Information-Security-Management-Systeme

Mit strukturiertem Handeln zu mehr Sicherheit

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

Inhaltsverzeichnis

Mit strukturiertem Handeln zu mehr Sicherheit

Information-Security-Management-Systeme (ISMS) entlasten Unternehmensleiter von Haftungspflichten für Betriebsrisiken

Sicherheit und Risiken – ein unauflöslicher Zusammenhang im menschlichen Leben. Mit Sicherheit geht jeder Mensch jeden Tag Risiken ein, genauso sicher unterscheidet sich die Risikowahrnehmung jedes Einzelnen. Und eine Vielzahl an Risiken wird den meisten erst dann bewusst, wenn sie eingetreten sind oder sie einen glaubwürdigen Erfahrungsbericht von Betroffenen gehört haben.

Der Betrieb von IT-Systemen ist „per se" immer mit Risiken verbunden, allem voran droht der Ausfall der Systeme. Läuft hingegen alles stabil, vermittelt die Technik trügerische Sicherheit – denn dann ist die Vorstellung besonders weit weg, dass dieser Zustand keineswegs selbstverständlich oder gar garantiert ist. Natürlich lässt sich nicht planen, wann, wo und in welchem Umfang Risiken eintreten. Und ihre Folgen kann man deshalb auch nicht vorhersagen. Alles in Ordnung also, mögen unerschütterbare Optimisten denken. Im privaten Bereich mag das auch so seine Richtigkeit haben, je nach Charakter und individueller Risikowahrnehmung. Aber schon dort finden sich zahlreiche Versicherungsverträge, wo es darum geht, Abhängige abzusichern – etwa wenn der Familienvater eine Lebens- oder Unfallversicherung abschließt. Das Risiko an sich wird damit nicht aufgehoben, aber seine Auswirkungen werden handhabbar gemacht.

Im Unternehmensumfeld kommt es nicht einmal auf das Bewusstsein einer Verantwortung an, wenn es um den Umgang mit Risiken geht. Hier gibt es eine Reihe rechtlicher Vorschriften, die von Unternehmern, Geschäftsführern oder Vorständen einfordert, Vorsorgemaßnahmen zu ergreifen und Risikobewältigungsstrategien zu entwickeln. Diese Verpflichtung ergibt sich unter anderem aus dem GmbH-, dem Aktien-, dem Kontroll- und Transparenzgesetz. Kurz gesagt, fordern diese, die Sorgfalt eines ordentlichen Geschäftsmanns anzuwenden und deshalb geeignete Maßnahmen zu ergreifen und zu überwachen, die den Fortbestand des Unternehmens sichern und gefährdende Entwicklungen früh erkennen. Das gilt insbesondere dann, wenn das Unternehmen für seinen Betrieb technische Einrichtungen einsetzt. Ergreifen sie solche Maßnahmen nicht, haften die Verantwortlichen gegenüber Gesellschaftern, Aktionären bis hin zu möglichen Gläubigern mit ihrem gesamten Vermögen für Schäden, die vermeidbar gewesen wären.

Diesem Risiko entkommt jedoch, wer den Nachweis erbringen kann, dass er geeignete Maßnahmen zur Abwehr oder Bewältigung solcher Risiken ergriffen hat. Was den Betrieb von IT-Systemen anbetrifft, gelten Information-Security-Management-Systeme als angemessene Instrumente. Je nach Branche und Unternehmensumfeld können sie unterschiedlichen Standards folgen, wie etwa der ISO 27001, dem BSI-Grundschutz oder den MaRisk-Kontrollstandards der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Sie dokumentieren eine strukturierte Herangehensweise, was den Umgang mit Unternehmensrisiken anbelangt. Dazu gehört unter anderem die Entwicklung einer Risikobewältigungsstrategie auf Basis einer gründlichen Analyse, der Aufbau einer dafür geeigneten Organisation sowie der benötigten Ressourcen und des Personals. In dieser Strategie sind Maßnahmen verbindlich festgelegt, deren Durchführung überwacht und dokumentiert wird. Auf Grundlage eines umfassenden Reportings, erfolgt außerdem eine regelmäßige Erfolgskontrolle, bei der Anpassungen nach dem Plan-Do-Check-Act-Schema festgelegt werden.

