Bundesverband

Whitepaper

Wirtschaftsschutz in Deutschland

Nationale Herausforderungen im Lichte globaler Megatrends

Stand: 11. Januar 2016

Globale Megatrends bedrohen auch heimische Unternehmen am Standort Deutschland. Sie müssen sich dieser Gefahren bewusst werden und entsprechend aufstellen. Erfolgreich können sie nur im Verbund sein.

Vier globale Megatrends bedrohen die Sicherheit der deutschen Wirtschaft

Eine Reihe globaler Megatrends bedrohen die Sicherheit Deutschlands im Ganzen und die Sicherheit der deutschen Wirtschaft im Speziellen.

Megatrend Staatszerfall

Einer dieser Trends ist der Zerfall von Staatlichkeit rund um den Globus, insbesondere in Afrika. Nach dem Abzug der Kolonialmächte blieb den indigenen Völkern ein übergestülptes Staatssystem, mit dessen Führung sie gänzlich überfordert waren. So wurde der Staat letztlich als Beute verstanden, als Option, Profit zu machen. Staatliche Strukturen stehen dabei im Weg.

An dieser Bereicherung können lediglich einige Wenige partizipieren, ein Großteil der Bevölkerung wird ausgeschlossen. Diese Exklusion legt den Grundstein für einen Widerstand, welcher sich asymmetrisch in Form von Rebellenbewegungen und Terrorgruppen manifestiert. Ihm wird mit verstärktem Gewalteinsatz seitens der führenden Eliten begegnet, was wiederum dem Widerstand Sympathisanten in die Arme treibt. Sinkende Verteilungsspielräume auf Seiten der Machthaber, ausgelöst durch Gebietsverluste, weg brechende Unterstützung und sinkende Einnahmen sind Initialzündungen zu einer Abwärtsspirale, die Akzeptanz und Macht der Regierung schwinden lassen und in ein von Anomie geprägtes Machtvakuum führen. Der Staat zerfällt, Verteilungskämpfe und Unruhen brechen aus, eine Ökonomie der Bürgerkriege entwickelt sich.

Wo es keinen funktionierenden Staat gibt, können sich Terroristen und Kriminelle festsetzen – ohne mit Strafverfolgung rechnen zu müssen. Ihr Aktionsradius bleibt nicht regional beschränkt.

Auch der Ost-West-Konflikt im vergangen Jahrhundert ist als mitursächlich für die heutige Situation zu sehen. Die disparaten Anschauungssysteme der beiden Blöcke führten zur Unterstützung schwacher, oft totalitärer Staaten durch finanzielle Zuwendungen oder militärisches Gerät durch die Supermächte. Nach dem Zusammenbruch der Sowjetunion und dem Ende des Kalten Krieges waren diese Unterstützungen nicht länger notwendig. Die politischen und ökonomischen Systeme der Länder in der Dritten Welt hatten sich jedoch längst auf die ausländischen Zuwendungen eingestellt. So genannte Rentier-Staaten waren entstanden. Auch die in den Zeiten des Kalten Krieges gesäten Feindschaften zwischen Völkern überdauerten die Zeit des Ost-West-Konfliktes. Die einst gesäte Feindschaft trägt bis dato Früchte und ist Anlass für zahlreiche bewaffnete Auseinandersetzungen.

Während in vielen Teilen der Welt Nationen kollabieren, versuchen andere Staaten ihren Einfluss weiter auszudehnen. Zu denken wäre an den schwelenden Konflikt im Südchinesischen Meer, wo China durch Aufschütten künstlicher Inseln seine Gebietsansprüche auf die rohstoffreiche Region zu untermauern versucht. Näher dran an Deutschland ist der Ukraine-Konflikt, der ebenfalls auf eine expansionistische Politik einer Großmacht zurückzuführen ist. Letztlich jedoch darf man sich fragen, ob nicht auch diese, von vermeintlicher Stärke zeugenden Politiken auf eine innere Schwäche der Länder zurückzuführen sind und damit auch hier ein Zerfall von Staatlichkeit die Ursache ist.

Megatrend klimatische und ökologische Verwerfungen

Es ist der Klimawandel und es sind Eingriffe in die Natur, die einen weiteren Megatrend bedeuten: Globale klimatische und ökologische Verwerfungen. Ein Rückgang von Rohstoffen, insbesondere eine massive Wasserknappheit bis hin zur Desertifikation, Verseuchung weiter Landstriche, unkontrolliertes Abholzen und ein dramatisches Artensterben führen bereits jetzt zu lokal enormen Problemen und können künftig globale Verwerfungen mit sich bringen. Betroffen von dramatischen Umweltproblemen sind in erster Linie Schwellen und Entwicklungsländer, wo Umweltstandards meist keinerlei Bedeutung haben.

Aber auch Industrienationen wie die USA – insbesondere in Kalifornien – stehen vor massiven Herausforderungen aufgrund von Wassermangel. „Wasserkriege" drohen insbesondere in den Regionen von Nil, Indus, Jordan sowie Euphrat und Tigris.

Neben Krieg und Gewalt als großen Flüchtlingstreibern führen Hunger – ausgelöst durch Ernteausfälle aufgrund von Dürre – und künftig zunehmend Überschwemmungen zu massiven Flüchtlingsströmen. So sorgt der Klimawandel für mehr und heftigere Stürme und ein Ansteigen des Meeresspiegels, was vielen Menschen Land und Lebensgrundlage rauben wird.

