Schutz und Zukunfts-sicherung zugleich

Informationsicherheit befasst sich mit der Behandlung aller Geschäftsrisiken, die sich unternehmensweit aus dem Umgang mit Information ergeben und ist damit weit mehr als IT-Sicherheit. Eine über ein Managementsystem geführte Informationssicherheit hilft Bedrohungen und Schwachstellen systematisch zu erkennen und die damit verbundenen Risiken abzuschätzen, zu bewerten und adäquat zu behandeln. So können Strukturen und Prozesse verbessert, die betriebliche Kontinuität sichergestellt, geschäftsschädigende Einflüsse minimiert und unternehmerische Chancen maximiert werden.

Datenarchivierung, Datenschutz, Datensicherheit, Datensicherung, Informationssicherheit, IT-Sicherheit – alles ein und dasselbe? Fast täglich werden wir mit diesen Begriffen konfrontiert, in der Fachpresse wie auch in Gesprächen mit Verkäufern von Produkten und Dienstleistungen vielerlei Art. Häufig findet der Begriff Verwendung, der gerade besonders in Mode ist. Davon verspricht man sich ein besonders gutes Verkaufsergebnis. Zu einem genauen Verständnis von Informationssicherheit führt das nicht. Und ein Nutzen für den Kunden entsteht so sicher nicht.

Informationsicherheit – eine Definition

Der international anerkannte Standard ISO/IEC 27001:2005 (Informationssicherheits-Managementsysteme – Anforderungen) definiert Informationssicherheit als die Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit von Information. Dabei bedeuten:

- Vertraulichkeit: Die Eigenschaft, dass Information nicht-autorisierten Individuen, Instanzen oder Prozessen weder verfügbar gemacht noch offenbart wird.
- Integrität: Die Eigenschaft, die Richtigkeit und Vollständigkeit von wertvoller Information zu sichern.
- Verfügbarkeit: Die Eigenschaft, dass Information für autorisierte Instanzen bei Bedarf zugänglich und verwendbar ist.

ZUM AUTOR

Karsten M. Decker
Decker Consulting GmbH
Birkenstrasse 49
CH-6343 Rotkreuz

Telefon +41 (0)41 790 90 80
www.mit-solutions.com
decker@mit-solutions.com

Was ist Information?

Grundsätzlich ist Information ein Unternehmenswert, der genauso wie andere wichtige Unternehmenswerte für die Geschäftstätigkeit wesentlich ist und infolgedessen angemessen geschützt werden muss. Information kann in den unterschiedlichsten Formen vorkommen, zum Beispiel auf Papier gedruckt oder geschrieben; elektronisch gespeichert; per Post oder E-Mail versandt oder mit elektronischen Mitteln übertragen; auf Fotos, in Videos oder Filmen gezeigt; in Besprechungen, am Telefon oder in der Öffentlichkeit gesprochen; mittels eines Fotokopierers oder Faxgeräts verarbeitet oder übermittelt.

Der Inhalt kann zum Beispiel Angaben zu Personal und Kunden betreffen; technische Spezifikationen und Entwürfe; Details von technischen Infrastrukturen, Produktionseinrichtungen und -prozessen; Beschreibungen von Erfindungen, innovativen Prozessen und Verfahren sowie geistigem Eigentum im allgemeinen; Marktanalysen und Marktstrategie; Unternehmensziele und -strategien.

Warum ist Informationssicherheit wichtig?

Informationssicherheit hilft Gesetze, Verordnungen und Regulatorien einzuhalten. In der Schweiz betrifft dies zum Beispiel die gestiegenen Anforderungen des revidierten Obligationenrechts und Datenschutzgesetzes, die Geschäftsbücherverordnung und die Eigenkapitalvorschriften Basel II. Laut dem breit angelegten 10th Annual Global Information Security Survey von Ernst & Young im Jahre 2007 ist die Einhaltung von Gesetzen, Verordnungen und Regulatorien für 64 Prozent der befragten Manager Grund, sich mit Informationssicherheit zu beschäftigen.