Management Summary
Die Verantwortung für den sicheren Betrieb von IT-Systemen liegt in Unternehmen jeglicher Größe und Rechtsform bei der Unternehmensführung. Zahlreiche Gesetze regeln außerdem, dass die Verantwortlichen für entstehende Schäden mit ihrem gesamten Vermögen haften. Wer dem entgehen möchte, sollte geeignete Sicherheitsmaßnahmen ergreifen. Werden diese Maßnahmen mit einem übergeordneten Risikomanagement verknüpft und von IT-Security-Beratern ausgeführt, bürgen sie für eine Zunahme an Sicherheit und entlasten die Unternehmensleitung durch die Vorsorge und eine sorgfältige Dokumentation von ihrer Haftungspflicht. Darüber hinaus begünstigt eine sorgfältige Analyse der einzelnen Prozessschritte ein hohes Maß an Prozessbewusstein, das mit dazu eingesetzt werden kann, Effizienzvorteile zu erzielen.

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

1. Die gesetzlichen Pflichten von Unternehmensvorständen, Geschäftsführern oder Einzelunternehmern

Eine der Kernaufgaben jeder Unternehmensleitung, ob börsennotiert oder nicht, liegt darin, die Risiken ihres unternehmerischen Handelns zu erkennen und damit umzugehen. Im Umgang mit Informations-und Kommunikationssystemen bedeutet das vor allem, durch Sicherungsmaßnahmen und Kontrollen geregelte Arbeitsabläufe sicherzustellen. Und wenn dennoch einmal Risiken eintreten, soll dies einerseits zeitnah festgestellt werden. Andererseits sollten bereits definierte Gegenmaßnahmen zur Eindämmung der Risiken vorgenommen werden können.

Dazu sind Personen gesetzlich verpflichtet, die Leitungsaufgaben in Unternehmen wahrnehmen. Grundlage hierfür sind sowohl § 43, Absatz 1 des GmbH-Gesetzes (GmbHG) als auch § 93, Absatz 1, Satz 1 des Aktiengesetzes (AktG), das besagt, dass die Mitglieder der Geschäftsleitung bei der Führung der Geschäfte die Sorgfalt eines ordentlichen Geschäftsmanns anzuwenden haben. Und in § 91, Absatz 2 des Aktiengesetzes werden sie sogar verpflichtet, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Dass diese Forderung auch für die Geschäftsführer einer GmbH gilt, ist in Juristenkreisen allgemein anerkannt. Brisant werden diese Regelungen für die Funktionsträger dadurch, dass sich aus der Verpflichtung auch eine Haftung gegenüber dem Unternehmen ergibt, wenn sie ihre Pflichten nicht oder nur unzureichend erfüllen (vgl. § 43 Abs. 2 GmbHG, § 93, Abs. 2 AktG). Dass dies auch für IT-Risiken gilt, besonders wenn die IT-Systeme kritische Geschäftsprozesse unterstützen oder erst ermöglichen, hat der Bundesgerichtshof in der sogenannten ARAG-Garmenbeck-Entscheidung vom 21.04.1997 präzisiert. Wer es versäumt, Risikoüberwachungs- und Abwehrsysteme zu etablieren, haftet als Mitglied der Geschäftsleitung mit seinem gesamten Vermögen.

