DER BETRIEBSWIRT

Organisation ist wichtiger als Technik

Spektakuläre Datenschutzverstöße in Großunternehmen, Notfall-Evakuierungen aus Libyen, längerfristige Unterbrechungen von Versorgungsketten nach Naturkatastrophen. Auf den ersten Blick haben diese Vorfälle wenig gemeinsam. Aber alle betreffen ein immer bedeutender werdendes Thema: die Unternehmenssicherheit. In der Realität besteht häufig noch eine Organisationsstruktur, die solchen komplexen Risiken nicht gerecht wird.

Von Timo Kob und Christian de Lamboy

Traditionell wird in vielen Unternehmen noch immer nach IT-Sicherheit, physischer und personeller Sicherheit unterschieden. Die ganze Absurdität dieses weithin vorherrschenden Silo-Denkens wird sichtbar, wenn man die aktuelle Umsetzung des Themas Sicherheit in Unternehmen auf die Arbeitsweise der Polizei abbildet. Schon der gesunde Menschenverstand würde eine Schaffung von Dezernaten „Banküberfälle und Tötungsdelikte mit Messern“ sowie „Banküberfälle und Tötungsdelikte mit Pistolen“ als offensichtlich unsinnig identifizieren. In vielen Unternehmen wird aber tatsächlich nach Angriffsmitteln getrennt statt nach Angriffszielen und -konsequenzen.

Aber nicht nur überholtes Denken in Silos erschwert die effektive und effiziente Umsetzung des Themas Sicherheit in Unternehmen. Die in fast allen Unternehmen fehlende Ableitung der Sicherheitsmaßnahmen aus der Unternehmensstrategie und -situation trägt ebenfalls dazu bei. Schutzbedarfe werden nach Bauchgefühl ermittelt (genauer gesagt: vermutet). Auf dieser Grundlage wird dann „irgendwas, irgendwie“ geschützt – aber eben nicht konkret aus betriebswirtschaftlicher Sicht abgeleitet und priorisiert.

In welchem Verhältnis zum Beispiel soll in den Schutz der Produktionsanlagen vor Feuer oder in den Schutz geistigen Eigentums vor Diebstahl investiert werden? Ist die Ergreifung eines Datendiebs für das Unternehmen wichtiger als die schnellstmögliche Herstellung des Normalbetriebs kritischer Prozesse? Untersuchungen zeigen, dass sich innerhalb von 30 Jahren das Verhältnis von materiellen zu immateriellen Gütern am Unternehmenswert von 80 zu 20 in das Gegenteil umgekehrt hat. Dieser dramatische Wandel hat aber bei der „klassischen“ Unternehmenssicherheit noch nicht zu entsprechenden Konsequenzen geführt. Das althergebrachte Bild der Unternehmenssicherheit führt dazu, dass auch in Zeiten von Compliance und Corporate Governance das Thema „Sicherheit“ noch häufiger mit bewaffnetem Schutzpersonal und sogenannten Ermittlungen als mit Unternehmensstrategien und Wertschöpfungsketten verbunden wird.

Gern wird zwar darauf hingewiesen, welche überragende Bedeutung der IT im Unternehmen zukommt. Tatsächlich wird dabei aber häufig vergessen, zu erwähnen, dass IT in den seltensten Fällen den Selbstzweck des Unternehmens darstellt. Diese Aussage ist offensichtlich banal. Gerade auch im Mittelstand – aber beileibe nicht nur dort – beschreibt sie dennoch erstaunlich oft die Regel, die Kernkompetenz für den IT-Sicherheitsverantwortlichen in der Technologie und nicht an der Schnittstelle von IT zum Geschäft festzulegen. Angesichts dieser teilweise über Jahrzehnte hinweg gewachsenen Strukturen und Verantwortlichkeiten ist hier ein Paradigmenwechsel notwendig, der nicht zuletzt sämtliche mit Sicherheitsfragen befassten Mitarbeiter vor neue fachliche und persönliche Anforderungen stellt. Experten werden natürlich auch weiterhin benötigt.

In Zukunft bedarf es aber zusätzlich auch expliziter und übergreifender Management-Kompetenzen, um den Herausforderungen der Zeit angemessen zu begegnen. Mit Blick auf die Entwicklung der Unternehmenssicherheit im internationalen Umfeld ist davon auszugehen, dass es kaum eine andere Funktion im Unternehmen geben wird, die mehr Schnittstellen zu den anderen Bereichen hat als sie. Vom Management zur Definition der Vorgaben über die Fachbereiche zum Schutz der individuellen Wertbeiträge bis hin zu fast allen Querschnittsfunktionen von der Revision bis zum Personal oder Projektleitern müssen alle Funktionen in die Betrachtung einbezogen werden.