Trinkwassermangel wird eine der weltweit größten Herausforderungen werden – mit weitreichenden Folgen auch für die deutsche Sicherheit.

Schnell bildet sich die Kausalkette Krieg/Hunger, Armut, Krankheit, Flucht bis zu Pandemien. Aberglaube, schlechte Hygiene, mangelnde ärztliche Versorgung und Hunger bieten einen idealen Nährboden für die Ausbreitung von Krankheiten, die dank moderner, schneller Transportmittel binnen kürzester Zeit die Welt umrunden können.

Megatrend Digitalisierung und Vernetzung

Ein rapide wachsender technischer Fortschritt im Sinne einer Digitalisierung und Vernetzung ist ein weiterer Megatrend. Vieles wird für uns dank Technik komfortabler, günstiger, sicherer, schneller erreichbar oder überhaupt erst erreichbar – einschließlich eines längeren Lebens. Wer mit seinem Auto von A nach B möchte, gibt das Ziel in sein Navigationssystem ein und wird geführt – Nachschlagen in Karten ist nicht mehr notwendig. Auf der Fahrt warnen Abstandssensoren bei Gefahr, Bremsassistenzsysteme helfen in kritischen Momenten und im Falle des Falls schützen einen Airbags.

Aber die Technik bietet auch zahllose neue Angriffsflächen. Sie macht uns verwundbarer. Wo sich Gasventile aus der Ferne regeln lassen, können diese auch bewusst fehlgesteuert werden. Wenn Stromzähler an das Internet angeschlossen sind, lassen sich diese von überall auf der Welt manipulieren und das Netz kann überlastet werden. Ein System, dass immer online ist, ist auch immer angreifbar. Wenn Computer miteinander vernetzt sind, kann ich über jeden dieser Computer das gesamte System angreifen.

Je mehr Systeme miteinander vernetzt und ans Internet angeschlossen werden, desto mehr Angriffsflächen bieten sich Kriminellen, Terroristen und fremden Staaten.

Die breite Vernetzung und das ständige Onlinesein erlauben es Angreifern jederzeit von jedem Fleck der Erde jedes System anzugreifen – ohne dabei entdeckt zu werden. Die erforderlichen Fähigkeiten sind vergleichsweise einfach zu erwerben.

Megatrend asymmetrische Bedrohung und hybride Kriegsführung

Aus dem technischen Fortschritt heraus erwächst ein weiterer Megatrend: Asymmetrische Bedrohung und hybride Kriegsführung. Militärisch relativ schwache Gruppen stellen sich ihren übermächtigen Gegnern nicht in einer offenen Feldschlacht. Angegriffen wird, wo der Feind eine Schwäche hat und man selbst nur wenig Ressourcen einsetzen muss. Die Folge sind (Terror-)Anschläge durch Autobomben oder Selbstmordattentate auf Polizeistationen, Patrouillen, Märkte oder Unternehmen. Oder der Angriff über den Cyber-Space. Hier ist der Übergang von asymmetrischen Bedrohungen zur hybriden Kriegsführung fließend.

Auch wer eine gewisse militärische Stärke besitzen mag, setzt diese nicht unbedingt offen ein. Irreguläre Kräfte ohne Abzeichen können „auf dem Feld" agieren, während gleichzeitig über das Netz begleitende Propaganda verbreitet wird. „Information Warfare" ist hier das Stichwort. Hierzu werden auch „feindliche" Webseiten gehackt und übernommen. Militärischen Aktionen gehen immer öfter Cyber-Attacken voraus. Diese müssen sich nicht auf militärische Ziele beschränken.

Staaten beschränken sich bei Angriffen nicht länger auf ihr Militär. Die Hemmschwelle, einen Konflikt auszutragen sinkt damit – und neue Ziele geraten ins Visier der Angreifer.

Implikationen für die deutsche Wirtschaft

Die aufgeführten Megatrends treffen auch die deutsche Wirtschaft. Der Zerfall von Staaten lässt Handelspartner wegbrechen, erschwert den Import von Zulieferprodukten sowie Rohstoffen und gefährdet Handelsrouten. Klimawandel und ökologische Katastrophen können dieselben Implikationen bedeuten. Aus beiden folgen zudem Flüchtlingsströme mit Auswirkungen auf die innere Sicherheit. Paris war ein blutiges Beispiel für die asymmetrische Bedrohungen. Die Digitalisierung und Vernetzung öffnet allen Angreifern – Terroristen, Kriminellen, Staaten – neue Angriffswege. Und es wird deutlich, dass sich alle Megatrends gegenseitig verstärken können.

Dieses Papier befasst sich jedoch nicht mit volkswirtschaftlichen Herausforderungen wie dem Wegbrechen von Absatzmärkten, Währungsinstabilitäten, Handelsembargos, steigenden Rohstoffpreisen oder Ähnlichem. Der Fokus richtet sich auf Bedrohungen, die unmittelbar die deutsche Wirtschaft – auch auf deutschem Boden – betreffen und damit eine Gefahr auch für solche Unternehmen sind, die kaum Auslandsgeschäft betreiben und vielleicht gar nicht auf (ausländische) Zulieferungen angewiesen sind.