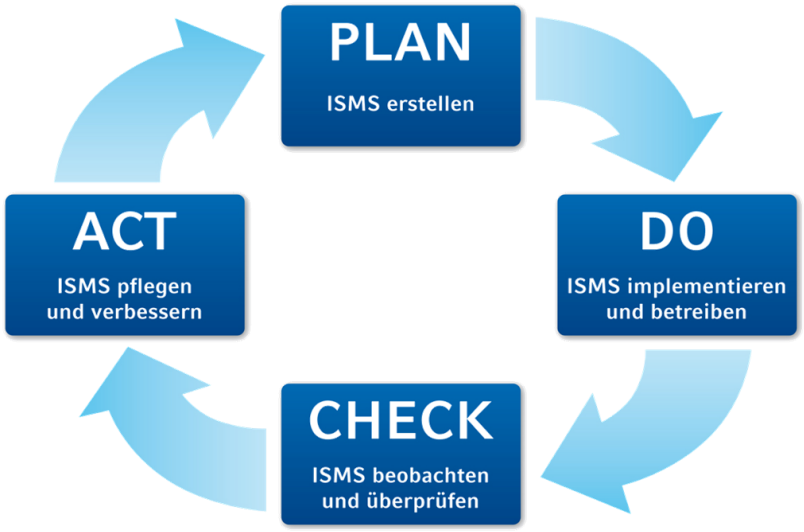
Die gesetzliche Ausgangslage ist also klar: Wer ein Unternehmen leitet, ist dazu verpflichtet, ein angemessenes Risikomanagement zu etablieren, das ein IT-Risikomanagement einschließt. Darüber hinaus verlangt das Bundesdatenschutzgesetz (BDSG), das gemeinsam mit den Datenschutzgesetzten der Länder den Umgang mit personenbezogenen Daten regelt, von der Geschäftsführung eines Unternehmens, Pflichten wahrzunehmen, die nur durch ein präzises Reporting belegt werden können. Dazu gehören die Gewährung der Betroffenenrechte (Benachrichtigung, Auskunft, Korrektur, Sperrung und Löschung von Daten), eine transparente und dokumentierte elektronische Datenverarbeitung, die im Sinne der IT-Sicherheit geschützt ist, sowie die Nachvollziehbarkeit von Zugriffen auf Daten oder deren Weitergabe an Dritte sowie von Änderungen an den Daten.

2. Information-Security-Management-Systeme als Bestandteil des Risikomanagements

Wer seinen gesetzlichen Pflichten im Umgang mit IT-Risiken nachkommen möchte, dem bietet die Implementierung eines Information-Security-Management-Systems (ISMS) eine geeignete Grundlage. Als strukturierte Herangehensweise für den Umgang mit Risiken, die sich aus dem Betrieb von IT-Systemen ergeben, weist es nach, dass eine Unternehmensführung ihre Leitungsaufgabe in diesem Bereich angemessen erfüllt. Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die Aufgaben und Aktivitäten lenkt, die auf Informationssicherheit ausgerichtet sind. Dazu gehört auch ihre Planung, ihr Einsatz und ihre Durchführung sowie die Überwachung und Verbesserung. Als grundlegende Komponenten umfasst ein ISMS die Management-Prinzipien, die zur Verfügung stehenden Ressourcen und Mitarbeiter sowie den darauf aufbauenden Sicherheitsprozess. Der Sicherheitsprozess wiederum besteht aus einer Leitlinie zur Informationssicherheit, in der sowohl die Sicherheitsziele als auch die Strategie zu ihrer Umsetzung dokumentiert sind. Dazu kommen noch das zugrundeliegende Sicherheitskonzept und die eingesetzte Informationssicherheitsorganisation. Dabei sind die Informationssicherheitsorganisation sowie das Sicherheitskonzept Werkzeuge, mit denen die Verantwortlichen ihre Sicherheitsziele umsetzen. Einmal geplant, müssen die Sicherheitsmaßnahmen regelmäßig überprüft werden, um festzustellen, ob sie wirksam, angemessen und anwendbar sind – und auch tatsächlich angewendet werden. Lassen sich dabei Schwachstellen oder Verbesserungsmöglichkeiten erkennen, müssen die Maßnahmen entsprechend angepasst werden – ebenfalls nach einer Planungs- und Umsetzungsphase.

Informationssicherheit als Prozess
Gelebte Realität wird ein ISMS im Unternehmen deshalb erst, wenn ein Informationssicherheitsprozess implementiert wurde. Dieser Prozess kann generell modifiziert werden und muss sich jeweils den aktuellen Gegebenheiten anpassen. So ergibt sich ein dynamischer Prozess mit wiederkehrenden Phasen:

- Planung
- Umsetzung/Durchführung
- Überwachung der Ziele/Erfolgskontrolle
- Beseitigung von Schwachstellen, Optimierung/Verbesserung



Gemäß der englischen Benennung der einzelnen Phasen ergibt sich daraus das sogenannte PDCA-Modell (Plan-Do-Check-Act). Das PDCA-Modell ist auch Teil des ISO 27001-Standards und lässt sich auf alle mit dem Sicherheitsprozess verbundenen Aufgaben anwenden.

