Frameworks zum Management von IT-Sicherheit

Rechtsrahmen

Martin Wundram

Der Aufbau sicherer IT-Systeme sowie das Einhalten der gesetzlichen Vorschriften in diesem Dunstkreis sind komplizierte Angelegenheiten. Ohne bewährte Methoden kann das nicht gelingen. Die internationale Norm ISO/IEC 27001 sowie die IT-Grundschutz-Kataloge helfen hier weiter.

Durch zahllose Datenschutz- und Datensicherheitsskandale befeuert, steigt der Druck in Unternehmen und Behörden, effektive Maßnahmen gegen Schlendrian, das Ausspionieren von Belegschaften und technische Unzulänglichkeiten zu ergreifen. Denn solcherlei Affären ramponieren nicht nur nachhaltig das Image, sondern kommen die Übeltäter gelegentlich teuer zu stehen. Sogar der Gesetzgeber sah Handlungsbedarf und hat sowohl die Anforderungen an die IT-Sicherheit als auch die Sanktionen abermals verschärft.

Das Erfüllen der vielen gesetzlichen Vorgaben sowie ein wirksames IT-Sicherheitsmanagement ist praktisch nur noch mit umfassenden und erprobten Methoden möglich, die zudem fortwährend angepasst und verbessert werden müssen. Dazu gehören Managementsysteme für Informationssicherheit (Information Security Management System, ISMS) wie die Norm ISO/IEC 27001 und die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Rahmenbedingungen wie der US-amerikanische Sarbanes-Oxley Act (SOX) und die 8. EU-Richtlinie gelten zunächst nur für große, kapitalmarktorientierte Unternehmen. Ihre Strahlkraft erstreckt sich jedoch auch auf kleinere Unternehmen, etwa GmbHs. Gesetze wie das Bundesdatenschutzgesetz (BDSG) gelten selbstredend für alle, egal ob klein oder groß.

Um die gesetzlichen, vertraglichen und firmeninternen Regelungen einzuhalten, müssen Unternehmen Prozesse zur IT-Compliance einführen. Dieser Bestandteil der IT-Governance gehört als Teilbereich zur Corporate Governance, die das Gestalten von Führung und Überwachung zum Ziel hat (siehe Kästen „Regeln einhalten“ und „Definierte Sicherheit“). Entsprechend muss sich das Management der IT-Sicherheit angemessen in die übergeordneten Unternehmensprozesse eingliedern und sauber in die internen Kontroll-, Risikomanagement- und Revisionssysteme integrieren. IT-Sicherheit bezieht sich damit immer auf die Bedürfnisse des Unternehmens.

Härtere Strafen und Imageprobleme

Das BDSG fordert in § 9 technische und organisatorische Maßnahmen, die nötig sind, um die hier niedergelegten Vorgaben zu erfüllen (dazu gehören zum Beispiel Zugriffskontrollen, Verfügbarkeitsprüfungen und aktuelle Verschlüsselungsverfahren). Bei Verstößen sieht das Gesetz Bußgelder bis zu 300 000 Euro beziehungsweise bis zu einer vollständigen Gewinnabschöpfung und sogar Freiheitsstrafen vor. Seit der zweiten Novellierung 2009 sind nach § 42a bestimmte Vorfälle, in denen unberechtigte Dritte Kenntnis über besonders vertrauliche Daten erlangen, unverzüglich den betroffenen Personen mitzuteilen. Und das Gesetz zur Angemessenheit der Vorstandsvergütung von 2009 führt für diesen Personenkreis eine nicht versicherbare Privathaftung ein (VorstAG, Art. 2). Unternehmen mit unsicheren IT-Systemen haben also nicht nur Kratzer in ihrer Außendarstellung zu befürchten, sondern auch erhebliche finanzielle Einbußen.

Ohne Frameworks geht es nicht

Der Sarbanes-Oxley Act verlangt explizit – formuliert durch die Börsenaufsicht SEC (US Security and Exchange Commission) – die Verwendung anerkannter Frameworks, etwa das COSO-Modell (Committee of Sponsoring Organizations of the Treadway Commission), das die interne Kontrolle vor allem der Finanzberichterstattung verbessern soll. Dieses Verlangen gilt konsequenterweise auch für das IT-Management, sodass CobiT (Control Objectives for Information and Related

Technology) und ISO/IEC 27001 entsprechend einzusetzen sind.