Unternehmensintern hilft Informationssicherheit, freiwillige Richtlinien und Weisungen einzuhalten. So können Bedrohungen und Schwachstellen erkannt und abgewehrt, beseitigt oder gemildert werden. Das betrifft zum Beispiel die unerlaubte Einsichtnahme, Manipulation, Weitergabe oder den Verlust von Information durch Mitarbeiter, Lieferanten und Kunden. In der Regel geschieht dies aus Neugierde, Irrtum, Unkenntnis, Gutgläubigkeit oder Nachlässigkeit. Es betrifft aber auch den Diebstahl durch Mitarbeiter oder Drittpersonen zum Zwecke der Bereicherung oder Sabotage. Im günstigsten Fall gehen so Wettbewerbsvorteile verloren. Im Extremfall ändert sich die Natur der Geschäftstätigkeit, in dem ein Unternehmen sich von einem eigenständigen, innovativen Produzenten zu einem einfachen Lohnfertiger mit hohem Margenschwund und Verlust an Unabhängigkeit wandelt.

Schutz vor Verlust geschäftskritischer Information hilft aber nicht nur den Innovationsvorsprung und damit Wettbewerbsvorteile zu sichern. Auch wachsende vertragliche Anforderungen von Auftraggebern wie Liefertreue und -qualität, Geheimhaltung von Information sowie sonstige formale Anforderungen an die Geschäftsprozesse können so erfüllt werden. So können Ausschlüsse von Ausschreibungen vermieden werden.

Ausgangspunkt Risikobeurteilung

Nicht jede Information muss gleichermassen geschützt werden. Der Ausgangspunkt einer geführten Informationssicherheit nach ISO/IEC 27001:2005 ist somit eine systematische Risikobeurteilung aller Unternehmenswerte, die in Form von Information vorliegen. Das Vorgehen ist bekannt vom Management anderer unternehmerischer Risiken.

Zunächst werden dazu sämtliche Unternehmenswerte identifiziert und deren Bedeutung beschrieben. Falls ein solches Inventar bereits besteht, gilt es dieses auf Vollständigkeit zu über-

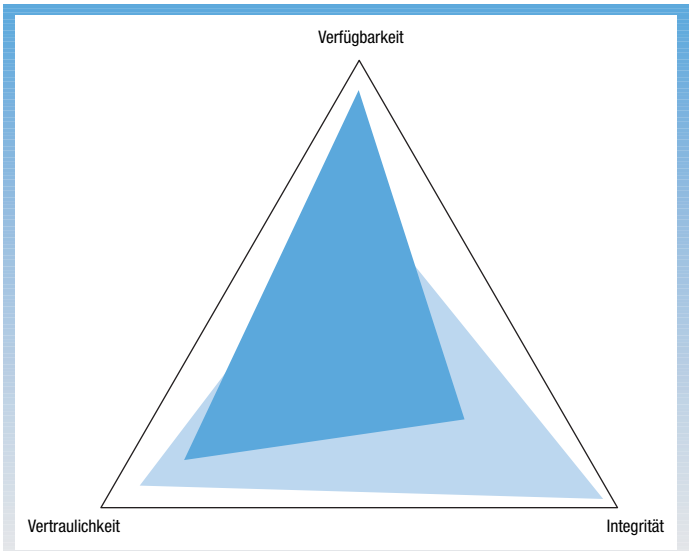

Bild 1: Risikogerechte Balancierung von Vertraulichkeit, Integrität und Verfügbarkeit für zwei verschiedene, fiktive Unternehmen.

PD Dr. Karsten M. Decker studierte Physik, Informatik und Chemie und ist Geschäftsführer der Decker Consulting GmbH. Er ist ISO/IEC 27001: 2005 zertifizierter Lead Auditor, akkreditierter Trainer für Informationssicherheit, Experte für IT Service Management und internationales Projektmanagement. Karsten Decker besitzt mehr als 20 Jahre Erfahrung in Management und Beratung und unterrichtet an der Hochschule Luzern, Technik & Architektur.
Decker Consulting GmbH hilft Unternehmen, Informationssicherheit und IT strategisch und operativ optimal in ihre Geschäftstätigkeit zu integrieren.

prüfen und bei Bedarf zu ergänzen. Die Risikobeurteilung erfolgt dann in zwei Schritten, einer Risikoanalyse und einer anschliessenden Risikobewertung. Bei der Risikoanalyse werden für jeden Unternehmenswert Risikoquellen wie Bedrohungen und Schwachstellen systematisch identifiziert, um dann die Eintrittswahrscheinlichkeit und den Effekt (das Schadensausmass) abzuschätzen, falls Vertraulichheit, Integrität oder Verfügbarkeit verloren gehen. Bei der anschliessenden Risikobewertung werden die so ermittelten Risiken mit unternehmensspezifischen Richtwerten verglichen, um die Bedeutung der Risiken für das Unternehmen zu bestimmen.