Zur Planungsphase des Informationssicherheitsprozesses gehört die gründliche Analyse der Rahmenbedingungen, die Festlegung der Sicherheitsziele sowie die Ausarbeitung einer Strategie, mit der diese Ziele erreicht werden sollen. Mit Hilfe des Sicherheitskonzepts und einer geeigneten Struktur der Informationssicherheitsorganisation wird dieses Konzept dann umgesetzt und wie geplant einer Erfolgskontrolle unterzogen. Allerdings hat jedes Unternehmen und jede öffentliche Einrichtung ihre eigenen spezifischen Ausgangsbedingungen, auf die das Konzept entsprechend der jeweiligen Bedürfnisse angepasst werden muss. Deshalb kann das PDCA-Schema grundsätzlich nur eine Orientierung bieten. Empfehlenswert ist es, gemeinsam mit einem erfahrenen Informationssicherheits-Berater das geeignete Managementsystem individuell anzupassen. Das gilt vor allem dann, wenn das Unternehmen frei in der Wahl der eingesetzten Mittel ist und weder durch Marktvorgaben noch gesetzliche Richtlinien auf die Anwendung eines bestimmten Standards festgelegt. Besonders in einer solchen Konstellation schafft das ISMS sinnvolle Leitlinien für den strukturierten Umgang mit IT-Risiken. Dann bedeutet es keinen unnötigen Regelungswust – wie er vielfach mit dem Begriff „Managementsystem“ verbunden wird.

Damit der Informationssicherheitsprozess sinnvoll aufgebaut und praktisch umgesetzt werden kann, sind einige Grundvoraussetzungen erforderlich. Am wichtigsten ist, dass die Unternehmensleitung die Gesamtverantwortung für den Prozess übernimmt. Denn nur wenn die Leitungsebene die Informationssicherheit auch in angemessenem Maße ernst nimmt, kann sich bei den Mitarbeitern das notwendige Bewusstsein für die Bedeutung sicherer Prozesse einstellen. Darüber hinaus ist es notwendig, dass die Informationssicherheit zum integralen Bestandteil aller Prozesse der jeweiligen Organisation gemacht wird. Sicherheitsanforderungen dürfen sich nicht auf den IT-Bereich beschränken, sondern sie müssen beim Design von Geschäftsprozessen in angemessener Weise mit berücksichtigt werden.

Für den Erfolg des Informationssicherheitsprozesses ist es deshalb wichtig, dass die Unternehmensführung den Sicherheitsprozess initiiert und dafür eine vollständige Strategie mit sinnvollen Zielen festlegt, deren Einhaltung sie überwacht und steuert. Dazu gehört es, die Mitarbeiter zur Mitwirkung an den Sicherheitszielen zu motivieren, die erforderlichen Ressourcen bereitzustellen sowie die organisatorischen Rahmenbedingungen zu schaffen. Damit der Informationssicherheitsprozess effektiv greifen kann, müssen darüber hinaus auch die Auswirkungen von Sicherheitsrisiken auf die gesamte Geschäftstätigkeit beziehungsweise die Aufgabenerfüllung der Organisationseinheit ermittelt werden. Nur so lässt sich seine Bedeutung effektiv ermitteln und herausstellen. Darüber hinaus ist es ganz wesentlich, dass bei der Einführung des Prozesses erreichbare Ziele gesetzt werden – denn Informationssicherheit ist ein langfristiger, kontinuierlicher Prozess. Wird dieser gleich zu Beginn mit zu ehrgeizigen Zielen oder unrealistischen Vorgaben belastet, ist sein Scheitern deutlich wahrscheinlicher. Oft ist es deshalb empfehlenswert, in einzelnen überschaubaren Bereichen zu beginnen und das angestrebte Sicherheitsniveau erst schrittweise durchgängig zu erreichen. Gleiches gilt für den Einsatz der Mittel: Zuerst sollten die effektivsten Maßnahmen durchgeführt werden, die für Schutz gegen die größten Risiken sorgen. Um das einschätzen zu können, ist es wichtig zu erkennen, welche die wichtigsten Geschäftsprozesse sind. Denn nur so lassen sich die wesentlichen Handlungsfelder bestimmten.