Oben aufgeführte Megatrends bedeuten vereinfacht zusammengefasst, dass

1) es immer mehr Menschen gibt, die ihren Lebensunterhalt kaum aus legaler Arbeit decken können,
2) zu exzessiver Gewalt und schwerster Kriminalität bereite Menschen gewissermaßen herangezüchtet werden
3) mehr und mehr Räume entstehen, wo sich diese Menschen festsetzen können, ohne mit einer Strafverfolgung rechnen zu müssen
4) Staaten und Unternehmen sich einem härteren globalen Wettbewerb ausgesetzt sehen, der für sie Spionageaktivitäten rechtfertigt
5) Angriffe auf Unternehmen praktisch jederzeit und von jedem Ort auf der Welt ausgeführt werde können
6) die Fähigkeiten für immer komplexere Angriffe weltweit zunehmen und gleichzeitig
7) täglich neue Angriffsflächen geboten werden.

Hinzu kommt, dass das Bewusstsein für diese Bedrohung in Deutschland gefährlich unterbelichtet ist. Die genannten Megatrends werden kriminelle Aktivitäten und Spionage gegen deutsche Unternehmen weiter anwachsen lassen.

Cyber-Crime als Werkzeug

Cyber-Crime ist genau genommen kein eigener „Tatbestand" sondern vielmehr ein Werkzeug. Die Möglichkeiten über diesen Angriffsvektor steigen rasant. Zum einen verbreitet sich das Wissen über Computertechnologie und Programmierung über den gesamten Globus. Darüber hinaus lassen sich Angriffskomponenten auch ganz einfach im so genannten „Dark Web" oder „Deep Web" bestellen. Ob Spam-Angriff, Bot-Netz, Trojaner oder Viren – alles ist für relativ kleines Geld zu haben. Während sich die einen darauf spezialisieren, Lücken in Systemen zu finden, basteln andere geeignete Angriffswerkzeuge. Wieder andere verkaufen gestohlene Identitäten, Dritte waschen Gelder, die durch illegale Aktivitäten generiert wurden. Es ist eine hoch professionalisierte, arbeitsteilige Welt. Und diese Arbeitsteilung findet über den gesamten Globus verstreut statt.

Angriffe von überall möglich

Ein nur schlecht ausgebildeter Nigerianer kann von einem Internetcafé in Abuja aus an einem Tag mehr Geld verdienen als bei einer guten Yams-Ernte. Russische, gut ausgebildete Programmierer werden diesen Lohn noch um ein Vielfaches übertreffen, wenn sie als „Black Hat" in fremde Rechner eindringen und wertvolle Informationen stehlen und ebenfalls mehr, als wenn sie einer legalen Beschäftigung nachgehen – wenn sie denn überhaupt einen Job bekämen. In China sitzen tausende staatlich beschäftigte Hacker, die täglich Computer von Unternehmen infiltrieren, manipulieren und sabotieren. In jedem Land gibt es Hacker mit unterschiedlicher Fähigkeiten – vom so genannten „Skript Kiddy" bis zu wahren Profis – die auf eigene Rechnung, als Teil einer kriminellen Organisation, als Terroristen oder Aktivisten oder für Staaten ihre Fähigkeiten gegen das Wohl von Unternehmen einsetzen.

So vielfältig die Angreifer, so vielfältig sind auch ihre Ziele.

Nahezu jedes Delikt der Wirtschaftskriminalität findet inzwischen auch online statt

So breit die Phalanx an Angreifern ist, so breit ist auch deren Betätigungsfeld. Fließend sind hier die Grenzen von Wirtschaftskriminalität, Aktivismus, Terrorismus und kriegerischen Handlungen.

Ist die Verbreitung von „Botschaften" oder Propaganda mittels Cyber-Attacken eine kriminelle oder eine terroristische Aktion? Wie ist es, wenn Aktivisten die Webseite der GEMA lahm, um auf ihre Wertvorstellung aufmerksam zu machen? Wie ist es zu bewerten, wenn der IS seine Botschaften auf den gehackten Seiten von Le Monde verbreitet?

Oftmals ist simple Bereicherung das Ziel von Cyber-Attacken. Wie im Falle eines der größten Bankraube aller Zeiten: Weltweit wurden 34 Millionen Euro erbeutet, als 2013 in verschiedenen Städten von einem Konto mit gefälschten Kreditkarten 1,7 Millionen Euro abgehoben wurden. Möglich wurde dies durch einen raffinierten Hacker-Angriff durch den zuvor das Limit des Kontos erhöht worden war.

Auch Erpressung geht digital: 2014 wurden der VoIP-Anbieter Sipgate sowie die Münchner Direktbank Fidor Bank Ziel einer DDoS-Attacke. In Erpresserschreiben wurde gedroht, die Angriffe zu intensivieren, wenn kein „Lösegeld" gezahlt werde.

Die Perspektivlosigkeit vieler Menschen trifft auf leicht verfügbare Werkzeuge, die es ihnen ermöglichen, ohne allzu großes Fachwissen oder besondere Fähigkeiten weltweit kriminell aktiv zu werden. Dabei wächst durch die Tatsache, dass immer mehr Prozesse miteinander vernetzt werden und rund um die Uhr online sind auch die Zahl der Angriffsmöglichkeiten quasi ins Unendliche. Mit Industrie 4.0 wird diese Problematik gänzlich neue Ausmaße annehmen.

