Wirtschaftsspionage und organisierte Kriminalität – Gefährdetes Controlling

von Günther Holzhauser

Neue Technologien und unsere digitale Sozialisation in einer vernetzten Welt schreiten mit enormen Schritten voran. Wir leben in einer Zeit des Umbruchs. Machtblöcke gehen und neue entstehen. Die Regionen Asien-Pazifik und Süd- und Lateinamerika erfahren einen wirtschaftlichen Aufschwung. China und Russland nehmen geostrategisch immer mehr Einfluss auf das Weltgeschehen.

Deutschland ist aktuell eine der stärksten Nationen in der Europäischen Union und eines der innovationsstärksten Länder der Erde. **Deutschlands Politik, Militär, Wirtschaft und Wissenschaft stehen stark im Fokus der Spionage**. Unsere Wirtschaft wiederum steht im Kontext ihrer Weltgeltung stark im Fokus der Wirtschaftsspionage und der organisierten Kriminalität (OK) (siehe Abbildung 1).

Abb. 1: Die Hauptbedrohungen für die deutsche Wirtschaft

Die Entwicklung des transnationalen Verbrechens – eine Herausforderung für Staat und Wirtschaft

Ausländische Nachrichtendienste, global agierende Unternehmen und zunehmend die OK beschaffen sich das Know-how und die Informationen zur Entwicklung ihrer eigenen Märkte und kriminellen Geschäftsmodelle in Deutschland. Das internationale Verbrechen operiert zunehmend auf dem Territorium der Bundesrepublik Deutschland. Deutschland ist Aktionsraum für dieses Verbrechen geworden. Es wird immer schwieriger Grenzen zwischen Wirtschaftsspionage, Wirtschaftskriminalität, CyberCrime und dem organisierten Verbrechen zu ziehen.

Mittlerweile können sogar Verbindungen zwischen Organisierter Kriminalität (OK), dem Terrorismus sowie dem Extremismus hergestellt werden. Das Geschäftsmodell ›Crime as a Ser-

vice‹ wir zunehmend populärer. Das Verbrechen hat eine hohe Innovationsfähigkeit. Qualität und Quantität von Angriffen auf unseren Nationalstaat und unsere Wirtschaft stellen für die deutschen Sicherheitsbehörden eine große Herausforderung dar.

Die digitale Sozialisation und weitere Metatrends sind die Brandbeschleuniger für die Bedrohung durch Wirtschaftsspionage und organisierte Kriminalität

Was sind die aktuellen neuen Entwicklungen und die Themen der Zukunft? Social Media, mobile Endgeräte, vernetzte Mobilität, Internet der Dinge, Industrie 4.0 und die Metaebene Social Business. Die Vernetzung von Mensch und Unternehmen schreitet unaufhörlich und mit rasantem Tempo voran. Die „digitale Sorglosigkeit" des Menschen stellt eine große Bedrohung für Unternehmen und Organisationen dar.

Alle vorher erwähnten Trends überlagern sich, sie vernetzen sich und stehen in Abhängigkeit zueinander. Hier entstehen komplexe und heterogene Bedrohungen und Risiken, die wir heute noch nicht einschätzen können. **In diesem Komplex spielt der Mensch eine entscheidende Rolle**. Jedoch ist schon abzusehen, dass diese Trends und Entwicklungen dazu führen, zukünftig Menschen und vertrauliche Informationen schneller zu enttarnen, Menschen, Informationen und Prozesse schneller zu manipulieren und Netzwerke schneller zu sabotieren. Aus Sicht des Autors wird **die Sabotage und die Desinformation in Zukunft zu den Hauptbedrohungen** gehören. Fremde Nachrichtendienste – damit Nationalstaaten – können sicherlich heute schon Netzwerke (z. B. Industrie 4.0) und Kritische Infrastrukturen in verschiedenen Ländern per Mausklick manipulieren oder abschalten. Organisierte Kriminalität kann letztendlich auch bedeuten, einen industriellen Wettbewerber mit seinem Produktionsnetzwerk auszuschalten, zu erpressen oder die beschafften Betriebs- und Geschäftsgeheimnisse an wen auch immer zu verkaufen.

