen Umfrage bei deutschen Unternehmen widerspiegelt:

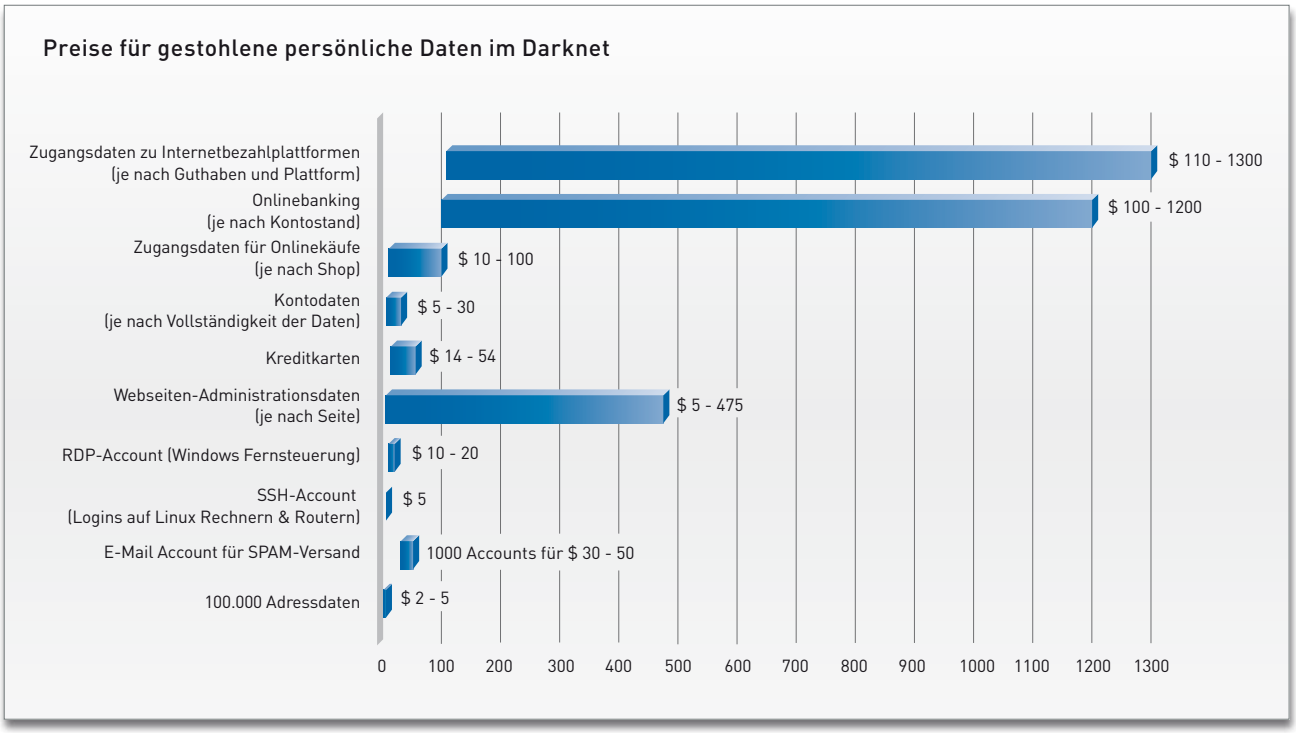


Sicherheitstrends der Zukunft

Privatsphäre im 21. Jahrhundert

Während die Möglichkeiten solcher Technologien immer weiter ausgetestet werden, schenken die Entwickler der Manipulationsgefahr derzeit noch zu wenig Aufmerksamkeit. Das Risiko von Datendiebstählen steigt: große Datenmengen sind viel Geld wert. Das weckt Begehrlichkeiten. Dementsprechend aufwendig ist der Schutz der damit befassten IT-Systeme. Dieser Schutz aber kostet Geld – daran wird bei der Entwicklung anfangs oft gespart.

Die organisierte Kriminalität hat das längst erkannt und Geschäftsmodelle entwickelt, die auf der Verwertung persönlicher Daten beruhen. Steigende Fallzahlen für Identitätsdiebstahl sowie die Preise für persönliche Daten aus dem sogenannten Darknet – dem Tummelplatz für Kriminelle im Internet – belegen dies.



Gefahr droht aber nicht nur durch externe Hacker, auch die Gefahr von Innentätern darf nicht vernachlässigt werden. So waren z.B. die Steuer-CDs, die der deutsche Fiskus gekauft hat, auch nicht durch Hacker von außen, sondern durch eigene Mitarbeiter der jeweiligen Banken gestohlen worden.

Dem riesigen, von den Benutzern weitgehend akzeptierten Geschäftsmodell „Datensammlung" steht die Datenschutzgesetzgebung diametral gegenüber. Das bisherige deutsche Datenschutzrecht war zwar sehr konkret, durch die schwache Strafandrohung am Ende jedoch ein zahnloser Tiger.