Grundsätzlich entsteht Informationssicherheit immer aus dem Zusammenwirken von Organisation und Technik. Dabei lassen sich die Kosten für Technologie und Sicherheitsprodukte unmittelbar am Budget ablesen. Sie sollten so eingesetzt werden, dass sie optimalen Nutzen bieten. Dafür müssen sie zweckgerichtet und zielorientiert eingesetzt werden – und die Mitarbeiter für den Umgang mit ihnen geschult werden. Es ist deshalb weder nötig noch sinnvoll, maximale Sicherheit allein über die Technologie zu erreichen. Der Kostenaufwand dafür ist nicht vertretbar. Hier lohnt es sich, Expertenrat einzuholen. Grundsätzlich kommt es aber bei der Einführung des Informationssicherheitsprozesses besonders darauf an, dass die Verantwortlichen mit gutem Beispiel vorangehen, an sämtlichen Schulungen teilnehmen und alle Maßnahmen konsequent umsetzen.

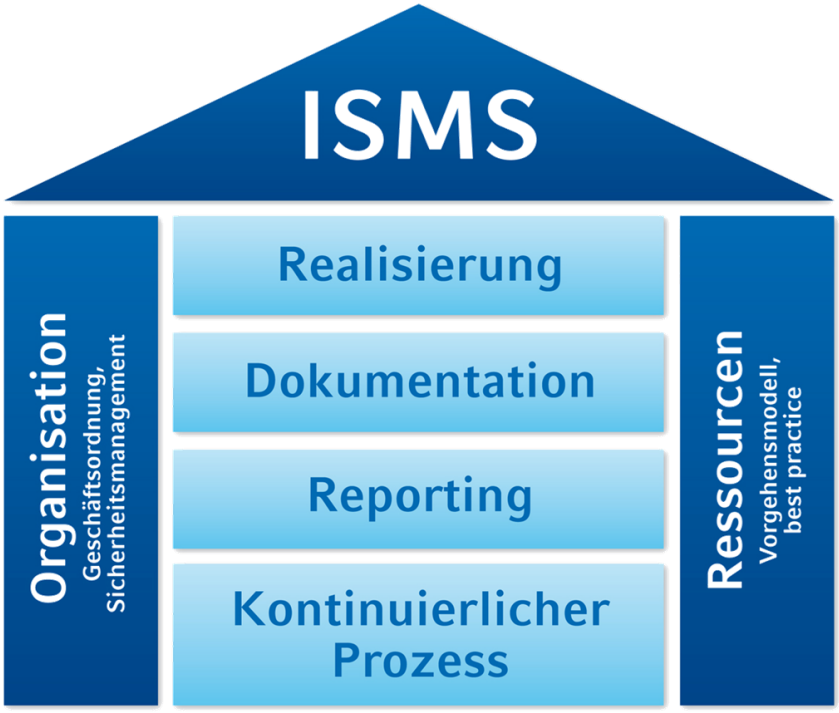
Um den Erfolg des Prozesses einschätzen zu können und dauerhaft zu gewährleisten, sind regelmäßige Überprüfungen und kontinuierliche Verbesserungen erforderlich. Und der Erfolg der Maßnahmen muss sich in der Praxis herausstellen. Es muss klar werden, dass Strategie und Konzept tatsächlich funktionieren. Damit das regelmäßig ermittelt wird, gehören Überprüfungsaudits zu einem funktionierenden Informationssicherheitsprozess. Sie sollten von externen Auditoren vorgenommen werden, da es ungleich schwieriger ist, Fehler oder Verbesserungsmöglichkeiten in den eigenen Konzepten zu finden. Außerdem muss immer wieder überprüft werden, ob die zugrundeliegenden gesetzlichen Vorgaben noch aktuell sind. Die regelmäßige Kontrolle des Sicherheitsprozesses ist dabei insgesamt gesehen ein Instrument zu seiner Verbesserung und schärft die Wirksamkeit und Effizienz der gewählten Sicherheitsstrategie. Gelingt das nicht oder verändern sich ihre Ziele über die Zeit, so sollte die Strategie noch einmal überdacht und gegebenenfalls neu geplant werden.