Im Kontext von Industrie 4.0 verschwinden die territorialen Grenzen. Die klassischen hierarchischen Organisationen von Unternehmen werden sukzessive durch autonome und virtuelle Organisationen ersetzt. Im Vordergrund dieser Bestrebungen steht die Erhöhung der Produktivität durch Vernetzung und die Sichtbarmachung von Menschen und Wissen. Wenn wir angegriffen werden, stellt sich die Frage, sind wir die Opfer und die Unschuldigen oder sind wir selber Teil des Problems? Der Autor ist der Meinung, dass **die komplexe und heterogene Bedrohungslage** mit ihren noch kaum abzusehenden Risiken **für die Metatrends Social Media, Industrie 4.0, Internet der Dinge, vernetzte Mobilität und Social Business als Bedrohung in Politik und Wirtschaft noch nicht angekommen ist**. Im Kontext der Sicherheit müssen zukünftig die Netzwerke mit allen Beteiligten betrachten werden, die Betrachtung einzelner Beteiligter oder Unternehmen greift zur kurz. Nur durch Bedrohungs- und Risikoanalyse eines Netzwerkes mit seinem Umfeld können notwendige Sicherheitsstrukturen abgeleitet werden. Die vielfältigen und aktuellen Vorfälle z. B. zeigen, dass das Verbrechen in diesen Bereichen bereits in der Fläche angekommen ist.

Experten gehen davon aus, dass in der Zukunft die Milliarden von mobilen Endgeräten noch unsicherer werden. Diese Anzahl von Geräten verteilt sich auf wenige unterschiedliche Betriebssysteme der Marktführer. Weltweit arbeiten jetzt schon viele Millionen professionelle Angreifer mit unterschiedlichsten Motiven an Angriffswerkzeugen für Geräte und Menschen.

Die Anzahl der Angreifer in der Zukunft wird dramatisch zunehmen, die digitale Sozialisation wird das Verbrechen leichter machen. Die deutschen Sicherheitsbehörden sprechen jetzt schon von einer massiven Zunahme der Angriffe in Qualität und Quantität. **Die Anzahl der potenziellen Angriffsziele auf Menschen und Netzwerke steigt exponentiell**. Das Analyseunternehmen Gartner geht davon aus, dass im Jahre 2020 ca. 220 Milliarden Geräte mit dem Internet verbunden sein werden. Entstehen hier nicht Milliarden von potenziellen Sicherheitsrisiken in Form der Geräte und sogar der Menschen, die sich mit ihren Geräten „sorglos" in den Netzwerken bewegen?

Die Netzwerke der Zukunft können wir uns wie ein Spinnennetz vorstellen. Ziehen Sie an einem Ende des Spinnennetzes (der erfolgreiche Angriff), dann hat dies Einfluss auf das ganze Gewebe und das Netz, es kommt in Bewegung. Unsere Netzwerke der Zukunft mit den vielen vernetzten und verbundenen Einzelakteuren bieten insgesamt eine enorme Angriffsfläche.

Die Bundesregierung und die Wirtschaft erhöhen das Tempo im Kontext der digitalen Sozialisation. Auf dem letzten Weltwirtschaftsforum in Davos hat die Bundesregierung der Industrie entsprechende Vorgaben ins Lastenheft geschrieben. Es soll sicher gestellt werden, dass Deutschland im globalen Geschehen den Anschluss nicht verliert.

Angreifer und ihre Methoden

Zu dem professionellen Spektrum der Angreifer werden fremde Nachrichtendienste, Wirtschaftsunternehmen, die Industrie- und Wettbewerbsspionage betreiben, sowie die organisierte Kriminalität gezählt. Wobei in anderen Ländern oftmals Wirtschaftsunternehmen mit den eigenen Nachrichtendiensten zusammenarbeiten. Im professionellen Spektrum sind die Angriffsmethoden nahezu gleich.

Ein Großteil der deutschen Wirtschaft denkt in erster Linie in ihrem Verständnis von Sicherheit an IT und physikalischen Schutz. Das gesamtheitliche Verständnis für Schutz und das breite Spektrum der Bedrohungen und Angriffe sowie die Quellen für ungewollten Informationsabfluss

Autor

Dipl.-Ing. Günter Holzhauser

Selbständiger Berater im Bereich Wirtschaftsschutz, Spionageabwehr und Unternehmenssicherheit für Wirtschaft und Organisationen. Ausbildungen in Ingenieurwissenschaften, Unternehmenssicherheit und Spionageabwehr.

E-Mail: holzhauser@wirtschaftsschutz.eu

fehlen meist. Studien belegen, dass der Großteil der Schadensfälle für ungewollten Know-how-Verlust nicht über die IT kommen. Das Problem ist die Verortung der Information, die Migration der Information und die Zugänge zur Information.