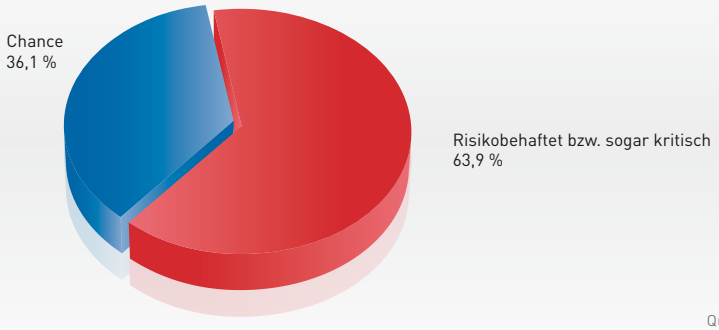
Die neue europäische Datenschutzrichtlinie droht zwar nun mit sehr empfindlichen Strafen, ist aber rechtlich sehr komplex und birgt noch große Unsicherheiten. In den Firmen wird der Datenschutz oft als Geschäftsverhinderer gesehen und der Datenschutzbeauftragte als „Frühstücksdirektor" besetzt. Auch die Ausstattung der Datenschutzbehörden in den Bundesländern ist häufig dem Thema nicht angemessen. Noch komplexer wird die rechtliche Situation international: Das Safe Harbor Abkommen[1] mit den USA wurde vor Gericht gekippt, das neue EU-US Privacy Shield steht noch auf dem Prüfstand.

1) Das Safe-Harbor-Abkommen (englisch für „sicherer Hafen") ist ein Beschluss der Europäischen Kommission auf dem Gebiet des Datenschutzes aus dem Jahr 2000. Durch das Abkommen, das die EU mit den USA schloss, sollte es Unternehmen ermöglicht werden, personenbezogene Daten in Übereinstimmung mit der europäischen Datenschutzrichtlinie aus der EU in die USA zu übermitteln. Der Europäische Gerichtshof (EuGH) erklärte jedoch das Abkommen am 6. Oktober 2015 für ungültig. Seit dem 1. August 2016 kann eine Nachfolgeregelung angewendet werden, die den Namen EU-US Privacy Shield trägt.

Dabei unterscheidet sich die Datenschutzgesetzgebung in Europa und Amerika systematisch. Während in Europa der Staat möglichst klare Regeln vorgeben will, muss sich eine Firma in Amerika im Wesentlichen an das halten, was sie dem Benutzer verspricht. Wenn eine US-Firma das nicht tut, verfolgt die für Verbraucherschutz zuständige Federal Trade Commission (FTC) das sehr unnachgiebig und die Strafen durch das Rechtssystem (Sammelklagen, Jury-Urteile und Strafzahlungen) sind drakonisch.

In einigen Bereichen kann man in der 2018 wirksam werdenden europäischen Datenschutzgrundverordnung (DSGVO) aber schon die Übertragung von Verantwortlichkeiten von den zuständigen nationalen Behörden (in Österreich: Datenschutzkommission) auf die Daten-Verarbeiter (Behörden und Unternehmen) erkennen. Wo früher eine einfache Meldung einer Datenanwendung an die Datenschutzkommission gereicht hat (die dann in das Datenverarbeitungsregister (DVR) aufgenommen wurde), wird nun die Verantwortlichkeit hinsichtlich Schutz von personenbezogenen Daten (die DSGVO schützt vorrangig Daten von natürlichen Personen) den Verarbeitern oder den von diesen Beauftragten Dienstleistern übertragen. Das heißt, die für den Schutz der relevanten Daten Verantwortlichen haben in Eigenverantwortung eine risikomanagementbasierte Datenschutz-Folgeabschätzung vorzunehmen und ihre Datenschutzorganisation dahingehend in die jeweilige Organisation zu implementieren. Die Überwälzung der rechtlichen Verantwortlichkeit, wie sie in anderen Bereichen (beispielsweise in der Gewerbeordnung) entsprechend der Bestimmungen des Verwaltungsstrafgesetzes möglich ist, fällt nun weg. Die zuständige Behörde assistiert maximal bei Unklarheiten im Rahmen eines Konsultationsverfahrens.

Sehen Sie das Europäische Datenschutzgesetz als Chance oder eher risikobehaftet bzw. sogar kritisch für Ihr Unternehmen?



GRAFIK 18

Quelle: Corporate Trust 2017

Der europäische Weg in der Datenschutzgesetzgebung steht massiv unter Druck. Hauptsächlich kommt dieser Druck von den Benutzern selbst, von denen viele sich immer öfter für subventionierte Angebote im Internet entscheiden (während sie innerlich Profiling und Big Data generell ablehnen, versteht sich). Und er kommt von der europäischen IT-Industrie, die den Datenschutz nach europäischem Vorbild für innovationsfeindlich hält. Sie befürchtet, dass innovative Produkte, die Big-Data-Analysen nutzen, in Zukunft vor allem aus Nordamerika und Asien kommen werden, wo Datenschutz deutlich weniger streng ist.