Reporting: Aussagekräftige Daten in Echtzeit überwachen

Um diese wichtigen Überprüfungen vornehmen zu können, sind eine gute Dokumentation und ein aussagekräftiges Reporting wesentliche Elemente, auf die sich der Informationssicherheitsprozess stützt. Es liefert die Datenbasis, auf deren Grundlage die Geschäftsleitung ihre Lenkungsverantwortung wahrnehmen kann. Über die grundsätzliche Risikosteuerungspflicht hinaus verlangt das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) nämlich ein Früherkennungssystem, das Aussagen zu Risiken und Risikostruktur zulässt. Um das erstellen zu können, ist es erforderlich, Compliance-Anforderungen, die für ein Unternehmen gelten, gemeinsam mit den Maßnahmen zur Lenkung (Governance) in Kennzahlen zu überführen, die sich im Unternehmensalltag messen lassen. Werden diese Daten über einen längeren Zeitraum hinweg gesammelt und gebündelt, bieten sie die Möglichkeit zum Periodenvergleich, aus dem Trends ablesbar sind. Hat das Unternehmen die Trends erst einmal erkannt, bieten sie die Grundlage für Maßnahmen, die dem Trend entgegenwirken oder ihn unterstützen können. Beispiele für Kennzahlen aus dem technischen Bereich können etwa die Anzahl der erkannten Viren pro Tag oder Nutzer am Gateway oder Client, die Anzahl der Firewall-Regeln und Regeländerungen pro Monat, die Anzahl der externen Kommunikationspartner und die Anzahl der erkannten Einbruchsversuche sein. Im Bereich Datenschutz eignen sich beispielsweise die Anzahl der Anträge auf Selbstauskunft, die Anzahl der Datenlöschungsanträge, die Anzahl der überwachten/nicht überwachten Systeme, die Anzahl der Störmeldungen oder Angriffe, die Anzahl und das Ergebnis der Notfallübungen sowie die Anzahl und das Ergebnis von Penetrationstests.

Da das Reporting dem Management als Steuerungsinstrument dienen soll, müssen die Kennzahlen für das Management zusätzliche Anforderungen erfüllen. Sie müssen aussagekräftig sein, für sich selbst sprechen und einen Trend erkennen lassen, während sie gleichzeitig einfach gestaltet und überschaubar sind. Das ist erforderlich, damit die Kennzahlen übersichtlich sind und den Bedürfnissen der jeweiligen Management-Ebene entsprechen. Beispiele für diese aufbereiteten Kennzahlen sind etwa die prozentuale Änderung der Kundenbeschwerden über die Verletzung der Informationssicherheit, die prozentuale Änderung der Kundenbeschwerden über die Verletzung ihres Datenschutzes, die Anzahl unakzeptabler operativer Risiken und ihre Änderung, die Anzahl des Fehlverhaltens von Mitarbeitern in Zusammenhang mit Sicherheitsvorfällen und ihre Änderung sowie die Budgetreue des ISMS-Projekts. Die Auswahl und Definition der geeigneten Kennzahlen sollte deshalb in enger Abstimmung mit einem Fachmann für Informationssicherheit erfolgen. Dessen Know-how ist insbesondere beim Abgleich zwischen den gesetzlichen sowie betrieblichen Anforderungen und den technisch wie organisatorisch vorhandenen Möglichkeiten wertvoll.