Schadenshöhe durch Wirtschaftskriminalität geht in die Milliarden

Delikte wie Diebstahl, Unterschlagung, Betrug und Untreue, die Verletzung von Geschäfts- und Betriebsgeheimnissen, Produkt- und Markenpiraterie, Erpressung, Geldwäsche, Korruption und Datenmissbrauch bleiben also weiterhin bestehen. Sie bekommen durch die Cyber-Komponente jedoch eine zusätzliche Dramatik, da der Täter nicht mehr vor Ort sein muss. Entsprechend hoch ist der Schaden, der durch „Computerkriminalität" entsteht. KPMG schätzt den Gesamtschaden allein in den beiden vergangenen Jahren auf 54 Milliarden Euro[1]. Wie hoch genau er ist, lässt sich schwer sagen, da von einer hohen Dunkelziffer auszugehen ist.

Auch der Gesamtschaden, der durch Wirtschaftskriminalität entsteht, ist schwer zu fassen. Das Bundeskriminalamt bestätigt für 2014 insgesamt mehr als Dreiundsechzigtausend Fälle, die der Wirtschaftskriminalität im engeren Sinn zugeordnet werden.[2] 2013 wurde ein Schadensanstieg auf fast vier Milliarden Euro konstatiert[3]. Die tatsächliche Zahl dürfte deutlich höher liegen. Eine besondere Herausforderung bei der Wirtschaftskriminalität besteht darin, dass es sich nicht um einzelne feststehende Straftaten oder um ein scharf abgrenzbares Deliktbündel handelt, sondern um ein komplexes kriminelles Umfeld, was unter anderem dazu führt, dass wirtschaftskriminelle Handlungen in der Polizeilichen Kriminalstatistik verschiedenen Straftatgruppen zugeordnet werden[4]. Zudem ist davon auszugehen, dass es ein großes Dunkelfeld nicht angezeigter oder nicht erkannter Straftaten gibt[5]. Der Grund hierfür ist zumeist der drohende Reputationsverlust, der häufig höher gewichtet wird als der rein monetäre Verlust[6]. KPMG schätzt den jährlichen Schaden auf 80 Milliarden Euro.

Wirtschaftsspionage nimmt zu

Die oben aufgeführten Aktivitäten sind meist auf Einzelschicksale zurückzuführen. Hohe Arbeitslosigkeit oder politische Radikalisierung machen aus Menschen Täter. Doch auch Staaten sehen sich einem wachsenden Konkurrenzkampf ausgesetzt, fürchten um ihre (machtpolitische) Stellung und Zukunft. Sie fühlen sich von innen durch Separatisten oder Oppositionelle bedroht und von außen durch Anrainerstaaten, die ihnen im wahrsten Sinne des Wortes das Wasser abgraben wollen, oder Ländern, die eine andere politische Ausrichtung verfolgen. Ihnen sind fast alle Mittel recht, um ihre Stellung zu verbessern. Wenn das militärisch nicht gelingt, muss dies wirtschaftlich erfolgen. Daraus ergeben sich dann schnell Allianzen mit heimischen Unternehmen, die dasselbe Ziel verfolgen: wirtschaftliche Stärke. Und wer aus eigener Kraft nichts Innovatives leisten kann, besorgt sich das Know-How auf anderem Wege. Der Markt der illegalen Informationsbeschaffung mit nachrichtendienstlichen Mitteln wächst entsprechend. Gerade bei Technologie- und Innovationsunternehmen steht Wirtschaftsspionage auf der Tagesordnung.

Wirtschaftskriminalität und Spionage haben nicht selten dieselbe Ursache: Mangelnde Perspektiven, durch legale Anstrengungen etwas zu erreichen.

1 KPMG Studie: e-Crime - Computerkriminalität in der deutschen Wirtschaft 2015

2 BKA, „Polizeiliche Kriminalstatistik (PKS) 2014"; in das Gesamtbild einzubeziehen sind zudem sicherlich signifikante Anteile der fast 1 Million weiteren Betrugsdelikte und der ca. 74 Tsd. Fälle von Computerkriminalität, die das BKA separat ausgewiesen hat.

3 BKA: „Wirtschaftskriminalität, Bundeslagebild 2013"

4 Vgl. BKA, „Polizeiliche Kriminalitätsstatistik (PKS) 2014", wo z. B. zwischen „Wirtschaftskriminalität", „Computerkriminalität" und „Betrug" unterschieden wird.

5 Jörg Ziercke, Bundeslagebild Wirtschaftskriminalität 2013

6 Bundesministerium des Innern, http://www.bmi.bund.de/DE/Themen/Sicherheit/Kriminalitaetsbekaempfung/Wirtschaftskriminalitaet/wirtschaftskriminalitaet_node.html (02.09.2012)

International ist Wirtschaftsspionage oftmals so verankert, dass in vielen Ländern dieser Welt die rechtliche Verpflichtung des Staates besteht, die einheimische Wirtschaft aktiv zu unterstützen. Wie deutsche Verfassungsschützer eindrücklich zu schildern wissen, kann das in der Praxis so aussehen, dass ein ausländisches Konkurrenzunternehmen eines deutschen Konzerns sein Produkt oder seine Dienstleistung optimieren möchte und sich hilfesuchend an seinen Staat wendet, der wiederum seinen Nachrichtendienst mit der Beschaffung der gewünschten Informationen betraut. Das heißt, der deutsche Konzern würde in diesem Fall von einem professionellen Nachrichtendienst angegriffen, um an die entsprechenden Unternehmensdaten zu kommen.