Zweifellos: Die IT-Branche bewegt sich so rasend schnell, dass sie das Datenschutzrecht mit jeder neuen Entwicklung vor Herausforderungen stellt. Ein relativ leichter Ausweg aus dieser Lage wäre mehr Anonymität im Internet. Es hat sich in der Vergangenheit aber gezeigt, dass dieser Schutz besonders oft von Kriminellen für ihre Taten missbraucht wird.

In den nächsten Jahren werden wir neue Rechtsinstrumente brauchen, um den Missbrauch von Datensammlungen und den gläsernen Bürger zu verhindern.

Wir brauchen ein Recht auf Pseudonyme und Schulungen im Umgang damit im Netz. Wir brauchen das Recht auf Löschung aller persönlichen und selbst eingestellten Daten bei einem Anbieter – es geht nicht, dass dieser, wie z.B. Facebook, zum Eigentümer der Daten wird. Wir brauchen eine Verpflichtung von Anbietern, alle persönlichen Daten in einem dokumentierten Standardformat exportieren zu können, um Profile wirklich zu einem anderen Anbieter „umziehen" zu können und so einen echten Wettbewerb in Sachen Datenschutz und Sicherheit in Gang bringen zu können.

Die Privatsphäre, wie wir sie bisher kannten, ist tot. Wir sollten alle daran arbeiten, einen gesunden Mittelweg zwischen innovationsfeindlichem Misstrauen und „Big Brother"-ähnlicher Totaltransparenz zu finden. Am Ende hängen unsere persönliche Freiheit als Bürger, aber auch unser zukünftiger Wohlstand davon ab.

Sicherheitstrends der Zukunft

Wettrüsten im Cyberraum

Aktuell findet im Cyberbereich ein unkontrolliertes Wettrüsten statt, das mit dem atomaren Wettrüsten zu Anfangszeiten des Kalten Krieges vergleichbar ist.

Autor:

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit
& Computerkriminalität
Corporate Trust

Als Max M., Klinik-Direktor einer gut ausgestatteten Privatklinik, an jenem Junimorgen seinen Computer hochfährt, erscheint auf dem Bildschirm eine giftgrüne Schrift. Er liest „Encrypted" und weiß zunächst nicht, was das bedeutet. So viel ist klar: Das Computersystem funktioniert nicht - im gesamten Krankenhaus. Irgendwann wird deutlich, dass alle Daten verschlüsselt sind. Ein Mitarbeiter hat auf den Anhang einer gut gemachten und täuschend echt aussehenden E-Mail geklickt. Die daraufhin gestartete Schadsoftware hat sich in Windeseile im ganzen Krankenhausnetz verbreitet. Nachdem das Computersystem inklusive der modernen IT-gestützten medizinischen Geräte übernommen worden war, forderten die Hacker Lösegeld in Bitcoins. Er fand erst später heraus, dass es sich dabei um eine digitale Krypto-Währung handelt. Eine Säuberung braucht zu viel Zeit, Operationen müssten verschoben, Bestrahlungen abgesagt, Patienten verlegt werden. Die Klinik zahlt.

Ist so etwas möglich? Woher sollten Erpresser dieses Know-how haben? Die Antwort ist leider ja, genau das ist bereits passiert. Der geschilderte Fall ist nicht fiktiv. Eine Gruppe namens „ShadowBrokers" hat einige Monate zuvor Cyberwaffen von einer Einheit namens „EquationGroup" entwendet. Die EquationGroup wiederum ist ein Code-Name für eine Arbeitsgruppe innerhalb des amerikanischen Nachrichtendienstes NSA, genau genommen der Abteilung S32 für sogenannte „Tailored Access Operations" (gezieltes Eindringen). Diese hochentwickelten Waffen wurden angepasst und für einen Angriff auf Wirtschaftsunternehmen verwendet. Selbst gut gewartete und ausgestattete IT-Netzwerke sind solchen ausgefeilten und mit viel Geld für den Cyberwar entwickelten Waffen nicht gewachsen. Nähere Informationen dazu finden Sie in unserem NSA Report, Seiten 44 und 85 (https://www.corporate-trust.at/de/portfolio-items/nsa-report?portfolioCats=5%2C12).

Aktuell findet im Cyberbereich ein unkontrolliertes Wettrüsten statt, das mit dem atomaren Wettrüsten zu Anfangszeiten des Kalten Kriegs vergleichbar ist. Die Gefahr ist nicht ein tausendfacher Overkill des Planeten, sondern die konkrete Bedrohung der Wirtschaft und unserer modernen Lebensweise. Das Potenzial von Cyberwaffen wächst mit jeder neuen IT-Revolution und wird im Zeitalter von Industrie 4.0, selbstfahrenden Autos, computergesteuerten Stromnetzen und dem „Internet of Things" eine Zerstörungskraft erreichen, die man durchaus mit einem atomaren Angriff vergleichen kann.