Nach Massgabe der Risikobeurteilung erfolgt dann die Risikobehandlung. Durch die Auswahl und Implementierung entsprechender Massnahmen kann die Eintrittswahrscheinlichkeit und/oder das Schadensausmass reduziert oder begrenzt werden. Die Bedeutung eines Risikos für ein Unternehmen bestimmt und rechtfertigt die Ausgaben für die Massnahmen zur Behandlung dieses Risikos. Alternativ kann ein Risiko wissentlich akzeptiert werden, wenn es die Sicherheitspolitik und die Kriterien eines Unternehmens für die Akzeptanz von Risiken objektiv erfüllt. Ein Risiko kann aber auch an Dritte transferiert werden, zum Beispiel an eine Versicherung oder einen Lieferanten. Schliesslich müssen die Restrisiken auf der Basis eines bewussten Entscheidungsprozesses durch entsprechend autorisierte Funktionsträger genehmigt, abgezeichnet, dokumentiert und kommuniziert werden.

Das Ergebnis der Risikobeurteilung hilft angemessene Managementaktivitäten und -prioritäten zu bestimmen, um vor den ermittelten Risiken zu schützen. Der Risikoansatz regelt auch, wie die 39 Hauptsicherheitskategorien von ISO/IEC 27001:2005 mit ihren 39 Massnahmenzielen und insgesamt 133 Massnahmen angegangen werden müssen. Ausführliche Handlungsempfehlungen für die Implementierung dieser Massnahmen sind in ISO/IEC 27002:2005 (Leitfaden für Informationssicherheitsmanagement) zusammengestellt. Die Massnahmen umfassen Politiken, organisatorische Strukturen, Prozesse, Verfahren und Handlungsweisen sowie Richtlinien und Praxisgepflogenheiten, die administrativer, technischer, betriebswirtschaftlicher oder gesetzlicher Natur sein können. Massnahmen jeglicher Art kommen also erst an zweiter Stelle. Nur so erreicht man eine unternehmensspezifische und risikogerechte Balance von Vertraulichkeit, Integrität und Verfügbarkeit für jeden einzelnen Unternehmenswert (Bild 1). Das Ziel von Informationssicherheit kann man also auch so formulieren:

Unternehmenswerte, die in Form von Information jeglicher Art vorliegen, in allen Geschäftsprozessen und den organisatorischen Strukturen eines Unternehmens risikogerecht schützen.

Kontinuierliche Verbesserung im Zentrum

Informationssicherheit in einem Unternehmen kann man nicht durch ein einmaliges Projekt auf Dauer sicherstellen. Einmal gegründet, implementiert und aktiv betrieben, gilt es das Informationssicherheitsmanagementsystem (ISMS) ständig zu überwachen und periodisch zu überprüfen, unterhalten und verbessern. Gemäss Standard kommt hierzu der kontinuierliche Verbesserungsprozess nach dem Plan-Do-Check-Act-Modell (PDCA-Modell) zum Einsatz. Dieser Prozess ist vielen Unternehmen etwa vom Qualitätsmanagement nach ISO 9001:2000 bereits bekannt. Der PDCA-Prozess steht im Zentrum des ISMS. Er hilft Schwachstellen zu identifizieren und zu beheben. Er hilft aber auch, die Informationssicherheit an die ändernden Anforderungen eines Unternehmens und des Umfeldes anzupassen. Wesentlich ist es, die Unternehmenswerte periodisch zu aktualisieren, danach die Risikobeurteilung zu überprüfen und allenfalls anzupassen. Schliesslich müssen sämtliche Massnahmen auf Angemessenheit, Vollständigkeit und vor allem auf Wirksamkeit überprüft und bei Bedarf korrigiert werden.

Erfolgskriterien

Die praktische Erfahrung zeigt, dass die folgenden Kriterien ausschlaggebend für die erfolgreiche Einführung eines ISMS sind:

- Politik, Zielvorgaben und Massnahmen der Informationsicherheit spiegeln die Unternehmensziele wieder.
- Ansatz und Rahmen für die Implementierung, den Unterhalt, die Überwachung und die Verbesserung der Informationssicherheit sind konsistent mit der Unternehmenskultur.
- Erkennbare Unterstützung und Verbindlichkeit auf allen Führungsstufen, inklusive operativer und strategischer Geschäftsführung.
- Ein gutes Verständnis der praktischen Anforderungen an die Informationssicherheit, die Risikobeurteilung und das Risikomanagement.
- Die Behandlung von Informationsrisiken ist in das unternehmensweite Risikomanagement integriert.