Verlangt wird neben der fachlichen Expertise ein vertieftes Grundverständnis von Betriebswirtschaft und Recht. Ohne dieses sind gerade in multinational agierenden Unternehmen die jeweiligen gesetzlichen Anforderungen unter sicherheitstechnischen Aspekten erst gar nicht zu verstehen, zu konsolidieren oder umzusetzen. Dies heißt nicht, dass der prototypische Leiter Unternehmenssicherheit demnächst ein Jurist oder Volkswirt sein wird. Die zentral erforderlichen Aufgaben, die Verbindung zum Management, die Ableitung der ganzheitlichen Risikolandkarte aus der konkreten Unternehmenssituation und -strategie verlangen aber generalistischere Kompetenzen. So werden Schwierigkeiten heute meist technisch und nicht organisatorisch gelöst, was maximal die Sicherheit von heute, aber nicht die von morgen gewährleistet.

Die Sicherheit von morgen wird nur zu gewährleisten sein, wenn Sicherheit als eigene Management-Disziplin verstanden wird. Wie alle anderen solchen Disziplinen bedarf sie eigener Strukturen, Prozesse, Schnittstellen zu anderen Unternehmensbereichen – vor allem aber einer angemessenen Aufmerksamkeit durch die Geschäftsführung. Vergleicht man aber die personelle, technische und finanzielle Ausstattung der Unternehmenssicherheit deutscher Mittelständler mit derjenigen vergleichbarer Länder (Großbritannien, Frankreich oder Japan), muss man feststellen, dass die deutschen Unternehmen hier erstaunlich blauäugig agieren und gegenüber der Konkurrenz im Hintertreffen liegen. Durch Ad-hoc-Investitionen in Technik wird Scheinsicherheit erzeugt, während sich unbemerkt bereits die nächsten Lücken öffnen. Proaktivität zur Verhinderung von Problemen sowie Notfallvorsorge für den ja nicht zu 100 Prozent verhinderbaren Vorfall sind noch immer eher die Ausnahme.

Potenziert wird diese Herausforderung neben der meist diskutierten informationstechnischen Angreifbarkeit auch durch die raumgreifende Internationalisierung gerade auch der mittelständischen Industrie. Reisetätigkeiten, Entsendungen oder Niederlassungen auch in Ländern mit hohen Sicherheitsrisiken werden zunehmend die Regel. Planerische Schwachstellen, die in der westlichen Welt lediglich geringe Eintrittswahrscheinlichkeiten von Sicherheitsrisiken berücksichtigen, werden so zu ernsthaften Bedrohungen für die Unversehrtheit von Mitarbeitern und den Erfolg von Projekten oder ganzen Unternehmen.

Angesichts der Tatsachen, dass einerseits die zunehmende Bedeutung der Sicherheit in vielen Unternehmen erkannt wird und andererseits dieser Erkenntnis ein leergefegter Arbeitsmarkt gegenübersteht, muss das Thema meist mit intern verfügbaren Kräften bewältigt werden. So gewinnt das Thema Weiterbildung von Mitarbeitern an Bedeutung. Dies wird auch im akademischen Umfeld erkannt, wo sich verschiedene neue Ausbildungsangebote entwickeln. Ein Beispiel ist ein im September startender berufsbegleitender Studiengang „Certified Security Manager“ an der Frankfurt School of Finance & Management. Eingebettet ist er in ein Programm mit Schwesterstudiengängen wie etwa dem „Certified Fraud Manager“ oder „Certified Compliance Professional“. In die gleiche Richtung, aber als klassische Masterstudiengänge und mit jeweils etwas differierenden Zielbildern gibt es auch Angebote etwa an der Fachhochschule Brandenburg, der Hochschule für Wirtschaft und Recht Berlin oder der Fachhochschule Campus Wien.

Ein erfolgreiches und zukunftsfähiges Unternehmenssicherheitsmanagementsystem kann sich nicht mehr nur einzelnen Teilaspekten wie der Informations- oder der Liegenschaften-Sicherheit widmen, sondern muss die gesamte Breite der Risikolandkarte als relevantes Themenfeld annehmen. Nur mit diesem breiten Ansatz kann die Fokussierung auf die kritischen Werte im Unternehmen sinnvoll erfolgen und ein durchgängiges und angemessenes Sicherheitsniveau erreicht werden. Ist die Herangehensweise vom Kopf (den Angriffsarten) auf die Füße (die unternehmensspezifischen Auswirkungen) gestellt, so wird nicht nur die Unternehmenssicherheit als eine wesentliche Voraussetzung für den Unternehmenserfolg verbessert, sondern durch die breite Betrachtung gewinnt das Unternehmen auch einen anderen, oft erst im Nachgang bemerkten Mehrwert, nämlich eine signifikant gesteigerte Transparenz und hierdurch Kosteneinsparungen innerhalb des Unternehmens – auch losgelöst von Sicherheitsaspekten. Sicherheit kann in diesem Fall „vom Bremser zum Erfolgsfaktor“ für ein Unternehmen werden.

Christian de Lamboy ist Leiter des Competence Centers Governance & Audit an der Frankfurt School of Finance & Management. **Timo Kob** ist Vorstand der Sicherheits-Managementberatung HiSolutions AG in Berlin.