Für eine bessere Effizienz des Risikomanagements ist es erstrebenswert, die Kontrolle der wichtigsten Kennzahlen in Echtzeit durchführen zu können. Das fördert eine schnelle Risiko-Erkennung und trägt zur Vermeidung beziehungsweise einem besseren Umgang mit den Risiken bei. Das gelingt insbesondere dann gut, wenn das ISMS so aufgestellt ist, dass es Wiederholungen erkennt, vereinheitlicht und zusammenführt, damit die jeweiligen Daten nur einmal interpretiert werden müssen. Dafür muss immer wieder der jeweilige Stand der Dinge mit den Vorgaben abgeglichen werden. Das entlastet dann auch die einzelnen Geschäftseinheiten von unnötigen Zusatzaufgaben. Gelingt dies mit einem hohen Reifegrad, so lassen sich die Vermögensrisiken für das Unternehmen durch den Informationssicherheitsprozess weitgehend ausschalten – insbesondere dann, wenn alle Beteiligten durch regelmäßige Berichte über den aktuellen Status im Bilde sind. Denn so festigt sich im Unternehmen eine sicherheits- und risikenbewusste Unternehmenskultur, die dazu beiträgt, Risikobetrachtungen bereits im Zuge einer Entscheidungsfindung vorzunehmen.



3. Information Security Management als Bestandteil der IT-Governance

Konsequent umgesetzt, gehören die Elemente des Informationssicherheitsprozesses in den Aufgabenbereich der IT-Governance. Das bedeutet, die Identifizierung, Bewertung und Steuerung IT-spezifischer Risiken sowie die Berichte darüber sollten automatisiert erfolgen und auf demselben Weg auch Nutzereingriffe nur dort einfordern, wo sie notwendig sind. Zu den regelmäßig zu behandelnden IT-Risiken gehören unter anderem die Steuerung der Informationssicherheit vertraulicher Unternehmensdaten im Unternehmensnetzwerk sowie im Internet, das Outsourcing und Offshoring von IT-Leistungen, die Nutzung externer Speichermedien (verbunden mit der Gefahr von Datenverlusten und Manipulationen) sowie die wachsende Verbreitung von Computerviren.

Um alle diese Risikobereiche kontinuierlich zu betrachten, wurde eine Reihe von Informationssicherheitsstandards entwickelt, die jeweils ein Grundgerüst der notwendigen Bausteine enthalten. Darüber hinaus definieren sie die Schnittstellen zu den vorhandenen Überwachungssystemen sowie dem gesamten Berichtswesen. Darauf aufbauend, muss ein zentrales Workflow-Managementsystem entwickelt werden, das alle relevanten Daten zur Erfassung und Bewertung der Unternehmensrisiken bereitstellt und standardisierte Reaktionsweisen enthält. Der für ein Unternehmen geeignete Standard sollte dabei in Abstimmung mit einem Experten ausgewählt, festgelegt und angepasst werden. Unternehmen, die internationale Geschäftskontakte unterhalten, sollten beispielsweise oft schon alleine deshalb den ISO 27001-Standard einsetzen, weil sie damit weltweit anerkannte Normen erfüllen. In Deutschland hat sich insbesondere im behördlichen Umfeld die IT-Grundschutz-Vorgehensweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) etabliert. Und Banken müssen sich den Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) stellen. Allen diesen Systemen ist gemeinsam, dass sie komplexe Zusammenhänge mit einer strukturierten Herangehensweise vereinheitlichen, für einen nachvollziehbaren Überblick sorgen und damit die Voraussetzungen für eine gezielte Steuerung schaffen. Sie enthalten jeweils die typischen Grundanforderungen des Umfelds, aus dem sie stammen. Darüber hinaus gibt es eine Reihe weiterer Information Security Management Systeme, die jeweils sinnvolle Kriterien aus ihrem Entstehungsumfeld bündeln und standardisieren. Sind die Regeln im Unternehmen implementiert und werden in der täglichen Praxis eingehalten,

kann sich die Firma nach dem jeweils angewandten Standard zertifizieren lassen. Für Unternehmen, die an keine direkten Branchenanforderungen gebunden sind, empfiehlt es sich, gemeinsam mit Experten ein schlankes Modell zu entwickeln, dass die eigenen Risiken und Anforderungen effizient abdeckt, sich dabei aber an bestehenden Vorgehensweisen orientiert. Ein solches individuell angepasstes ISMS sitzt wie ein Maßanzug, ohne im selben Maße teuer zu sein. Eingebettet in sämtliche relevanten Geschäftsprozesse und mit dem übergeordneten Risikomanagement verknüpft, trägt es darüber hinaus dazu bei, die Effizienz der gesamten Organisation zu verbessern, indem es das Prozessbewusstsein in allen wichtigen Unternehmensbereichen schärft.