In bis zu 80 Prozent der Fälle ist laut Fachstudien der Mensch die Schwachstelle. Im Kontext der professionellen Angreifer ist die IT eine Facette; sie ist aber nicht die wichtigste Facette. Aus der Erfahrung der operativen Feldarbeit des Verfassers mit mittelständischen Unternehmen lässt sich durchaus die Aussage tätigen, dass gerade der massiv bedrohte Mittelstand diese Tatsache noch nicht wahrgenommen hat. Die aktuellen Vorfälle und die Professionalität der Angreifer lassen die gewagte Frage in den Raum stellen, »ob es eine IT-Sicherheit in der heutigen Zeit überhaupt noch gibt«. Weltweit können Militärs, Regierungen, Großunternehmen und sensible Infrastrukturen gehackt werden. Die Angreifer – das Verbrechen und fremde Geheimdienste – scheinen uns immer um einiges voraus zu sein.

Die Angriffsmethoden und damit die Bedrohungen sind äußerst vielfältig. Schwachstellen und fehlende Schutzmaßnahmen sind in der Regel im Bereich Innen-/Außentäter, Social Engineering, Social Media, IT/Hacking, Kommunikation, Geschäftsreisen, Besucher/Delegationen, Wirtschaftspartner, Messen und externe Dienstleister zu finden. Übergeordnet ist die größte Schwachstelle meist der Schutz der kritischen Information eines Unternehmens. Hier fehlen neben der gesamtheitlichen Betrachtung die unternehmensspezifischen Schutz- und Präventionskonzepte für das Know-how.

Welche Unternehmen und welche Bereiche sind gefährdet?

Nahezu jedes Unternehmen kann Opfer von Wirtschaftsspionage oder organisierter Kriminalität werden. In der deutschen Wirtschaft ist zu großen Teilen der Irrglaube verhaftet, dass nur große Unternehmen und technologieorientierte Unternehmen, die Patente und Forschung und Entwicklung betreiben, betroffen seien. Diese Einschätzung ist nicht zutreffend. **Nahezu jedes Unternehmen kann heute Opfer von Wirtschaftsspionage, Industrie- und Wettbewerbsspionage oder organisierter Kriminalität werden.** Entscheidend sind die Branchen und die Kernkompetenzen eines Unternehmens. In Deutschland sind fast alle Branchen betroffen. Militär, Maschinenbau, Umwelttechnik, Medizintechnik, Pharma, Automotive, Luft- und Raumfahrt, Finanzen und Versicherungen, Handel sind nur einige Beispiele (siehe Abbildung 2).

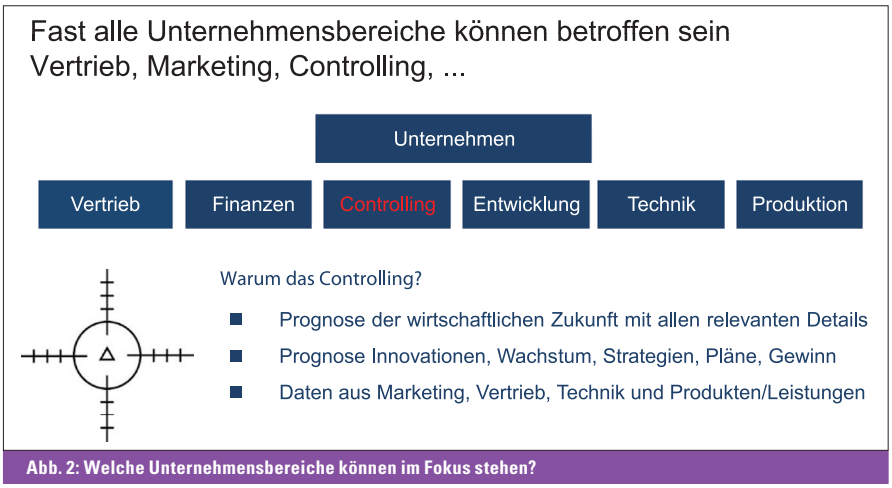

Abb. 2: Welche Unternehmensbereiche können im Fokus stehen?

Aber auch erfolgreiche Geschäftsmodelle können einen Impuls für Angriffe auslösen. Die Unternehmensgröße – ob Großunternehmen, mittelständisches Unternehmen oder Kleinstunternehmen – spielt für die Angreifer keine Rolle. Entscheidend ist das, was aus den Unternehmen „beschafft" werden kann."

Gefährdete Bereiche in den Unternehmen sind die Abteilungen

- Beschaffung/Einkauf,
- Vertrieb und Marketing,
- Controlling,
- Strategieabteilung,
- Forschung & Entwicklung,
- Produktion und Technik
- Personal.