Anschaulich wird das an einem dreisten Fall von Wirtschaftsspionage, den die Firma ENERCON schon vor einigen Jahren in den USA über sich ergehen lassen musste. Die Firma hatte weltweit eine Alleinstellung auf dem Gebiet getriebeloser Windräder. Als sie jedoch auf dem Riesenmarkt USA hierfür ein Patent anmelden wollte, leitete völlig überraschend das amerikanische Konkurrenzunternehmen Kenetech ein Verfahren ein, weil es die eigenen Patente für getriebelose Antriebe verletzt sah. ENERCON erhielt unter anderem ein Importverbot in den USA. Erst durch späteren Einblick in Gerichtsakten erfuhr ENERCON, dass sich Mitarbeiter von Kenetech Zugang zu einer der ersten neuen Windanlagen in Deutschland verschafft haben sollen. So konnten sie alle Details fotografieren und waren in der Lage, die Technologie zu kopieren. Auch wenn die Angelegenheit mittlerweile bereinigt ist, bedeutete sie für ENERCON dennoch einen jahrelangen, schmerzhaften Marktausschluss[7].

Auch die Firma Solarworld aus Bonn soll 2012 Opfer eines geheimdienstlich motivierten Cyberangriffs geworden sein. Laut Informationen des US-Justizministeriums ist die amerikanische Tochter von Solarworld eines von fünf Unternehmen, das von Hackern der chinesischen Volksbefreiungsarmee ins Visier genommen worden sei. Der vermutete Hintergrund: Eine Anti-Dumpingklage Solarworlds gegen chinesische Konkurrenten. Daraufhin hätten sich die chinesischen Hacker in die Unternehmenskommunikation eingeklinkt, die Klageschrift mitgelesen sowie Informationen über die finanzielle Lage, Produktionsverfahren, Herstellungstechniken und Kostensituation des Unternehmens verschafft[8]. Die Chinesen bestreiten den Vorgang.

Schäden durch Wirtschaftsspionage dürften höher liegen als die durch Wirtschaftskriminalität

Bei der Spionage wird es noch schwieriger, den konkreten Schaden abzuschätzen. Alleine, da die allerwenigsten Fälle gemeldet werden – hier ist die Angst vor Reputationsverlust wohl noch größer ausgeprägt. Das Bundesinnenministerium schätzt den Schaden auf 50 Milliarden Euro pro Jahr[9], der Ingenieurverband spricht gar von 100 Milliarden Euro[10]. Die Datenerhebung der Spionagefälle ist sehr schwierig. Denn Unternehmen wissen oft nicht, dass sie Opfer eines Angriffs wurden oder zeigen einen Vorfall nicht an. Jedes vierte befragte deutsche Unternehmen berichtete über einen konkreten Spionagefall in den letzten Jahren. Fast genauso viele hatten zumindest einen entsprechenden Verdacht. Nur bei ca. jedem vierten Vorfall werden die Sicherheitsbehörden (Polizei oder Verfassungsschutz) hinzugezogen[11], die anderen bekannten Fälle wurden eher zufällig oder aufgrund von Ermittlungen der Sicherheitsbehörden entdeckt.

Auch wenn keine gesicherten Erkenntnisse über die genaue Höhe vorliegen: Der Schaden durch Wirtschaftsspionage ist enorm.

7 Handelsblatt Nr. 007. 10.01.2014
8 Spiegel-Online, 20.Mai 2014
9 Bundesinnenminister a.D. Hans-Peter Friedrich: Rede zur Veranstaltung „Wirtschaftsschutz gemeinsam gestalten“ (28.08.2013)
10 FAZ-Online, 03.02.2014
11 Studie: Industriespionage 2014, Cybergeddon der deutschen Wirtschaft durch NSA & Co.?, Corporate Trust Business Risk & Crisis Management GmbH

Faktor Mensch ist genauso wichtig wie die Technik

Trotz einer wachsenden technischen Bedrohung darf der Faktor Mensch nicht unterschätzt werden. Neben der technischen Komponente ist nämlich auch er ein wesentliches potenzielles Risiko. Seien es Kunden, Dienstleister, Berater oder eigene Mitarbeiter, indem sie bewusst kriminell handeln oder unbewusst mitwirken – sie alle können bei Angriffen eine wesentliche Rolle spielen. So belegen Studien, dass 55 Prozent der Täter eigene Mitarbeiter sind und in etwa jedem dritten Fall auch das Management oder Top-Management involviert war[12].

Social-Engineering, das Manipulieren von Menschen für eigene Zwecke durch die Ausnutzung von Eigenschaften wie Gutgläubigkeit, Hilfsbereitschaft, Respekt vor Autoritätspersonen, Stolz oder Konfliktvermeidung ist auf dem Vormarsch. Ein aktueller Fall aus den USA beschreibt fast lehrbuchhaft die Möglichkeiten des Social-Engineerings. Danach wurde ein Manager der amerikanischen Firma Scoular Co. mit Hilfe gefälschter E-Mails dazu veranlasst, über 17 Millionen Dollar auf ein chinesisches Bankkonto von Betrügern zu überweisen. Die E-Mails waren mit dem Namen des Scoular-Geschäftsführers unterzeichnet und ihr Inhalt für den Manager plausibel. Es wurde im vorgegaukelt, dass es um die dem Manager bekannte Übernahme einer chinesischen Firma ging, die jetzt im Rahmen eines streng vertraulichen Vorgangs in Zusammenarbeit mit der amerikanischen Börsenaufsicht SEC zum Abschluss gebracht werden solle. In den E-Mails wurde er drei Mal aufgefordert, immer größere Beträge an eine Bank in Shanghai zu überweisen, was er guten Glaubens auch tat. Um den zum Stillschweigen Verdonnerten zu ermutigen und um Vertrauen aufzubauen, hatte man ihn zuvor ebenfalls per E-Mail mit dem falschen Namen und der Telefonnummer eines vermeintlichen Mitarbeiters der Rechnungsprüfungsfirma von Scoular versorgt. In seinen Anrufen dort wurde ihm sein Vorgehen selbstverständlich bestätigt[13].