Die Veröffentlichungen von Edward Snowden haben die Cyberfähigkeiten der NSA einer breiten Öffentlichkeit plastisch vor Augen geführt. Er hat damit ein klar ausgesprochenes Ziel verfolgt. Er wollte, dass die Aktionen von Geheimdiensten besser kontrolliert werden. Das mag an einzelnen Stellen auch funktioniert haben. Auf einem globalen Maßstab betrachtet ist aber leider das Gegenteil

Einladung zur Auktion der Cyber-Waffen der NSA-Elitegruppe "Equation Group" durch eine Gruppe namens „Shadow Brokers:

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

passiert. Vielen Staaten wurde vor Augen geführt, wie weit der Vorsprung des amerikanischen, militärisch-industriellen Komplexes im Cyberbereich ist.

Seit den Veröffentlichungen von Edward Snowden wurden in jedem G20 Land und in nahezu jedem anderen Staat die Ausgaben für Spionage und Angriffe im Cyberbereich erhöht. Nach dem Vorbild der NSA sind rund um die Welt weitere aktive Cybereinheiten entstanden, die wie kleine „Mini-NSAs" agieren und ihre eigenen Arsenale von Cyberwaffen aufbauen. Mit diesen „Exploits" genannten Softwarestücken kann man in geschützte IT-Systeme eindringen, Informationen stehlen oder Computer lahmlegen. Die Idee hinter einem solchen Exploit ist oft genial und einzigartig. Da die „Waffen" im Einsatz von verschiedensten Personen benutzt werden sollen, sind sie in der Bedienung möglichst einfach und entsprechend gut dokumentiert. Die Wertigkeit einer Cybereinheit bemisst sich anhand der Anzahl und Qualität der Exploits, die sie in ihrem Arsenal hat. Die Entwicklungszeit von Geheimdienst- oder Militäreinheiten bemisst sich nicht in Monaten, sondern in Jahren. Die Ergebnisse der momentan laufenden Entwicklung werden also erst nach und nach sichtbar.

Am besten kann man die künftige Entwicklung wohl am Beispiel des bisher fortschrittlichsten Cyber-Geheimdienstes der Welt nachvollziehen, der NSA. In den letzten Jahren wurden dem Geheimdienst von vier verschiedenen Whistleblowern Informationen gestohlen (Binney, Tice, Drake, Snowden). Darüber hinaus wurden sowohl der NSA als auch der CIA im letzten Jahr Cyberwaffen entwendet. Dabei unternimmt die NSA sogar große Anstrengungen, um das eigenen Know-how zu schützen. Die Abteilung Q (Security & Counter-Intelligence) ist zuständig für den Schutz der NSA-Einrichtungen, die Spionageabwehr sowie den zivilen und militärischen Personenschutz. Außerdem stellt sie die bewaffnete und uniformierte NSA-interne Polizeitruppe. Zusätzlich ist die 3.000 Mann starke Abteilung „Information Assurance" für die Abwehr von Cyberangriffen zuständig.

In der klassischen Sicherheit hat der Verteidiger zwei Möglichkeiten, um einen Dieb aufzuhalten, nämlich beim Eindringen oder beim Wegschaffen des Diebesguts. Im Cyberbereich zeigt sich hier ein Grundproblem der virtuellen Welt. Am Ende sind es nur Bits und Bytes, die kopiert, manipuliert oder gelöscht werden. Um eine Atomwaffe zu stehlen, ist ein erheblicher Logistik- und Transportaufwand notwendig. Ein Stück Software kann man in jeder Jackentasche oder sogar E-Mail verstecken. Der Aufwand für einen Diebstahl reduziert sich daher im Wesentlichen auf das Eindringen in ein System.

Cyberwaffen haben noch eine weitere besondere Eigenschaft. Manche dieser Waffen hinterlassen Spuren, durch deren Analyse man die Idee hinter der Waffe herausfinden kann. Ein Experte kann diese Waffe dann nachbauen oder eine Verteidigung dagegen entwickeln. Es besteht also die Gefahr, dass durch den Einsatz einer solchen Waffe diese in falsche Hände gerät oder nutzlos wird. So ist dies z.B. bei Stuxnet geschehen, dem Programm, das für den Angriff auf das iranische Atomprogramm entwickelt wurde. Teile von Stuxnet bzw. die Ideen dahinter finden sich noch heute in vielen Schadprogrammen, die gegen die Wirtschaft eingesetzt werden.