Welche Informationen sind für professionelle Angreifer interessant? Welche Informationen lassen sich im Kontext von Wirtschaftsspionage und organisierter Kriminalität verwenden? Im Fokus der Angreifer stehen zum Beispiel folgende Betriebs- und Geschäftsgeheimnisse aus den Unternehmen:

- Unternehmensstrategien, Marktstrategien und Marktdaten, Wachstumspläne, Finanzdaten
- Vertriebsstrategien, Vertriebsstrukturen, Vertriebsorganisationen, Vertriebspartner
- Merger & Akquisition
- Forschung und Entwicklung, Produktentwicklungen, Innovationen
- Patente und Schutzrechte
- Einkaufsdaten, Projektkalkulationen, Kunden- und Lieferantenbeziehungen/-daten
- Ausschreibungen und deren Kalkulationsgrundlage

Gefährdetes Controlling

Das Controlling ist ein Schlüsselbereich in jedem Unternehmen. Das Controlling konsolidiert alle relevanten und sensiblen Daten des Unternehmens und erstellt ein in die Zukunft gerichtetes Lagebild für das Unternehmen. **Gerade dieses Zukunftsbild mit den Aussagen über Strategien, Wachstum, Veränderung von Märkten, Globalisierung, Umsatz- und Gewinnerwartung, ist für die verschiedenen Angreifer von Interesse.**

Im Kontext der Wirtschaftsspionage und der Industrie- und Wettbewerbsspionage benötigen andere Nationalstaaten und deren Wirtschaftsunternehmen diese Informationen, um eigene Industrien aufzubauen und sich mittelfristig Wettbewerbsvorteile zu verschaffen. Die organisierte Kriminalität hat Interesse an diesen Informationen, um sie **den Wettbewerbern des ausgespähten Unternehmens oder auf dem Schwarzmarkt** (Darknet/Peer-to-Peer Netzwerke) **zum Verkauf anbieten zu können, sie können** aber auch als Kompromat (eine für die Erpressung geeignete Information) eingesetzt werden, um das Unternehmen zu erpressen.

Wenn solche Informationen ungewollt aus dem Controlling abfließen, können vielfältige und massive Schäden für das Unternehmen entstehen. Verlust von Märkten und Wettbewerbsfähigkeit, Verlust von USP und Nachhaltigkeit, Reputations- und Imageschäden, Regress- und Schadensersatzforderungen.

Der erfolgreiche Angriff auf das Controlling ist ein ernstzunehmender Vorfall in einem Unternehmen. Der Autor ist aktuell Mitglied eines Ermittlerteams in einem größeren mittelständischen Unternehmen, bei dem das Controlling betroffen ist. Ein Mitarbeiter diese Abteilung hat über längere Zeit Betriebs- und Geschäftsgeheimnisse (das geplante Lagebild des Unternehmens der Zukunft) an einen Wettbewerber weitergegeben. Der Mitarbeiter galt als integer und vertrauenswürdig, war fleißig und gewissenhaft. Erst mit der Kündigung und dem Wechsel zu dem Wettbewerber hat der Leiter des Controllings angefangen, über verschiedene Vorgänge nachzudenken. Im Nachgang hat er viele Auffälligkeiten festgestellt. Im Rahmen der internen Ermittlungen konnte man von anfänglichen Verdachtsmomenten nun Beweise für die Weitergabe und mit Ausscheiden aus dem Unternehmen die Mitnahme/Diebstahl von Betriebs- und Geschäftsgeheimnissen nachweisen. Das Ermittlungsverfahren läuft. Über das Motiv lässt sich im Nachgang nur spekulieren. Der Leiter des Controllings geht davon aus, dass dieser Mitarbeiter zum Innentäter geworden ist, weil er vor einigen Jahren im Rahmen eines Change-Prozesses im Unternehmen keine Führungsposition übernehmen durfte. Die Persönlichkeitsstruktur des Mitarbeiters, die Enttäuschung und Rachegefühle werden wohl eine Rolle gespielt haben.

Das Entscheidende an diesem Beispiel ist, dass solche Vorfälle nur aufgeklärt werden können, wenn in einem Unternehmen die Prozesse der Sicherheit funktionieren. In diesem Unternehmen waren alle relevanten Abteilungen, die gefährdet sein können, in die Unternehmenssicherheit eingebunden. Leider ist dieses Unternehmen eine Ausnahme. Die meisten Unternehmen, die der Autor kennt, haben die Abteilung Controlling nicht in die Sicherheit des Unternehmens eingebunden. Somit wird es bei Vorfällen schwer, Regelverstöße insgesamt festzustellen, zu verfolgen und zu ahnden. Bei diesen Unternehmen können letztendlich keine Beweise für eine strafrechtliche Verfolgung erbracht werden.