Viele technische Attacken erfolgen in Kombination mit Innentätern oder ihnen geht ein Social-Engineering voraus.

Am gefährlichsten ist und bleibt aber der unzufriedene Mitarbeiter, der über seine legalen Zugangsmöglichkeiten Insiderwissen über Schwachstellen besitzt und beispielsweise Daten von Kunden verkauft. Das Schadenspotenzial ist hier wesentlich höher als bei einem externen Täter. Allerdings ziehen längst nicht alle Unternehmen Konsequenzen aus dem Risiko fehlender Loyalität ihrer Angestellten. Nicht einmal die Hälfte befragter Unternehmen, die selbst einräumen, dass sie über schützenswertes Fachwissen verfügen, hat dafür aktuell ein Schutzkonzept, wie die WIK-Sicherheitsenquete 2014/15 zeigt. Auch die häufige Unkenntnis von Mitarbeitern, welches Wissen schützenswert ist, birgt ein hohes Risiko. IT-Sicherheitsvorkehrungen reichen als Schutz hier nicht aus.

Ein weiterer großer Risikobereich ist das Abgreifen von Informationen auf Geschäftsreisen im Ausland. Viele Unternehmen gehen zu sorglos mit ihren Informationen um. Laut einer Studie von Corporate-Trust rüstet nur circa jedes sechste Unternehmen seine Geschäftsreisenden mit entsprechend verschlüsselter Hard- oder Software aus, viele treffen sogar keinerlei Sicherheitsvorkehrungen. Eng damit verknüpft schätzen Unternehmen die Verwendung mobiler Geräte wie Smartphones und Tablets und die sinkende Sensibilität der Mitarbeiter im Umgang mit geschäftskritischen Daten als zunehmendes Risiko ein. Aber auch die Themen Outsourcing von Dienstleistungen und Cloud Services werden hier als bedrohte Felder gesehen – und das gerade auch vor dem Hintergrund, dass gefühlt die Zahl von staatlich gelenkten Hackeraktivitäten steigt und Sicherheitsmanager von Unternehmen Ausspähung aktuell als zweitgrößtes Gefährdungsrisiko ansehen – auch das ein Ergebnis der WIK-Sicherheitsenquete 2014/15.

12 KPMG Studie (2014): Wirtschaftskriminalität in Deutschland
13 Spiegel-Online, 12.02.2015

Konkrete Abwehrstrategien sind zu entwickeln

Die beste Möglichkeit, sich vor den genannten Gefahren zu schützen, wäre sicherlich deren vollständige Beseitigung. Jedoch ist die Wiederherstellung von Staatlichkeit keine Aufgabe für ein deutsches mittelständisches Unternehmen, noch könnte es den technischen Fortschritts zurückdrehen oder alleine den Klimawandel stoppen. Selbst die vereinte Wirtschaftskraft Deutschlands wäre hier machtlos. Der deutsche Staat hat sicherlich im Verbund mit anderen Nationen gewisse Möglichkeiten beim Nation Building oder im Umweltschutz. Doch hier sind – wenn überhaupt – erst langfristig Erfolge zu erwarten. Es führt daher kein Weg daran vorbei, konkrete Abwehrstrategien jetzt zu entwickeln und umzusetzen.

Die Möglichkeiten und Schwerpunkte bei der Ausgestaltung der Unternehmenssicherheit sind vielfältig. Aber welcher Schutz ist wirklich notwendig? Gewisse Anforderungen lassen sich zumindest aus der Branchenzugehörigkeit ableiten.

So wird sich ein Online-Handel vor allem auf die Sicherheit der eigenen Internetplattform und der Kundendaten fokussieren müssen, während es für einen Automobilproduzenten darauf ankommt, technische Innovationen, Modellpolitik und Marketingpläne vor fremdem Zugriff zu schützen. Ein Pharmaunternehmen wird Augenmerk auf den Schutz eigener Forschungsergebnisse und Patente legen. Ein Versorgungsunternehmen muss vor allem die eigene Infrastruktur vor Sabotage schützen. Die Liste ließe sich fortsetzen.

Überblick über die Sicherheitslage und Erfassung von Vorfällen

Von grundlegender Bedeutung für jedes Sicherheitsmanagement ist es, stets einen möglichst aktuellen Überblick über die Sicherheitslage und relevante Sicherheitsvorfälle im Unternehmen zu behalten. Nur so kann gezielt analysiert, gegengesteuert und präventiv gehandelt werden. Je größer und diversifizierter ein Unternehmen ist, desto zahlreicher sind tendenziell die Sicherheitsvorfälle. Gleichzeitig wird es gerade in komplexeren Unternehmensstrukturen kontinuierlich schwieriger, den Überblick zu behalten und die Risiken in ihrer Gesamtheit zu erkennen. Hier empfiehlt es sich, Kriterien für die Meldepflicht von Sicherheitsereignissen sowie die Meldewege in Richtung Sicherheitsmanagement verbindlich festzulegen. Finden idealerweise geeignete IT-Tools für das Security Incident Management bzw. das Case Management Einsatz, können Vorfälle nicht nur revisionssicher dokumentiert und analysiert, sondern auch die Maßnahmen zur Gegensteuerung situationsgerecht eingeleitet und verfolgt werden. Mit Blick auf Datenschutz, Rechtssicherheit, Compliance sowie effizientem und effektivem Umgang mit knappen internen Ressourcen eine nicht ganz unbedeutende Angelegenheit.