Im Verhältnis zur klassischen Sicherheit ist der Verteidiger im Cyberraum damit systematisch im Nachteil. Während ein Angreifer nur EINE Lücke finden muss, muss der Verteidiger alle Lücken absichern. Der Spruch „Angriff ist die beste Verteidigung" gewinnt im Cyberraum damit eine neue Relevanz. Dementsprechend setzen die meisten militärischen Einheiten eher auf eine Doktrin der Abschreckung und entwickeln ständig neue, hochentwickeltere Cyberwaffen. Solange aber staatliche Cybereinheiten überall auf der Welt aufrüsten und gleichzeitig Hackergruppen deren Arsenale stehlen können, wird sich die Wirtschaft ständig hochentwickelten Cyberwaffen gegenübersehen. Damit wird die Verteidigung immer teurer. Der einzige Schutz besteht derzeit darin, dass die Chance einer nur noch eingeschränkten oder nicht mehr nutzbaren Cyberwaffe umso größer ist, je länger sie gelagert wurde.
Es geht aber nicht nur um die Waffen, sondern auch um die Menschen. Staatliche Stellen benötigen die gleichen IT-Sicherheitsexperten für Angriff, Spionage und Verteidigung wie die Wirtschaft zur Produktentwicklung und Verteidigung des eigenen Know-hows. Ein ohnehin leergefegter Personalmarkt an entsprechenden Fachkräften wird damit noch kleiner. Gleichzeitig steht der Verteidiger häufig auf verlorenem Posten – und wer will schon gerne der Verlierer sein?

Derzeit gibt es keine Regeln für diesen Kampf. Die Weitergabe sowohl des Basis-Wissens als auch der fertig aufbereiteten Waffen ist nicht strafbar. Dementsprechend hat sich ein reger Handel entwickelt. Es gibt Firmen, die kaufen Cyberwaffen von beliebigen Personen ein. Ein Beispiel wäre die Firma Zerodium. Die ursprünglich „Vupen" genannte Firma aus dem französischen Montpellier hat sich 2015 in Maryland, dem US-Bundesstaat in dem auch das Hauptquartier der NSA ist, neu gegründet. Grund war ein französisches Gesetz, das die Ausfuhr von Cyberwaffen unter Strafe stellt. Die Firma kauft Cyberwaffen an und verkauft bzw. vermietet diese danach an ihre Kunden. Die Preise für eine solche Cyberwaffe können sich sehen lassen: sie reichen von 10.000 USD für eine Lücke in der Webseitenverwaltung WordPress bis hin zu 500.000 USD für eine Lücke im iPhone Betriebssystem iOS.

Sicherheitstrends der Zukunft

Wettrüsten im Cyberraum

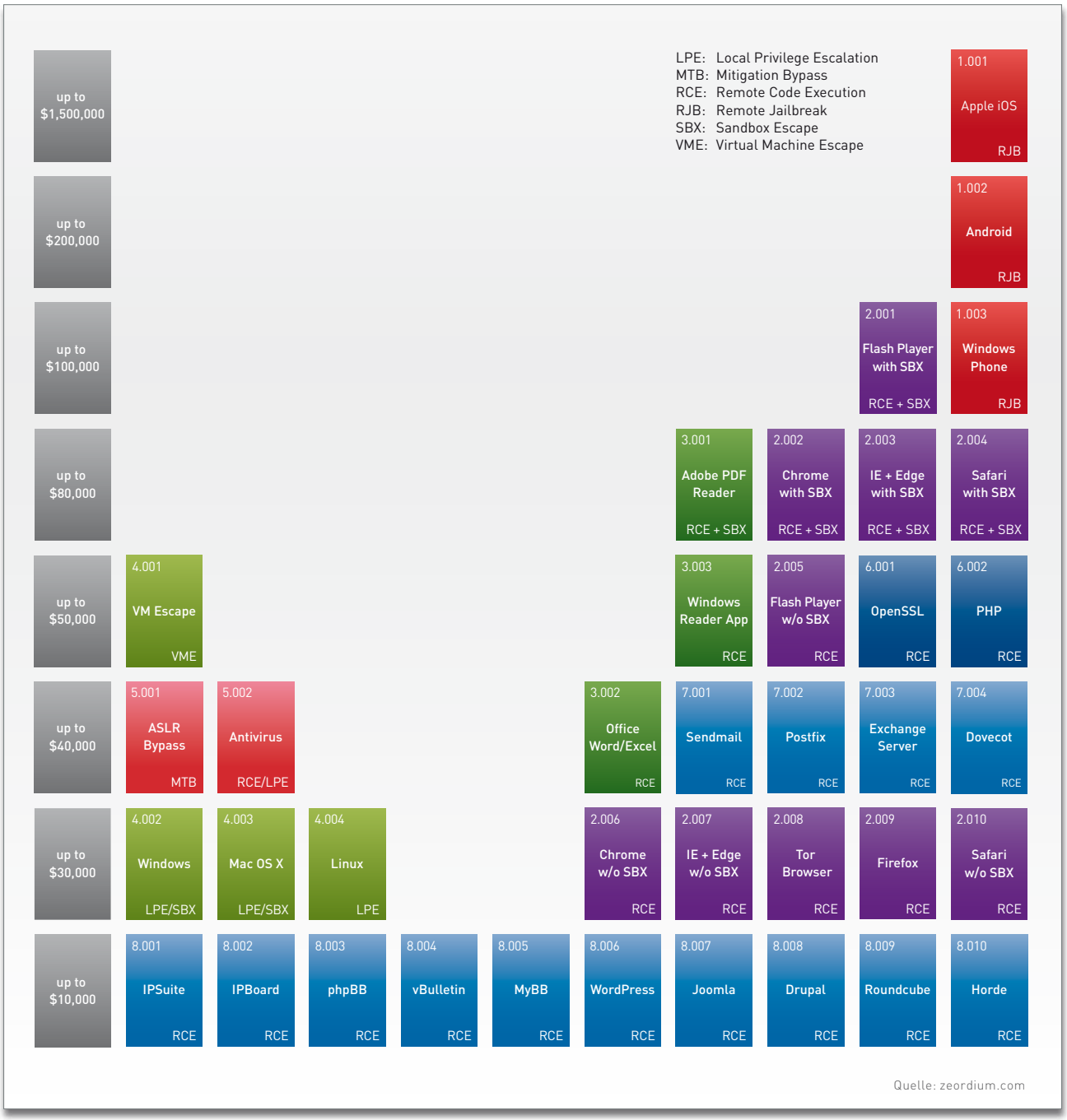
Gleichzeitig ist es im Cyberraum derzeit kaum möglich, einen Angriff klar einem bestimmten Angreifer zuzuordnen. Als Indizien werden hierfür z.B. häufig die Arbeitszeiten der Hacker eingesetzt, ihre eigenen Kommentare im Source Code oder die Art, wie sie sich auf einer englischen Tastatur vertippen. In jedem Fall sind solche Indizien eher schwach und leicht zu fälschen.