- Effektive Vermarktung von Informationssicherheit an alle Führungskräfte, Mitarbeiter und andere Beteiligte, um Bewusstsein zu bilden.
- Verteilung von Leitlinien zu Informationssicherheitspolitik und -standards an alle Führungskräfte, Mitarbeiter und andere Beteiligte.
- Bereitstellung von Geldmitteln zur Finanzierung von Führungsaufgaben im Bereich Informationssicherheit.
- Angebot angemessener Massnahmen für die Mitarbeitersensibilisierung, -ausbildung und -schulung.
- Einrichtung eines effektiven Führungsprozesses zur Behandlung von Informationssicherheitsvorfällen.
- Einführung eines Messsystems, um die Leistung des Managements der Informationssicherheit zu bewerten und Verbesserungsvorschläge auszuwerten.

Typische Fehler

Übernimmt die Geschäftsführung nur die rechtlich zugewiesene Gesamtverantwortung, ist das Unterfangen von vornherein zum Scheitern verurteilt. Ohne die Bereitstellung angemessener Ressourcen für die Führung des PDCA-Prozesses geht es nicht. Aber auch für Mitarbeitersensibilisierung, -ausbildung und -schulung müssen ausreichende Mittel bereitgestellt werden. Schliesslich muss die Geschäftsführung Zeit reservieren, um das ISMS mindestens einmal im Jahr auf Tauglichkeit, Angemessenheit und Effektivität zu überprüfen.

Wird Informationssicherheit durch die Geschäftsführung nicht konsequent vorgelebt, etwa indem Regelungen der Informationssicherheitspolitik verletzt werden (zum Beispiel Verletzung der Gerätepolitik für Laptops, Mobiltelefone, PDAs und Smartphones), ist eine geführte Informationssicherheit nicht mehr durchsetzbar.

Ein anderer typischer Fehler ist es, Informationssicherheit als die mechanistische Abarbeitung einer Checkliste zu begreifen. Dabei bleiben zum Beispiel Prozesse und organisatorische Strukturen unberücksichtigt. Und ganz wesentlich: der Risikozusammenhang fehlt. Ob Massnahmen erforderlich sind, wie sie zu implementieren sind und welche finanziellen und anderen Ressourcen dafür angemessen sind und gerechtfertigt werden können, kann so nicht beurteilt werden.

Ebenso wenig zielführend ist die spontane, improvisierte Implementierung einzelner technischer «Tools», häufig im Nachgang zu einem Sicherheitsvorfall. Besorgt und alarmiert auf mehreren oder gar allen Führungsstufen, wird blinder Aktionismus angeordnet. Das beruhigt zwar das Gewissen, führt aber in der Regel weder zu Massnahmen, die auf den Gesamtzusammenhang abgestimmt, noch kosteneffizient sind.

Häufig kann auch bei der Einführung eines ISMS Perfektionismus beobachtet werden. Die Ziele sind zu hoch gesteckt, man möchte gleich alles in einem einzigen Schritt «richtig» machen. In diesem Fall wird der Ansatz der kontinuierlichen Verbesserung nicht verstanden. Gründung und Implementierung werden langsam, die Mitarbeiter des Unternehmens überstrapaziert. Mit grosser Sicherheit geht so die Unterstützung durch Mitarbeiter und Führungskräfte verloren.

	Oktober 2008	September 2008	Mai 2008
Total	4848	4848	4500
Top fünf weltweit			
Japan	2789	2770	2554
Indien	427	426	421
UK	368	368	365
Taiwan	187	183	181
China	160	161	104
Top fünf in Europa			
UK	368	368	365
Deutschland	108	108	101
Ungarn	74	74	61
Tschechien	66	66	
Italien	54	54	

Anzahl und Verteilung der Zertifikate weltweit gemäss www.iso27001certificates.com. Seit September ohne BS 7799-2 Zertifikate.

ISO/IEC 27001:2005-Zertifikate weltweit

Die heute gültige Version des Standards wurde im Oktober 2005 verabschiedet und löste damit den de facto Vorgängerstandard BS 7799-2 der British Standards Institution ab. Im Durchschnitt wächst die Anzahl der Zertifikate weltweit um etwa 1000 pro Jahr. Die Tabelle zeigt die Anzahl und Verteilung nach Ländern gemäss dem freiwilligen Register www.iso27001certificates.com. Für die Schweiz werden insgesamt vier Zertifizierungen, acht weniger als im Mai 2008, genannt. Der Wegfall der BS 7799-2 Zertifikate mag die geringen Zuwachsraten in Indien, UK, Taiwan

und Deutschland und die Reduktion in der Schweiz erklären.