In Deutschland bestehen solche expliziten Vorgaben nicht, wenngleich etliche gesetzliche Rahmenbedingungen umfassende Maßnahmen zum Risikomanagement und der IT-Sicherheit verlangen und anerkannte Frameworks beispielhaft aufführen. So fordert etwa der Deutsche Corporate Governance Kodex ein angemessenes Risikomanagement und -controlling. Dies verlangen auch die Deutschen Rechnungslegungsstandards, zusätzlich verschiedene Prüfungsstandards des IDW, das Versicherungsaufsichtsgesetz und die Mindestanforderungen an das Risikomanagement (MaRisk BA und MaRisk VA). Letztere nennen die Normenfamilie ISO/IEC 2700X sowie den Vorläufer der IT-Grundschutz-Kataloge, das IT-Grundschutzhandbuch. Basel II/Solvency II, die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) verlangen ebenfalls IT-Sicherheit und somit den Schutz vor Hackerattacken, Datenverlusten und Systemausfällen. Unabhängig von den gesetzlichen Ansprüchen an große kapitalmarktorientierte Unternehmen propagieren das GmbH-Gesetz, das Aktiengesetz und das Handelsgesetzbuch ganz allgemein die Sorgfalt eines „ordentlichen Geschäftsmanns“. Daher muss auch ein GmbH-Geschäftsführer sich angemessen mit der IT-Sicherheit seines Unternehmens auseinandersetzen.

Zwangsverpflichtet zur sicheren IT

Die 8. EU Richtlinie 2006/43/EG, auch EuroSOX genannt, wurde 2009 durch das Bilanzrechtsmodernisierungsgesetz (BilMoG) in deutsches Recht überführt. Das Gesetz zwingt kapitalmarktorientierte Unternehmen zwar nicht grundsätzlich zur Einrichtung umfassender Risikomanagementsysteme, macht jedoch deutlich, dass Unternehmensleitung und -aufsicht sich mit der Notwendigkeit, Angemessenheit und Wirksamkeit solcher Systeme beschäftigen sollen. Vergleichbare Ver-

Regeln einhalten

IT-Governance ist wesentlicher Teil der Unternehmensführung und besteht aus den Organisationsstrukturen und Prozessen, die sicherstellen sollen, dass die IT die Unternehmensziele und -strategien erreicht beziehungsweise umsetzt. Dazu gehören Risikomanagement und damit auch IT-Sicherheit sowie IT-Compliance. Letztere kümmert sich um das Einhalten aller relevanten (gesetzlichen) Regeln, Anforderungen und Vorgaben.

Definierte Sicherheit

§ 2 Abs. 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik definiert IT-Sicherheit als „[…] die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen […]“. Das Gleiche gilt bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

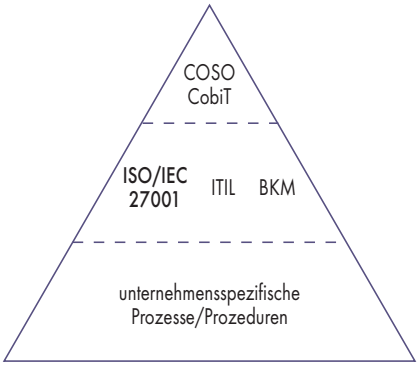
Onlinequellen

BSI IT-Grundschutz
www.bsi.bund.de/cln_156/DE/Themen/ITGrundschutz/itgrundschutz_node.html
ISO/IEC 27001 (kostenpflichtig)
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

pflichtungen existieren bereits, etwa durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG von 1998). Weiterhin müssen Unternehmensführungen und -aufsicht über angemessenen IT-Sachverstand verfügen, falls die Informationstechnik eine herausragende, elementare Bedeutung für die Organisation besitzt. IT-Sicherheit ist somit Chefsache.

Aus dem gesetzlichen Rahmen lassen sich einige zentrale Kriterien für IT-Sicherheit ableiten. Sie muss auf allen Ebenen (strategisch, taktisch, operativ) im jeweils passenden Abstraktionsgrad angemessene Berücksichtigung finden. Die Risiken aus dem IT-Betrieb, dazu gehören etwa Cyber-Attacken, muss das Unternehmen im allgemeinen Risikomanagement erkennen und abfedern. In Abhängigkeit einer individuellen Unternehmens- und Risikostrategie sind die Zuständigen angehalten, strategische Risikoziele zu definieren und das Management der IT-Sicherheit entsprechend zu gestalten. Dazu gehören auch Kompetenzbildung und -pflege auf allen verantwortlichen Ebenen bezüglich IT-Sicherheit.

