Dipl.-Ing. Günter Holzhauser

Keine Unternehmenssicherheit ohne gesamtheitlichen Informationsschutz

In unserer zunehmend digitalisierten Informationsgesellschaft arbeiten Unternehmen und Organisationen in hohem Maße mit wissensbasiertem Kapital. Die Metra-Trends Social Media, Industrie 4.0, Internet der Dinge und Social Enterprise führen zu einem überproportional hohen Vernetzungsgrad der Gesellschaft und der Wirtschaft. Die Sichtbarmachung von Menschen und Informationen ist teilweise Zielstellung dieser Trends. Günter Holzhauser hat als ausgewiesener IT-Sicherheitsspezialist schon eine ganze Reihe von Beiträgen zu diesem Thema im cpm forum veröffentlicht und berät Unternehmen auf diesem Gebiet.

Das wissensbasierte und meist schützenswerte Kapital respektive Know-how von Organisationen und Unternehmen ist heute schon sehr heterogen disloziert. Die Gefahr, dass diese schützenswerten Informationen ungewollt aus einer Organisation abfließen, ist in der heutigen Zeit enorm gestiegen. Globalisierung und Digitalisierung machen Angriffe auf das Know-how von Organisationen und Unternehmen oftmals sehr einfach. Angriffe sind in der Regel meist erfolgreich, da Unternehmen und Organisationen keinen gesamtheitlichen Informationsschutz betreiben. Wer stellt in diesem Kontext eine Gefährdung für Unternehmen und Organisationen dar?

Das Gefährdungspotential

Diverse Fachstudien haben herausgefunden, dass die eigenen und die ehemaligen Mitarbeiter der mit Abstand gefährlichste Personenkreis für Unternehmen und Organisationen sind. Die Mitnahme und Weitergabe (gewollt oder ungewollt) von Betriebs- und Geschäftsgeheimnissen ist Bedrohung Nr. 1. Dann folgen Wirtschaftspartner, Lieferanten, Wirtschaftsspionage, organisierte Kriminalität und Einzeltäter/Hacker.

Viele Unternehmen reduzieren den Informationsschutz auf die IT und die Datensicherheit. Aus der operativen Felderfahrung kann der Verfasser berichten, dass es kaum mittelständische Unternehmen gibt, die ein Verständnis für einen gesamtheitlichen Informationsschutz im Unternehmen haben. Gesamtheitlich bedeutet in diesem Kontext, dass der Informationsschutz über das gesamte Unternehmen mit allen Lokationen gezogen werden muss. Funktionierender Informationsschutz bezieht sich immer auf die Bereiche Mensch, Infrastruktur, IT und Prozesse.

Rechtliche Grundlagen

Rechtlich gesehen existiert kein Regularium für das Thema Informationsschutz respektive Know-how-Schutz. Vielmehr ist der Informationsschutz in einer Vielzahl von gesetzlichen Regelungen festgeschrieben. Ich möchte ausdrücklich erwähnen, dass Informationsschutz in diesen Regelungen für Unternehmen und Organisationen gesetzlich festgeschrieben ist. Klare gesetzliche Vorgaben gibt es z.B. in den Bereichen des Bürgerlichen Gesetzbuches (BGB), der Strafprozessordnung (StOP), dem Telekommunikationsgesetzes (TKG), dem Telemediengesetz (TMG), dem Bundesdatenschutzgesetz (BDSG) sowie dem Betriebsverfassungsgesetz (BetrVG). Hinzu kommen die Verkehrssicherungspflichten (Organisationspflicht und Aufsichtspflicht) sowie die Fürsorgepflicht. Beispiel: ein Unternehmen ist gesetzlich dazu verpflichtet, die Geheimhaltung von Geschäftsgeheimnissen eines Auftraggebers sicherzustellen. Zur Rücksicht auf Rechtsgüter des Vertragspartners erwächst eine Nebenpflicht auch ohne ausdrückliche Vereinbarung. Bei einem ungewollten Informationsfluss – Unterlassung von Sicherungsmaßnahmen – haftet das Unternehmen mit seinen handelnden Akteuren in der Breite des Wirtschaftsstrafrechtes. Solche Vorkommnisse haben in der Regel haftungs-, zivil- und strafrechtliche Auswirkungen.

SYSTEMATISIERUNG DES BEGRIFFSINHALTES „WISSEN"

Alle Abb.: Autor

Von Daten und Fakten zum Wissen im Kontext der Abschöpfung
Wissensträger

Wissen (Know how) manifestiert sich immer in Wissensträgern

- Dokumentiertes Wissen: z.B. Daten, Datei, Email, Patent, FEM/CAD-Modell, Brief, Bericht, Merkblatt usw.
- Persönliches Wissen: Wissen einer Person, das ständig weiter entwicklet wird. Z.B. Kompetenz, Erfahrung, Fähigkeit, Intuition, Vermutung, Einschätzung, usw.
- Kollaboratives Wissen: Wissen in Zusammenarbeit mehrerer Personen. Z.B. Teamwissen, Arbeitsgruppen, Forschungsprojekte, usw.
- Produktgebundenes Wissen: in Produkten hinterlegt und gebunden. Z.B. Materialien, Oberflächen, Geometrien, Design/Gestalt, Verfahrenstechnik, Fertigungsverfahren, Prozessdaten, usw.

