

Kapitel 2

IT-Sicherheitspolicy

2.1 Einordnung der IT-Sicherheitspolicy

Regelungen zur Sicherheit werden in einem Unternehmen auf drei Ebenen definiert, die im Folgenden beschrieben werden:

- **Sicherheitsgrundsätze:** Auf der obersten Ebene der Sicherheitsarchitektur befinden sich die Sicherheitsgrundsätze, die den Rahmen zur Umsetzung der Sicherheitspolitik aufzeigen und die prinzipiellen Verantwortlichkeiten festlegen.
- **Umsetzungsstrategie:** Die Umsetzungsstrategie beinhaltet weiterreichende Regeln und Strategien zu grundsätzlichen Sicherheitsanforderungen. Diese beschreiben das, was an Sicherheitsstrategien zu berücksichtigen und umzusetzen ist.
- **Sicherheitsmaßnahmen:** In den Sicherheitsmaßnahmen werden detaillierte Konzepte und als Unterbau weiterführende Anweisungen und technische bzw. organisatorische Maßnahmen festgelegt, die sich auf die aktuelle System-Plattform, auf Anwendungen oder aktuelle organisatorische Strukturen des Unternehmens beziehen. Diese Dokumente beschreiben das wie der Umsetzung der Sicherheitsstrategien.

2.2 Definition des Geltungsbereichs

Die Sicherheitsgrundsätze sind für alle Organisationseinheiten in einem Unternehmen verbindlich. Insbesondere richten sie sich an alle Mitarbeiter und externen Dienstleister, die IT-Komponenten für das Unternehmen entwickeln, betreiben oder deren Dienste vom Unternehmen selbst genutzt werden. Falls eine netzwerktechnische Anbindung für einen Dritten (Kunde) nicht entsprechend dem Sicherheitsstandard gestaltet werden kann, sind die Sicherheitsgrundsätze und die daraus abgeleiteten Regelungen auch für diesen bindend.

Die Sicherheitspolitik wird in Abstimmung mit der Geschäftsführung erstellt und von dieser verabschiedet. Die aktuelle Version wird zeitnah veröffentlicht und kommuniziert.

Ausnahmen, die von den Sicherheitsgrundsätzen und den untergelagerten Umsetzungsstrategien und Sicherheitsmaßnahmen abweichen oder diese nicht berücksichtigen, sind durch eine Entscheidungs-Vorlage mit der Begründung der Nichteinhaltung und den daraus entstehenden Risiken zu dokumentieren und müssen per Beschluss von der Geschäftsführung genehmigt werden.

2.3 Sicherheitsgrundsätze

Die Sicherheitsgrundsätze definieren die Sicherheitspolitik eines Unternehmens.

2.3.1 Sicherheitsgrundsatz 1: Unternehmensziel

Eine sichere Informationsverarbeitung ist unabdingbare Voraussetzung für alle Geschäftsprozesse im Unternehmen. Die Geschäftsleitung sieht die Sicherheit daher als integralen Bestandteil der Unternehmenspolitik an.

Aufgrund der Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung müssen Sicherheitsaspekte bei der Gestaltung und Umsetzung dieser Geschäftsprozesse besonders berücksichtigt werden. Die Ziele des Unternehmens können nur bei ordnungsgemäßer und verlässlicher Abwicklung der Geschäftsprozesse erreicht werden.

Ein hohes und unter betriebswirtschaftlichen Gesichtspunkten vertretbares Sicherheitsniveau dient dem Schutz des gesamten Unternehmens, der Geschäftspartner, Kunden und Mitarbeiter. Aus diesem Grund werden umfangreiche, fortlaufende Sicherheitsmaßnahmen in allen Bereichen ergriffen, um berechnete Interessen der Geschäftspartner, Kunden und Mitarbeiter zu schützen.

2.3.2 Sicherheitsgrundsatz 2: Schadensvermeidung

Ein Sicherheitsziel ist es, operationale Risiken durch Vorsorgemaßnahmen zu mindern und Schäden frühstmöglich entgegenzuwirken.

Risiken im Ablauf der Geschäftsprozesse und der genutzten Informationsverarbeitung zählen zu den operationalen Risiken im Unternehmen. Diese Risiken sind unter Berücksichtigung wirtschaftlicher Aspekte auf ein vertretbares Maß zu reduzieren.

Der Aufwand für die Schadensvermeidung hängt im Wesentlichen davon ab, welche Risiken im Bereich der Sicherheit vertretbar sind. Für die untragbaren Risiken sind geeignete Maßnahmen zu finden, um diese auf ein vertretbares Maß zurückzustufen. Die Maßnahmen können dabei die Reduktion der Eintrittswahrscheinlichkeit und/oder die Schadenshöhe beeinflussen. Die Kosten dieser Maßnahmen müssen in einem angemessenen Verhältnis zum vermiedenen Schaden stehen.