Welchen konkreten Gefährdungen unterliegt das Controlling?

Aus Sicht des Autors ist eins der größten Probleme überhaupt, dass viele Unternehmen und auch das Controlling keine Transparenz über die eigene Gefährdung haben. Wer keine Transparenz über eine Gefährdungslage hat, kann keine entsprechenden Sicherheitsmaßnahmen etablieren. Viele Unternehmen – gerade die kleinen und mittelständischen Unternehmen – haben alles, was Sicherheit betrifft, auf die IT-Sicherheit reduziert. Die Unternehmen glauben, IT-Sicherheit, Datensicherheit und Datenschutzbeauftragter seien eine ausreichende Sicherheitsarchitektur für ein Unternehmen. Die Reduzierung der Sicherheit auf diese Facetten greift zu kurz, sie stellt eindeutig keine Sicherheit für ein Unternehmen dar.

Wir lesen täglich von erfolgreichen Cyberangriffen und von Internetkriminalität. Was wir in diesem Kontext in der öffentlichen Berichterstattung wahrnehmen, sind oft nur die Symptome, dass eine Homepage gehackt oder übernommen wurde oder aus Organisationen und der Wirtschaft massenhaft Daten oder Informationen gestohlen wurden. Aus Sicht des Autors greift diese Bewertung zu kurz, da in fast allen Fällen, in denen nennenswerte oder massive Schäden entstehen, Angriffe auf diese Organisationen (den Menschen) lange vorher stattgefunden haben. Die IT ist ein Aktionsraum für Angriffe, die IT ist aber nicht DER Aktionsraum.

Bei der Aufklärung, der Ausspähung und der Vorbereitung von Angriffen durch das professionelle Verbrechen, spielt der Mensch eine entscheidende Rolle. Menschen werden angegriffen, weil sie organisations- oder firmenspezifisches Know-how haben, Zugang zu Wissensträgern (dort ist Know-how manifestiert) und die Zugänge zur internen IT-Systemarchitektur haben. Dies sind Gründe, warum Menschen zu den bevorzugten Angriffszielen von fremden Nachrichtendiensten und dem professionellen Verbrechen werden. Im Kontext des Verbrechens steht der **Mensch im Mittelpunkt**. Als Täter oder Innentäter stellen sich Menschen aus unterschiedlichsten Motiven und Bedürfnissen selbst in den Mittelpunkt, bei der Manipulation durch Angreifer werden Menschen ungewollt oder unbewusst zum Mittelpunkt gemacht. Beide Fälle stellen eine enorme Bedrohung für Organisationen und Unternehmen dar. Diese Bedrohungen gelten auch für das Controlling. Angriffe erfolgen von außen auf das Unternehmen und das Controlling, Innentäter stellen eine interne Gefährdung für das Controlling dar. Ein afrikanisches Sprichwort besagt treffend, suche den Feind im Schatten deiner Hütte.

Wie lässt sich das Controlling schützen?

Wie bereits vorher ausgeführt, lässt sich ein Unternehmen und das Controlling nur effektiv schützen, wenn die Gefährdungen und Risiken bekannt sind. Das Controlling sollte selber – wie auch alle anderen Abteilungen – einer Gefährdungsanalyse unterzogen werden. Hier wird das Controlling als Abteilung mit seinen Mitarbeitern, seiner Geschäftstätigkeit und der Verankerung in den Unternehmensprozessen betrachtet. Bei Unternehmen mit mehreren Lokationen und internationalem Geschäft, ist die Einbindung des Controllings in diese Strukturen zu prüfen. Zentral geführtes Controlling hat möglicherweise Schnittstellen zu anderen Standorten im In- und Ausland. Effektive Sicherheitsmaßnahmen für das Controlling können nur etabliert werden, wenn all diese internen und externen Facetten begutachtet wurden. Innerhalb des Controllings müssen für Sicherheitsmaßnahmen Transparenz und Akzeptanz hergestellt werden. Jeder Mitarbeiter ist Bestandteil der Sicherheit und muss seinen Beitrag leisten. Wenn sich Mitarbeiter nicht an die Sicherheitsbestimmungen halten, kann keine Sicherheit gewährleistet werden. Der Autor kann aus seiner operativen Arbeit mit vielen Unternehmen berichten, dass sich die wenigsten Unternehmen über die Sicherheit des Controllings Gedanken machen, aus verschiedensten Gründen wird diese Thematik massiv unterschätzt. **Die Bedrohungs- und Risikoanalyse des Controllings und die Ableitung von Maßnahmen sind wichtige und erste Schritte**. Es bleibt viel zu tun! ■