Operationen unter falscher Flagge, also Aktionen bei denen der Angreifer eine falsche Spur legt, um für jemanden anderes gehalten zu werden, sind daher leicht durchführbar. In einer solchen Situation dient die Zuordnung eines Angriffs meist nur den Interessen derer, die sie machen. Wenn also die Amerikaner einen bestimmten Cyberangriff Nordkorea zuordnen, dann stellt sich sehr wohl die Frage, wie viel das mit der Wahrheit und wie viel mit eigenen Interessen zu tun hat. In jedem Fall tun alle Beteiligten gut daran, Beschuldigungen im Cyberraum mit einer gewissen Skepsis zu begegnen. Dass Cyberangriffe kaum beweisbar sind, ist daher eine weitere große Hürde für eine notwendige Regulierung bzw. eine Strafverfolgung.

Gleichzeitig gäbe es durchaus Möglichkeiten für die Einschränkung der Cyberaktivitäten. Wenn eine Regierung die eigenen Einheiten anweist, bestimmte Länder nicht anzugreifen, dann kann man davon ausgehen, dass der Großteil sich an diese Regelung hält. Ein solches digitales Friedensabkommen wie es z.B. nach den Snowden Enthüllungen unter dem Begriff „No-Spy-Abkommen" in Deutschland diskutiert wurde, wird aber nur unter gleichwertigen Partnern zustande kommen. Die momentane Situation ist damit klar, es gibt nur wenige Freundschaften im Cyberraum. Der aktuelle Kampf folgt mehr einem „Jeder gegen Jeden" Prinzip als einer geregelten Auseinandersetzung mit klaren Frontlinien. Mitten zwischen den Fronten - und häufig genug in der Schusslinie - befindet sich dabei die Wirtschaft.

Die Politik ist hier gefragt. Wirtschaft und Zivilgesellschaft müssen davor geschützt werden, im Cyberraum zwischen die Fronten zu geraten. Es wird eine klare internationale Kontrolle für das Wettrüsten im Cyberraum und die Proliferation von Cyberwaffen benötigt. Gleichzeitig wird eine funktionierende und abschreckende Strafverfolgung für den Diebstahl und eine Sanktionierung für die Weiterverbreitung von Cyberwaffen benötigt. Es werden neue Einheiten bei der UNO und den internationalen Gerichtshöfen benötigt, die sich mit diesem Thema beschäftigen. Ohne durchgesetzte Regeln wird das Recht des Stärkeren den Cyberraum beherrschen und die Verteidiger werden verlieren. Je länger das Wettrüsten unkontrolliert weitergeht, umso größer wird die Diskrepanz zwischen Angreifer und Verteidiger und umso größer das Problem, vor dem wir am Ende stehen.

Einkaufspreise für Cyberwaffen bei Zerodium Anfang 2017



Quelle: zeordium.com

Derzeit ist ein Anwachsen von Mini-NSAs in aller Welt zu beobachten.