Um diese Ziele zu erreichen, sind nicht nur die umfassende Kenntnis, sondern auch die Dokumentation aller wesentlichen Prozesse und Ressourcen der IT und des Unternehmens unabdingbar. Wichtig dabei: Man sollte wissen, welche Abläufe von welchen IT-Prozessen in welchem Maße abhängen, damit Sicherheit nicht zum Selbstzweck wird, sondern weiterhin dem Schutz der Organisation und ihrer Daten dient. Bei dieser schwierigen Aufgabe können Frameworks wie ISO/IEC 27001 Beistand leisten. Über ihr Lebenszyklusmodell stellen sie sicher, dass IT-Sicherheit kein einmaliges Projekt bleibt. Zudem liefern sie eine klar dokumentierte und für alle Beteiligten verwendbare Basis. Auch für Außenstehende sollte darüber Transparenz und Nachvollziehbarkeit entstehen. Gegenüber selbst erarbeiteten Verfahren ergeben sich aus dem Einsatz der hier vorgestellten Frameworks potenzielle Sicherheitsvorteile. Denn anerkannte Fachgruppen arbeiten sie nicht nur aus, sondern entwickeln sie zudem kontinuierlich weiter. Und eine Zertifizierung der IT etwa nach ISO/IEC 27001 durch eine unabhängige Stelle erbringt den Nachweis eines geprüften ISMS [1]. Dies führt zu besserer Compliance, möglicherweise zu Wettbewerbsvorteilen, und wird von Geschäftspartnern sogar manchmal vorausgesetzt.



Normen und Standards im IT-Sicherheitsumfeld bauen aufeinander auf.

Verzahnungen und Abhängigkeiten

Management-Frameworks sind nicht nur hierarchisch miteinander verknüpft, sondern es existieren vielfach Überschneidungen in einzelnen Ebenen. Auf der Governance-Schicht lässt sich COSO, das ein internes Kontrollsystem beschreibt, durch CobiT um Aspekte der IT-Governance erweitern. Zwar beinhaltet dieses Framework Elemente für das Sicherheitsmanagement, beispielsweise definiert es Anforderungen an Informationen (Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit et cetera). Es bietet jedoch keine umfassenden Mechanismen für das Umsetzen von IT-Sicherheit. Die lassen sich in der Ebene „Sicherheit und Servicemanagement“ mit Frameworks wie den Grundschutz-Katalogen realisieren (siehe Abbildung).

Von den zahlreichen Frameworks eignen sich zwei besonders, wenn es um das Erfüllen gesetzlicher Vorgaben geht: die schon genannten ISO/IEC 27001 und die IT-Grundschutz-Kataloge. Unternehmen können sich nach beiden zertifizieren lassen. Beide sind grundsätzlich für das Management einer sicheren IT geeignet. Neben vielen Gemeinsamkeiten gibt es einige wichtige Unterschiede. ISO/IEC 27001 ist eine international entwickelte Norm, die Grundschutz-Kataloge hingegen kommen zurzeit überwiegend in Deutschland zum Einsatz. Ein global ausgerichtetes Unternehmen, das zum Beispiel SOX-konform sein muss, fährt daher mit ISO/IEC 27001 besser.

Konkret oder allgemein

Weiterhin unterscheiden sich beide Frameworks bei den thematisierten Schutzanforderungen. Die Grundschutz-Kataloge nehmen einen mittleren Bedarf an und beschreiben explizite technische Maßnahmen. Die Norm hingegen gibt einen Rahmen vor, den das Unternehmen an seine ureigenen Schutzbedürfnisse anpassen muss. Sie kümmert sich nicht um die konkrete Ausgestaltung der Technik. Die Organisation ist daher verpflichtet zu prüfen, wie hoch ihr Schutzbedarf in Sachen IT tatsächlich ist. Erfreulicherweise kann man zunächst mit dem ein wenig starren und ins Detail gehenden Werk des BSI einen kostengünstigen Grundschutz etablieren, der den gesetzlichen Mindeststandard abdeckt. Darauf aufbauend oder alternativ lässt sich ein Managementsystem nach ISO/IEC 27001 einführen. Die Grundschutz-Kataloge lehnen sich in Verbindung mit den frei verfügbaren BSI-Standards 100-1 bis 100-4 eng an die ISO-Norm an und positionieren sich damit als gleichwertige Alternative. Ein Unternehmen kann daher nach ISO/IEC 27001 auf der Basis von IT-Grundschutz eine entsprechende Beglaubigung erhalten. Darüber lässt sich zugleich ein angemessenes und wirksames ISMS sowie die korrekt implementierte Grundschutzmethodik nachweisen. (jd)

MARTIN WUNDRAM

ist Geschäftsführer der TronicGuard GmbH in Dormagen.

Literatur

[1] Ronny Frankenstein; Zertifizierung; Qual der Wahl, Zwei Rahmenwerke zur IT-Sicherheit unter der Lupe; *iX* Special "Sicher im Netz", *iX* 3/2010, S. 142