2.3.3 Sicherheitsgrundsatz 3: Sicherheitsbewusstsein

Alle Mitarbeiter müssen über ein ausgeprägtes Sicherheits- und Qualitätsbewusstsein bei der von ihnen ausgeübten Arbeit verfügen. Dieses verpflichtet einerseits jeden Mitarbeiter, bestehende Sicherheitsregelungen zur Kenntnis zu nehmen und anzuwenden, und andererseits, unverzüglich zuständige Führungskräfte oder Security-Beauftragte¹ über vorliegende Sicherheitsrisiken zu informieren.

Ein ausgeprägtes Sicherheits- und Qualitätsbewusstsein der Mitarbeiter ist Voraussetzung für eine erfolgreiche Planung, Umsetzung und Aufrechterhaltung der Sicherheit innerhalb des Unternehmens. Die Früherkennung möglicher Sicherheitsrisiken und deren sofortige Beseitigung sind im Interesse des Unternehmens sowie seiner Geschäftspartner von allen Mitarbeitern im Rahmen der täglichen Arbeit zu leisten. Insgesamt müssen Risiken konsequent auf ein akzeptables Risikoniveau gesenkt werden. Die Mitarbeiter müssen daher entsprechend sensibilisiert sein und durch geeignete Schulungen und/oder Informationen auf dem neuesten Stand gehalten werden. Hierbei ist die Verfügbarkeit und Aktualität der zugehörigen Dokumentationen von besonderer Bedeutung.

2.3.4 Sicherheitsgrundsatz 4: Gesetzliche, aufsichtsrechtliche und vertragliche Pflichten

Gesetzliche und aufsichtsrechtliche Verpflichtungen sowie vertragliche und unternehmensinterne Vorgaben an die Informationsverarbeitung sind zu erfüllen und dienen dem Schutz der Kunden, Geschäftspartner, Mitarbeiter und Anteilseigner des Unternehmens sowie des Unternehmens selbst.

Sicherheitsanforderungen und Sicherheitsmaßnahmen werden auf der Grundlage sicherheitsrelevanter gesetzlicher, aufsichtsrechtlicher und vertraglicher Re-

¹ Ansprechpartner, Koordinator zu Sicherheits-Themen im Fachbereich.

gelingen festgelegt. Änderungen oder neue Regelungen erfordern entsprechende Aktualisierung der Sicherheitskonzepte, Anweisungen und Maßnahmen sowie deren zeitnahe Umsetzung.

2.3.5 Sicherheitsgrundsatz 5: ***Maßnahmen gemäß allgemeingültiger Sicherheitsstandards***

Daten und Ressourcen des Unternehmens sind in hohem Maße durch technische und organisatorische Maßnahmen gemäß allgemeingültiger Sicherheitsstandards und -richtlinien zu schützen. Diese Maßnahmen dienen der Erreichung des gesetzten IT-Sicherheitsstandards. Zur grundsätzlichen Orientierung dienen das BSI-Grundschutzhandbuch sowie die einschlägigen Normen.

Die erforderlichen Sicherheitsmaßnahmen werden für alle Daten und Ressourcen geplant und umgesetzt sowie bei Veränderungen der Sicherheitsanforderungen kontinuierlich angepasst. Insbesondere müssen die Maßnahmen in ihrer Umsetzung sicherstellen, dass ein angemessener Schutz der Verfügbarkeit, der Vertraulichkeit, der Integrität, der Verbindlichkeit und Authentizität der Daten und Ressourcen erreicht wird und der störungsfreie und korrekte Ablauf aller Geschäftsprozesse gewährleistet ist. Soweit betriebswirtschaftlich vertretbar, sind die redundante Auslegung geschäftskritischer Anwendungen und Systeme, Backup und Bereitstellung aktueller Notfallkonzepte für die Kerngeschäftsprozesse des Unternehmens von sehr hoher Bedeutung.

2.3.6 Sicherheitsgrundsatz 6: ***Aufrechterhaltung des Geschäftsbetriebes***

Das mögliche Schadenspotenzial bei Störungen der Kerngeschäftsprozesse ist steuerbar. Geschäfte können auch in Krisen- und Notfallsituationen in vertretbarem Maß getätigt und abgewickelt werden.

Für geschäftskritische IT-Systeme und IT-Anwendungen existieren Notfall- und Kontinuitätspläne, die unter Berücksichtigung bestehender Verfügbarkeitsanforderungen Vorgehensweisen spezifizieren für:

- den eingeschränkten Betrieb oder die kontrollierte Einstellung des Betriebs;
- den geregelten Wiederanlauf.