Dr. Ben Wagner, Direktor der Forschungsstelle Internet und Menschenrechte
an der Europauniversität Viadrina in Frankfurt an der Oder
17.12.2015

Glossar

Begriffserklärungen

- **Bitcoin**
  Eine digitale Geldeinheit eines weltweit verwendbaren dezentralen Zahlungssystems. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet mithilfe einer speziellen Peer-to-Peer-Anwendung abgewickelt, sodass anders als im herkömmlichen Bankverkehr keine zentrale Abwicklungsstelle benötigt wird. Eigentumsnachweise an Bitcoin können in einer persönlichen digitalen Brieftasche gespeichert werden.
- **Bug**
  Ein Programmfehler, Softwarefehler oder Software-Anomalie, bezeichnet im Allgemeinen ein Fehlverhalten von Computerprogrammen. Dies tritt auf, wenn der Programmierer eine bestimmte Festlegung der Spezifikation nicht oder falsch umgesetzt hat, oder wenn die Laufzeitumgebung fehlerhaft bzw. anders als erwartet arbeitet.
- **Dschihad**
  Der Begriff Dschihad (arabisch für Anstrengung, Kampf, Bemühung, Einsatz; auch Djihad oder in der englischen Schreibweise Jihad) bezeichnet ein wichtiges Konzept der islamischen Religion: die Anstrengung bzw. den Kampf auf dem Weg Gottes.
- **Fake President**
  Auch bekannt unter CEO Fraud. Dabei handelt es sich um eine Betrugsmasche, bei der Firmen unter Verwendung einer falschen Identität und meist gut gefälschten E-Mails, die einen anderen Absender vorgaukeln, zur Überweisung von Geld manipuliert werden.
- **Gentrifizierung**
  Als Gentrifizierung (engl. gentry für „niederer Adel") bezeichnet man den sozioökonomischen Strukturwandel bestimmter großstädtischer Viertel im Sinne einer Attraktivitätssteigerung für eine neue Klientel und dem anschließenden Zuzug zahlungskräftiger Eigentümer und Mieter. Damit verbunden ist der Austausch ganzer Bevölkerungsgruppen.
- **Global Terrorism Database (GTD)**
  Eine Datenbank, die Terroranschläge ab 1970 enthält. Betrieben wird die Datenbank durch das National Consortium for the Study of Terrorism and Responses to Terrorism (START) an der University of Maryland, College Park, USA. Sie ist auch die Basis für andere Maßnahmen zum Thema Terrorismus, wie z.B. den Global Terrorism Index (GTI), der vom Institute for Economics and Peace veröffentlicht wird.
- **Härten**
  Unter „Härten" versteht man in der Computertechnik, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist und deren korrekter Ablauf unter Sicherheitsaspekten garantiert werden kann. Das System soll dadurch besser vor externen Angriffen geschützt sein. Ziel ist es, ein System zu schaffen, das von vielen, auch weniger vertrauenswürdigen Personen benutzt werden kann.
- **Internet of Things (IoT)**
  Als Internet of Things (Kurzform: IoT) bezeichnet man die Vision einer globalen Infrastruktur der Informationsgesellschaft, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen. Die immer kleineren eingebetteten Computer sollen Menschen unterstützen, ohne abzulenken oder überhaupt aufzufallen. So werden z. B. Industrieanlagen oder Haushaltsgegenstände vernetzt bzw. miniaturisierte Computer, sogenannte Wearables, mit unterschiedlichen Sensoren direkt in Kleidungsstücke eingearbeitet.
- **Islamischer Staat (IS)**
  Eine seit 2003 aktive terroristisch agierende sunnitische Miliz mit zehntausenden Mitgliedern, die derzeit Teile des Irak und Syriens kontrolliert, wo sie seit Juni 2014 ein als „Kalifat" deklariertes dschihadistisches „Staatsbildungsprojekt" unterhält. Die Organisation ist auch in anderen Staaten aktiv und wirbt um Mitglieder für Bürgerkriege sowie Terroranschläge. Sie wird des Völkermords, der Zerstörung von kulturellem Erbe der Menschheit wie auch anderer Kriegsverbrechen beschuldigt.