Da die Registrierung freiwillig erfolgt, ist die tatsächliche Anzahl Zertifikate sicher grösser. Aus dem gleichen Grund sollte man aus den Zahlenangaben für diejenigen grossen Industrienationen, für die nur wenige Zertifikate genannt werden, keine voreiligen Schlüsse ziehen. Bestimmt kann man jedoch sagen, dass das Thema Informationssicherheit in Japan besonders ernst genommen wird. Auch die Steigerung der registrierten Zertifikate in China um 54 Prozent und in Ungarn um 21 Prozent seit Mai 2008 ist bemerkenswert.

Dass Zertifizierung nicht immer eine pro-aktive, freiwillige Angelegenheit ist, zeigt die Situation in der Automobilindustrie. So schätzt man zum Beispiel in Fachkreisen übereinstimmend, dass BMW ca. 500 Zulieferer aufgefordert hat, sich nach ISO/IEC 27001:2005 zertifizieren zu lassen. Bei VW könnten sogar 1000 Zulieferer betroffen sein. Damit kommen die Zulieferer der deutschen Automobilbranche unter erheblichen Zugzwang.

Fazit

Informationssicherheit betrachtet Information jeglicher Art und in jeglicher Form, die geschäftskritisch ist. Sie regelt auch die Sicherheit von Systemen und Geräten zur Informationsverarbeitung und definiert damit auch den übergeordneten Rahmen für die IT-Sicherheit. Die IT-Sicherheit wiederum regelt im technischen Detail die Sicherheit von Information in elektronischer Form sowie die regelmässige Sicherung von Daten zum Schutz vor Verlust. Damit können Datensicherheit und Datensicherung als Teil der Informationssicherheit aufgefasst werden.

Informationssicherheit stellt im Umgang mit Information auch die Einhaltung von Gesetzen, Verordnungen und Regulatorien sicher. Sie setzt also die Leitplanken für den gesetzlich verlangten Datenschutz und die geforderten Massnahmen zur Datenarchivierung und macht so einen wichtiger Beitrag zur Umsetzung von Compliance. Das Risikomanagement von Unternehmenswerten, die in Form von Information vorliegen, ist ein wichtiger Teil des unternehmensweiten Risikomanagements, insbesondere für Hersteller und Anbieter von innovativen Produkten und Dienstleistungen. Damit wird Informationssicherheit auch zu einem wichtigen Element einer ordnungsgemässen Unternehmensführung (Bild 2).

ISO/IEC 27001:2005 ist ein auditierbarer Standard. Unternehmen können sich von jeder der für die Prüfung dieses Standards akkreditierten Zertifizierungsstellen zertifizieren lassen.

Aber auch wenn eine Zertifizierung nicht das Ziel ist, profitiert ein Unternehmen. Schwachstellen im Umgang mit Information in der organisatorischen Struktur und den Geschäftsprozessen werden identifiziert und gemildert oder beseitigt, das Risikomanagement wird kritisch überprüft. Nicht zuletzt können dadurch auch unternehmerische Chancen bessere genutzt werden.

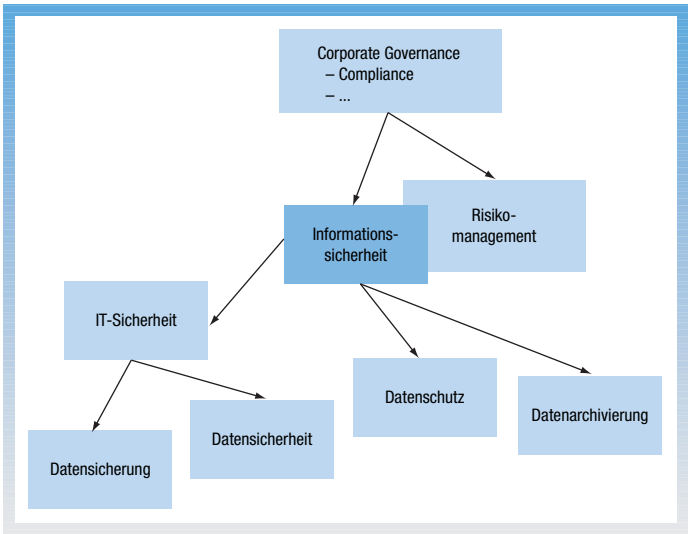

Bild 2: Positionierung der Informationsicherheit in einem Unternehmen.