Zuständig für Aktualisierung und Durchführung der in den Notfallplänen festgelegten Aktivitäten ist der jeweilige verantwortliche Eigentümer des Geschäftsprozesses. Ebenfalls ist sicherzustellen, dass Mitarbeiter und auch Dienstleister, die IT-Anwendungen, Komponenten und Systeme betreiben und betreuen, mit den entsprechenden Vorgehensweisen vertraut sind und diese im Rahmen regelmäßiger Übungen praktizieren.

2.3.7 Sicherheitsgrundsatz 7: Sicherheitsarchitektur

Die Umsetzung der Sicherheitspolitik erfolgt durch eine verbindliche Sicherheitsarchitektur, die von dem Sicherheits-Team des Unternehmens vorgegeben und kontinuierlich weiterentwickelt wird.

Die Sicherheitsarchitektur integriert sicherheitsrelevante Elemente wie Sicherheitsgrundsätze, -anforderungen, -maßnahmen und -dienste und ermöglicht eine zielgerichtete Umsetzung der Sicherheitspolitik innerhalb des Unternehmens. In der Sicherheitsorganisation werden Verantwortlichkeiten sowie ausreichende Kompetenzen zur Behandlung sicherheitsrelevanter Vorkommnisse vergeben. Die Umsetzung der festgelegten Sicherheitsziele erfolgt durch organisatorische und technische Maßnahmen.

2.4 Verantwortlichkeiten

2.4.1 Geschäftsführung und Management

Die Gesamtverantwortung für die Sicherheit innerhalb des Unternehmens liegt bei der Geschäftsführung. Sie ist insbesondere verantwortlich für:

- die Überprüfung, die Abnahme und das Vertreten der Sicherheitspolitik und
- die Weiterentwicklung der Sicherheitsorganisation.

In beratender, empfehlender und unterstützender Form nimmt diese Aufgabe das Sicherheits-Team (IT-Security-Officer) für die Geschäftsführung wahr.

Zur Erreichung eines angemessenen Sicherheitsniveaus tragen die Mitarbeiter im Management eine besondere Verantwortung. Sie müssen sicherstellen, dass im Rahmen der Umsetzung der ihnen und ihren Mitarbeitern übertragenen Aufgaben die Sicherheitsaspekte entsprechend berücksichtigt werden. Dazu gehört insbesondere die Sensibilisierung der Mitarbeiter sowie die Implementierung und Kontrolle von Sicherheitsmaßnahmen.

2.4.2 Sicherheitsorganisation

Die Umsetzung der Sicherheitsgrundsätze erfolgt durch die Sicherheitsorganisation sowie durch alle Mitarbeiter entsprechend ihren Aufgaben in der Linie. Den IT- und fachlichen Administratoren fällt eine besondere Rolle zu, da der sichere Betrieb von IT-Systemen und IT-Anwendungen eine der tragenden Säulen der Umsetzung darstellt.

Die Prüfung der Umsetzung und Einhaltung der Sicherheitsgrundsätze obliegt dem Sicherheits-Team gemeinsam mit den zuständigen Security-Beauftragten; situativ werden das Controlling (Risk-Controlling) und die Revision zusätzlich mit eingebunden. Unabhängig davon prüft die Revision im Rahmen ihrer Prüfpläne u. a. auch die Einhaltung von Sicherheitsmaßnahmen, die aus gesetzlichen und aufsichtsrechtlichen Anforderungen resultieren.

Mit der für das Controlling zuständigen Organisationseinheit erfolgt eine methodische und prozessuale Abstimmung bezüglich des Themas „Operationale Risiken“.

Die Sicherheitsorganisation wird gebildet aus:

- dem Sicherheits-Team (IT-Security-Officer, Team in der Abt. Organisation & Service);
- den Security-Beauftragten (mindestens ein Mitarbeiter je Bereich/Hauptabteilung);
- den Sicherheitsadministratoren (IT-Anwendungs- und IT-Systembetreuung, RZ-Betrieb);
- der Berechtigungsverwaltung.

Aufgaben des Sicherheits-Teams sind:

- Erarbeitung und Weiterführung der Sicherheitsstrategien, -regeln, -konzepte, -anweisungen und -maßnahmen;
- Allgemeine Beratung und Unterstützung zum Thema Sicherheit;
- Projektbegleitende Beratung zur Sicherheitskonzeption auf Anforderung des Fachbereichs und Prüfmaßnahmen bei der Übergabe von Projekten;
- Mitarbeitersensibilisierung und -schulung in Kooperation mit der Abteilung Personal;
- Bearbeitung und Auswertung von Sicherheitsvorfällen zur Lokalisierung von Schwachstellen;
- Prüfung der Umsetzung von Sicherheitsgrundsätzen, Umsetzungsstrategien und Sicherheitsmaßnahmen;
- Kontrolle und Überwachung der Durchführung regelmäßiger Prüfungen sicherheitskritischer Anwendungen und Systeme;
- Situative und ereignisbezogene Initiierung von Sicherheits-, Risikoüberprüfungen und Notfallübungen.