- **Ransomware**
  Ransomware (von englisch „ransom" für Lösegeld) sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf seine Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Die Daten auf dem Computer werden dabei meist verschlüsselt und für die Entschlüsselung ein Lösegeld gefordert.
- **Social Engineering**
  Ausspionieren über das persönliche Umfeld durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwendung einer „Legende"). Social Engineering hat das Ziel, unberechtigt an vertrauliche Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.
- **Safe-Harbor-Abkommen**
  Das Safe-Harbor-Abkommen (englisch für „sicherer Hafen") ist ein Beschluss der Europäischen Kommission auf dem Gebiet des Datenschutzes aus dem Jahr 2000. Durch das Abkommen, das die EU mit den USA schloss, sollte es Unternehmen ermöglicht werden, personenbezogene Daten in Übereinstimmung mit der europäischen Datenschutzrichtlinie aus der EU in die USA zu übermitteln. Der Europäische Gerichtshof (EuGH) erklärte jedoch das Abkommen am 6. Oktober 2015 für ungültig. Seit dem 1. August 2016 kann eine Nachfolgeregelung angewendet werden, die den Namen EU-US Privacy Shield trägt.
- **Spear-Phishing**
  Gezielt gegen eine Person oder Organisation gerichtete Versuche, über gefälschte E-Mails an persönliche Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Es handelt sich dabei um eine Form des Social Engineering, bei der die Gutgläubigkeit des Opfers ausgenutzt wird.
- **Troll**
  Im Netzjargon eine Person, die ihre Kommunikation im Internet auf Beiträge beschränkt, die auf emotionale Provokation anderer Gesprächsteilnehmer zielt. Dies erfolgt mit der Motivation, eine Reaktion der anderen Teilnehmer zu erreichen.
- **User Profiling**
  Als User Profiling wird die Erstellung eines Profils über das Nutzerverhalten einzelner Menschen im Internet, meist zu Marketingzwecken, verstanden.
- **Watering-Hole-Angriff**
  Durch Cyberkriminelle werden gezielt Webseiten mit einem Schadcode infiziert, von denen der Angreifer weiß, dass seine potenziellen Opfer diese immer wieder aufsuchen (abgeleitet von Watering Hole – engl. für Wasserstelle, Kneipe, Bar). Das Ziel ist es, den Computer des Opfers zu infizieren, um sich darüber Zugriff auf das Netzwerk zu verschaffen.
- **Wearables**
  Tragbare Computersysteme, die während der Anwendung am Körper des Benutzers befestigt sind. Wearable Computing unterscheidet sich von der Verwendung anderer mobiler Computersysteme dadurch, dass die hauptsächliche Tätigkeit des Benutzers nicht die Benutzung des Computers selbst, sondern eine durch den Computer unterstützte Tätigkeit in der realen Welt ist.
- **World Economic Forum (WEF), Weltwirtschaftsforum**
  Eine in Cologny im Schweizer Kanton Genf ansässige Stiftung, die in erster Linie für das von ihr veranstaltete Jahrestreffen gleichen Namens in Davos bekannt ist. Dabei kommen international führende Wirtschaftsexperten, Politiker, Intellektuelle und Journalisten zusammen, um über aktuelle globale Fragen zu diskutieren. Diese umfassen neben der Wirtschafts- auch die Gesundheits- und Umweltpolitik. Das Forum gibt auch Forschungsberichte heraus.
- **Zero-Day-Lücken**
  Eine Zero-Day-Lücke ist eine systematische Möglichkeit, um eine Schwachstelle in der EDV auszunutzen, die meist bei der Entwicklung eines Programms entstanden ist und die von Angreifern eingesetzt wird, bevor es einen Patch als Gegenmaßnahme gibt. Dabei werden mit Hilfe von Programmcodes Sicherheitslücken und Fehlfunktionen von Programmen oder ganzen Systemen ausgenutzt, um sich Zugang zu verschaffen. Entwickler haben dadurch keine Zeit (null Tage = engl. zero day) die Software so zu verbessern, dass der Angriff wirkungslos wird.

Ansprechpartner

CORPORATE TRUST

Alfred Czech
Geschäftsführer
czech@corporate-trust.at

Christian Schaaf
Geschäftsführer (Deutschland)
schaaf@corporate-trust.de

Uwe Knebelsberger
Geschäftsführer (Deutschland)
knebelsberger@corporate-trust.de

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit
& Computerkriminalität
oelmaier@corporate-trust.de

Sebastian Okada
Prokurist, Leiter Prävention &
Ermittlungen Wirtschaftskriminalität
okada@corporate-trust.de

Ingmar Heinrich
Leiter Intelligence
heinrich@corporate-trust.de

PARTNER

Rechtsanwalt Heinrich Weiss
Geschäftsführer
heinrich.weiss@bvsw.de

Bayerischer Verband für Sicherheit
in der Wirtschaft, BVSW e.V.
www.bvsw.de

Martin Ehling
Leiter Vertrieb Deutschland Industrie und Handel
Martin.Ehling@brainloop.com

Brainloop AG
www.brainloop.com

CORPORATE TRUST

Sebastian Schramm
Intelligence
schramm@corporate-trust.de

Lars Unger
Auslandssicherheit
unger@corporate-trust.de

Sabina Slominska
Krisenmanagement
slominska@corporate-trust.de

Marie Jungk
Sicherheitsmanagement
jungk@corporate-trust.de

Corporate Trust
Business Risk & Crisis Management GmbH

www.corporate-trust.at
www.twitter.com/corporatetrust

Der Future Report wurde durch die Corporate Trust Business Risk & Crisis Management GmbH erstellt. Begleitet und unterstützt wurde der Report durch den Bayerischen Verband für Sicherheit in der Wirtschaft e.V. (BVSW) und die Brainloop AG. Selbstverständlich stehen Ihnen alle Ansprechpartner jederzeit gerne für Fragen zur Verfügung. Wir würden uns über Anregungen oder eine Nachricht bezüglich Ihrer Einschätzung für die Entwicklung von Sicherheitstrends freuen.

CORPORATE TRUST
Business Risk & Crisis Management GmbH

Kirchenplatz 7/5
A-3400 Klosterneuburg-Kierling

Tel.: +43 1 318 0151 0
Fax: +43 1 318 0151 10

info@corporate-trust.at
www.corporate-trust.at

Regelmäßig aktuelle Informationen
von Sicherheitsexperten

Follow us: twitter
www.twitter.com/corporatetrust