Das hier skizzierte Vorgehen soll im Folgenden näher erläutert werden: Nehmen wir an, ein Unternehmen verfügt über eine recht große Zahl von Mitarbeitern, Kunden oder geschäftlichen Transaktionen. Dann wird es sich früher oder später dafür interessieren, welche Schäden durch deliktische Handlungen entstehen, in welcher Form und wo es angegriffen wird bzw. wie hoch beispielsweise der Anteil von internen Tätern ist. Erfahrungen interner Ermittler in sehr großen Firmen zeigen, dass sich dort im Grunde jede Straftat wiederfindet, die auch im gesamtgesellschaftlichen Kontext relevant ist.

Nur wer genau weiß, was passiert, kann sich künftig wirksam schützen.

Für ein weltweit agierendes Unternehmen dürfte es ebenfalls von Interesse sein, wie es um die Sicherheitslage in den einzelnen Landesgesellschaften bestellt ist. Über systematische Vergleiche – unter Berücksichtigung der jeweiligen nationalen Datenschutzbestimmungen – können lokale und überregionale Sicherheitsrisiken frühzeitig erkannt werden.

Um Vergleichbarkeit zu gewährleisten, ist es wesentlich, dass deliktische Handlungen und sonstige Sicherheitsvorfälle nach einheitlichen Kriterien erfasst werden. Mit Blick auf die Rechtsordnung in Deutschland bietet es

sich beispielsweise an, Delikte auf oberster Ebene zumindest nach Eigentumsdelikten, Sachbeschädigungen und Vermögensdelikten zu unterscheiden, die sich in weitere „Unterdeliktarten“ aufteilen lassen. Je mehrstufiger das hinterlegte Datenmodell, desto feiner können Auswertungen durchgeführt und desto besser können Schwachstellen und Risiken lokalisiert werden.

Werden Delikte und sonstige Sicherheitsvorfälle nicht nur nach einheitlichen Kriterien erfasst, sondern auch mit Personen-, Orts- und Zeitangaben sowie Tatmitteln verbunden, ergeben sich mehrdimensionale Auswertemöglichkeiten. Modi operandi können abgebildet und Häufungen bestimmter Delikte in regionaler und zeitlicher Hinsicht erkannt werden. Werden Daten über einen längeren Zeitraum gepflegt, können neben der jeweiligen Ist-Situation auch Entwicklungen und aktuelle Trends abgebildet werden. Hilfreich ist, wenn die eingesetzten IT-Tools über entsprechende Reporting- und Analysefunktionen verfügen.

Identifizierung der „Kronjuwelen“

Vor der Einleitung von Schutzmaßnahmen ist es zunächst erforderlich, die Top-Geschäftsgeheimnisse im Unternehmen zu identifizieren. Zu ihrer initialen Bestimmung ist die Durchführung einer Risikobewertung zu empfehlen. Sie geht vom Grad der Auswirkung aus, die ein Vertraulichkeitsverlust hätte. Dabei werden die Top Geschäftsgeheimnisse als „streng vertraulich“, also als durch Angriffe mit nachrichtendienstlichen Methoden gefährdet, eingestuft. Dementsprechend sind die Schutzmaßnahmen auszurichten. Auch im Zusammenspiel mit Dienstleistern und Lieferanten sollte man in diesem Zusammenhang das nötige Informationsschutzniveau messen. So berücksichtigt man sicherheitskritische Aspekte beispielsweise auch bei Einkaufsentscheidungen.

Abgestufte Maßnahmen einleiten

Sind nach erfolgter Risikoanalyse alle möglichen Bedrohungen identifiziert, wird zu jeder festgestellten Bedrohung eine passende risikominimierende Schutzmaßnahme vereinbart und implementiert. Bei technischen und IT-Angriffsszenarien werden mögliche zielgerichtete Angriffe durch zum Beispiel Einmal-Trojaner/Einmal-Schadware berücksichtigt. Hier finden dann besonders gehärtete Notebooks, USB-Sticks mit „Diebstahlsicherung“ oder eine spezielle Festplattenverschlüsselung Verwendung. Das heißt, die Informationen sind so gesichert, dass Angreifer auch im Verlustfall des technischen Geräts nicht zugreifen können. Eine Ende-zu-Ende-Verschlüsselung von Telefonen und Faxgeräten gehört ebenfalls in diesen Maßnahmentopf, ebenso wie der Abhörschutz für relevante Räume. Letzteres ist vor allem für den Geschäftsführungsbereich von großer Bedeutung. Wesentlicher Bestandteil eines solchen Schutzkonzeptes ist zudem die Festlegung von Verantwortlichkeiten, damit Klarheit besteht, wer zum Beispiel für die Identifikation beziehungsweise den Schutz einzelner Werte zuständig ist.