Das Know how oder das Wissen eines Unternehmens ist eine Ansammlung sehr heterogener Wissensinhalte, die in der Regel über verschiedene Lokationen und verschiedene Länder in unterschiedlichen Nationalitäten disloziert sind.

Was verstehen wir unter Wissens- und Informationsschutz?

Wissen und Information entsteht erst durch die Verknüpfung und Verdichtung von z.B. Daten und Fakten. Einzelne Daten, die in einem System hinterlegt sind, stellen noch kein Wissen oder Information dar. Wissen kann als eine Ansammlung sehr heterogener Wissensinhalte charakterisiert werden. In der Umgangssprache wird Wissen auch als Know-how bezeichnet. Wissen manifestiert sich immer in verschiedenen Wissensträgern. Sie transportieren die Wissensinhalte. Die Wissensübermittlung von einem Wissensgeber an einen Wissensempfänger wird als Wissenstransfer bezeichnet. Wissenstransfersituationen sind betrieblicher, persönlicher, organisatorischer oder produktbezogener Natur und beinhalten einen Mechanismus (Prozess) des Wissenstransfers.

Wissen und Information finden sich also grundsätzlich in allen Betriebs- und Geschäftsgeheimnissen einer Organisation oder eines Unternehmens. Hinterlegt sind sie meist in Geschäftsführung, Einkauf, Finanzen, Vertrieb, Marketing, Controlling, Produktion und Fertigung, Entwicklung und Konstruktion. Wissen und Information bewegen sich im Rahmen von Menschen, technischer Infrastruktur und der IT.

Informationsschutz für eine Organisation oder ein Unternehmen bedeutet in erster Linie erst einmal, die schützenswerten Informationen oder das Know-how zu identifizieren, um es in einer späteren Phase überhaupt schützen zu können. Ein oft vergessener und ganz wichtiger Aspekt im Bereich des Informationsschutzes ist das Erkennen von kritischen Wissenstransfersituationen. Mitarbeiter wissen meist nicht, wo sie unbewusst Wissen freiwillig preisgeben, oder wo sie ungewollt die Ausspähung von Wissen für potentielle Angreifer einfach machen. Aus diesem Grunde sollten in einem Unternehmen oder einer Organisation die für die Sicherheit verantwortlichen Mitarbeiter die kritischen Wissenstransfersituationen in ihrer Organisation kennen. Aus Sicht des Verfassers können diese Situationen nur durch Gespräche oder Interviews mit den Fachabteilungen offen gelegt werden. Zum Beispiel kann nur in Gesprächen herausgefunden werden, wie sich ein Geschäftsführer, ein Vertriebsleiter oder ein Ingenieur auf Reise, Messe oder in Kundenbesprechungen verhält und in welchen Situationen er wie und wo, Informationen verwendet. Ohne Transparenz über kritische Situationen kann kein funktionierender Informationsschutz aufgebaut werden.

Wie etabliere ich effektiven Informationsschutz?

Die Schlüssel für einen sicheren und funktionierenden Informationsschutz sind die Transparenz über die Information, Kenntnis über Transfersituationen und die Schulung und Sensibilisierung der relevanten Mitarbeiter. Gesetzliche, rechtliche und organisatorische Rahmenbedingungen tragen – wenn vorhanden – zu einem funktionierenden Informationsschutz in einem Unternehmen oder einer Organisation bei. In erster Linie sind hier Compliance und Governance, Mitarbeiterverträge mit Geheimhaltungs-/Datenschutz-Klauseln, Berechtigungs- und Zugriffskonzepte, Risiko- und Schwachstellenanalyse sowie Schulungsprogramme zu nennen. Aus Erfahrung des Verfassers sind die Befähigung und der Reifegrad der Sicherheitsverantwortlichen in einem Unternehmen oder einer Organisation von essenzieller Bedeutung. In der Regel haben Unternehmen mit nennenswerten Sicherheitslücken Sicherheitsverantwortliche mit geringer Befähigung und geringem Reifegrad.

Sicherheit fängt ganz oben an

Sicherheit und Informationsschutz in einer Organisation oder einem Unternehmen beginnen immer im Top-down. Leitung und Führungskräfte und hier insbesondere Vorstände von Aktiengesellschaften und Geschäftsführer von GmbHs sind aufgrund gesetzlicher Vorgaben verpflichtet, Sicherheitsvorkehrungen zu treffen, um die Organisation vor existenzgefährdenden Einflüssen zu schützen. An dieser Stelle sei nochmals angemerkt, dass Vorstände und Geschäftsführer per Gesetz verpflichtet sind, ein Risikomanagementsystem in ihrer Organisation zu betreiben. Absoluten Schutz wird es im Kontext des ungewollten Informationsabschlusses nicht geben. Es kann nur darum gehen, durch entsprechende Maßnahmen das Risiko herunterzusetzen. Auch hier gilt die 20:80%-Regel. Mit 20% Einsatz kann 80% Ergebnis erzielt werden. Die „Regelgröße“ ist der Mensch. Mitarbeiter, die ein geschultes Sicherheits- und Risikobewusstsein haben, tragen in erheblichem Maße zu einem funktionierenden Informationsschutzprozess bei. ■

GRUNDLEGENDE METHODIK ZUR ERFASSUNG DES INFORMATIONSSCHUTZES