4. Fazit

Sich zuverlässig gegen Risiken abzusichern, die sich aus ihrem Geschäftsbetrieb ergeben, gehört zu den gesetzlichen Grundanforderungen an Unternehmen. Gesetzte wie das Aktiengesetz (AktG), das GmbH-Gesetz (GmbHG), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und das Bundesdatenschutzgesetz (BDSG) enthalten zahlreiche Bestimmungen darüber, dass Unternehmen Vorsorgemaßnahmen treffen müssen und in welchem Umfang sie für Sicherheit sorgen sollen. Die Verantwortung für den Umgang mit Risiken sehen alle diese Gesetze grundsätzlich beim Unternehmer, dem Geschäftsführer einer GmbH oder dem Vorstand einer Aktiengesellschaft. Gemeinsam mit den Mitgliedern der Geschäftsleitung ist dieser Personenkreis für alle Schäden haftbar, die durch fehlende Schutzmaßnahmen entstehen. Auch bei Fahrlässigkeit sehen die Gesetze diejenigen in der Verantwortung, die aufgrund ihrer Position innerhalb der Organisation die Möglichkeit dazu hätten, für geordnete Verhältnisse zu sorgen.

Um einer Haftungspflicht zu entgehen, müssen die Verantwortlichen den Nachweis eines angemessenen Risikomanagements erbringen. Dazu ist insbesondere der Einsatz gängiger Information-Security-Management-Systeme (ISMS) geeignet. Mit einem kontinuierlichen Informationssicherheitsprozess als Herzstück werden dabei im Zuge einer strukturierten Herangehensweise die typischen Unternehmensrisiken kontinuierlich überwacht, so dass die Unternehmensleitung bei Bedarf steuernd eingreifen kann. Wer bei der Konzeption und Implementierung eines ISMS auf die Erfahrung eines Beraters für Informationssicherheit vertraut, kann darüber hinaus sichergehen, dass die Durchführung der Arbeiten fachlich einwandfrei erfolgt. Der Fachmann analysiert das Umfeld des Unternehmens gründlich, erkundet die Anforderungen der Kunden und des Marktes, erfasst besondere gesetzliche Bestimmungen und empfiehlt auf Grundlage der so gewonnenen Erkenntnisse die geeigneten Maßnahmen. Das heißt, er spricht eine Empfehlung aus, welcher Standard angewendet werden soll oder stellt für Unternehmen, die keinen branchenspezifischen Anforderungen unterliegen ein individuelles ISMS auf, das exakt auf den jeweiligen Bedarf zugeschnitten ist.

Für die Verknüpfung des IT-Risikomanagements mit den Arbeiten in allen Geschäftsbereichen des Unternehmens ist es erforderlich, die Abläufe genau zu analysieren. In diesem Zusammenhang entsteht ein hohes Maß an Prozessbewusstsein, über das sich häufig zusätzliche Effizienzvorteile generieren lassen. Zusätzlich gilt, dass die Unternehmen sich für die Einhaltung ihres ISMS zertfizieren lassen und damit den eigenen Kunden und dem Markt die Einhaltung von Branchenvorgaben und der gesetzlichen Bestimmungen dokumentieren können.
Unternehmen, die sich für den Einsatz eines ISMS entscheiden, gewinnen also die Sicherheit, dass sie alle gesetzlichen Vorgaben einhalten, Branchenbestimmungen erfüllen, ihre Geschäftsrisiken überschaubar halten und dabei auf effiziente Prozesse setzen. Wenn sie die Umsetzung der einzelnen Schritte an Informationssicherheitsexperten übertragen, bürgt deren Know-how für fachliche Qualität und stringentes Projektmanagement.

Links zu IT-Sicherheitsstandards:
ISO 27001: http://www.iso.org/iso/catalogue_detail?csnumber=42103
BSI-IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
MaRisk:
http://www.bundesbank.de/Redaktion/DE/Standardartikel/Kerngeschaeftsfelder/Bankenaufsicht/risikomanagement_marisk_2010.html