Nicht-technische Bedrohungen beziehen sich in erster Linie auf den Faktor Mensch. Gedankenlosigkeit oder Leichtsinn bei Geschäftsreisen, aber auch mögliche gezielte Angriffe unter Ausnutzung menschlicher Schwächen sind ein Risiko. Wichtig ist, dass die Maßnahmen nicht in Form von Verboten umgesetzt werden, sondern vielmehr durch den Einsatz von maßgeschneiderten, unternehmens- und mitarbeiterbezogenen Lösungen bestimmt sind. Ganz allgemeine Gegenmaßnahmen, die hier Anwendung finden, sind das Labelling von Dokumenten durch Wasserzeichen, Geheimhaltungsvereinbarungen besonders mit externen Partnern, Zugangsbegrenzungen (sowohl physikalisch als auch logisch) und eine „Total Clean Desk Policy“. Maßgeschneidert gibt es spezielle Trainings für Mitarbeiter, die mit Geschäftsgeheimnissen umzugehen haben. So werden Sekretariate zum Beispiel zum Thema „Umgang mit externen Besuchern“ extra geschult.

Nicht alles muss mit demselben Aufwand geschützt werden. Die Top-Unternehmensgeheimnisse sind zu definieren und entsprechend zu sichern.

Social Engineers zielen gern direkt auf den einzelnen Mitarbeiter ab. Durch entsprechende Sensibilisierungsmaßnahmen, wie zum Beispiel interaktive Awareness-Kampagnen, können Mitarbeiter in die Lage versetzt werden, Angriffe dieser Art zu erkennen und abzuwehren. Eng verknüpft mit den Gefahren durch das Social Engineering sind die Bedrohungen, die sich aus der Nutzung von Social Media ergeben. Auch hier werden die Mitarbeiter sensibilisiert, die Netzwerke verantwortungsvoll und sicherheitsbewusst zu nutzen. Wirtschaftsschutz ist dann am wirksamsten, wenn er bewusst von jedem einzelnen Mitarbeiter selbst ausgeht.

Auch bei Geschäftsreisen sind Schutzmaßnahmen erforderlich. Vor Reiseantritt sollte klar sein, welche Sicherheitskritikalität das zu besuchende Land aufweist. Wer kein eigenes Rechercheteam besitzt, kann sich zumindest über das Auswärtige Amt oder Sicherheitsbehörden Informationen und Verhaltensempfehlungen beschaffen. Besondere Vorsicht gilt stets bei der Mitführung mobiler Datenträger, die vertrauliche Informationen beinhalten, seien es Laptops oder Smart Phones, aber auch bei der Entgegennahme von Geschenken wie USB-Sticks.

Basisschutz hilft bereits viel und kostet wenig

Durch die „Kapselung“ des jeweiligen „Kronjuwels“ des Unternehmens mit dem Bündel von maßgeschneiderten technischen und nicht technischen Schutzmaßnahmen sowie Sensibilisierungsschulungen wird dessen Sicherheitsniveau erheblich erhöht. Damit wird das Erlangen von hochkritischen Informationen durch Unbefugte, auch unter Beachtung eines vernünftigen Kosten-Nutzen-Verhältnisses, maßgeblich erschwert.

Die genannten Schutzmaßnahmen zeigen, dass ein Einzelunternehmen bereits einen sehr hohen Sicherheitsstandard erreichen kann.

Gemeinsam handeln

Große internationale Unternehmen sind genau wie mittelständische und kleinere Unternehmen von den Megatrends betroffen und stehen im Fokus von Angreifern. Hier lässt sich als Einzelkämpfer nicht genug ausrichten. Fehlende Informationen, Erfahrungswerte und Ressourcen, um mit Sicherheitsvorfällen in diesem Spektrum umzugehen, sind ein Grund dafür. Für einen nachhaltigen und umfassenden Wirtschaftsschutz muss allerdings mehr getan werden. Der Austausch von Best-Practice-Erfahrungen mit anderen Unternehmen und eine aktive wie innovative Zusammenarbeit mit Instituten und Behörden sind ein unerlässlicher Zusatzschutz. Erst durch die enge Kooperation mit anderen nationalen und internationalen Sicherheitsentscheidern wird ein umfassendes Sicherheitslagebild erkennbar, mit dem weitere Schwachstellen identifiziert und beseitigt werden können. Daher ist die Vernetzung in sämtliche Richtungen ein ausschlaggebendes Mittel, um einen Wirtschaftsschutz auf hohem Niveau zu generieren. Für die Zukunft und mit Blick auf die absehbaren neuen Herausforderungen für die Unternehmenssicherheit durch Industrie 4.0 und das Internet der Dinge wird das noch entscheidender sein, als es heute schon ist.

Sicherheit lässt sich effektiv nur gemeinsam mit den Mitarbeitern und Partner gewährleisten.

Der ASW Bundesverband fördert die Entwicklung eines gemeinsamen Sicherheitsverständnisses durch enge Zusammenarbeit zwischen Unternehmen, staatlichen Stellen und Verbänden auch über Landesgrenzen hinaus. So unterstützen wir die Institutionalisierung der Zusammenarbeit für einen nachhaltigen Wirtschaftsschutz, damit alle Beteiligten Zugang zu den entscheidenden Sicherheitsakteuren haben, sei es in der Politik, in den Behörden, der Wirtschaft oder der Wissenschaft. Denn nur ein offener Informationsaustausch und der Zugang zu fundiertem Sicherheitswissen ermöglichen es, eigene Sicherheitsmaßnahmen erfolgreich abzuleiten und umzusetzen.