Aufgaben der Berechtigungskoordination als Funktion im Sicherheitsteam:

- Erstellung und Pflege von Berechtigungskonzepten (Rollendefinition, Neuanlage/Änderung/Löschung von Berechtigungen, Automatisierung der Pflege, Infodienste);
- Formal-, Plausibilitätsprüfung und Koordination aller Berechtigungsvergaben;
- Einholung notwendiger Zustimmungen für die Berechtigungsvergabe.

Aufgaben des Security-Beauftragten im Fachbereich:

- Erste Anlaufstelle für alle Mitarbeiter des Fachbereiches zu Sicherheitsfragen und -problemen;
- In Gefahren- oder Krisensituationen Einleitung von Sofortmaßnahmen zur Schadensvermeidung oder Schadensbegrenzung;
- Eskalation und Weitergabe von Informationen an Linienvorgesetzte und an das Sicherheits-Team;
- Bearbeitung von Sicherheitsvorfällen und Erstellung von Statusberichten;
- Mitwirkung an der Verbesserung und Aktualisierung der Sicherheitsregeln, -konzepte, -anweisungen und -maßnahmen;
- Koordination und Unterstützung bei Sicherheitsthemen (Projektbegleitung, Audits, Ausfallübungen, Schulung, Einweisung).

Aufgaben der Sicherheitsadministratoren des operationalen IT-Betriebs:

- Installation, Betrieb von IT-Sicherheitseinrichtungen;
- Überwachung von IT-Systemen und Durchführung von Kontrollmaßnahmen;
- Second-Level-Support bzgl. IT-Sicherheitseinrichtungen.

Aufgaben der jeweils zuständigen Berechtigungsverwaltung:

- Administration von Zugriffsrechten für die jeweiligen IT-Anwendungen und IT-Systeme;
- Verwaltung von technischen Accounts, wobei die Administration selbst an die zuständigen Systemadministratoren delegiert wird;
- zeitnahe Dokumentation und Fortschreibung der Berechtigungen.

Bei der Einführung neuer oder bei gravierenden Änderungen bestehender IT-Anwendungen oder IT-Systeme sind angemessene und dem Standard entsprechende Sicherheitskonzepte zu erstellen und zu implementieren. Das Sicherheitsteam berät auf Anforderung des Fachbereichs die Projekte und Aktivitäten bezüglich der Sicherheitskonzeption und überprüft bei der Übergabe im Rahmen eines Projekts die Schutzbedarfsfeststellung und das Sicherheitskonzept. Sofern sicherheitsrelevante Anwendungen oder Systeme durch Dritte betrieben werden, sind zum einen Sicherheitsanforderungen vertraglich zu regeln, zum anderen ist von diesen nachzuweisen, dass angemessene Schutzmaßnahmen implementiert sind.

Falls eine netzwerktechnische Anbindung aus betriebswirtschaftlichen oder technischen Gründen nicht entsprechend den Sicherheitsregeln, -konzepten und -anweisungen realisiert werden kann, sind die Sicherheitsgrundsätze und die daraus abgeleiteten Regelungen auch für diesen Netzwerkpartner (Dienstleister, Kunde)

bindend. Bei Gefährdungen oder Sicherheitsvorfällen, die gemeinsam genutzte Ressourcen betreffen, sind diese Netzwerkpartner in die Eskalationsverfahren und Meldewege mit einzubinden.

Zum Informations- und Erfahrungsaustausch dient ein Arbeitskreis „Sicherheitsmanagement“, an dem das Sicherheits-Team, der DSB, das Service-Management (Provider-Management), Revision, Personal, Berechtigungsverwaltung, Security-Beauftragte, Sicherheitsbeauftragte von Dienstleistern sowie weitere Gäste teilnehmen. Themenvorschläge kann jeder Beteiligte der Sicherheitsorganisation einbringen. Das Sicherheits-Team sammelt die Themen, bereitet die Agenda vor und beruft den Arbeitskreis ein.

2.4.3 Mitarbeiter

Geschäftsführung, Management und Sicherheitsorganisation können vielfach nur die Rahmenbedingungen für die sichere Nutzung, Entwicklung und den Betrieb der IT schaffen. Eine Erreichung der gesteckten Ziele ist wesentlich davon abhängig, dass jeder Mitarbeiter die vorliegenden Sicherheitsgrundsätze und die daraus abgeleiteten Umsetzungsstrategien und Sicherheitsmaßnahmen beachtet und im Rahmen der täglichen Arbeit umsetzt.

Es wird ein ausgeprägtes Sicherheitsbewusstsein von jedem Einzelnen erwartet, damit:

- notwendige Maßnahmen zur Erkennung und Abwendung von Bedrohungen für die Sicherheit von Personen, Informationen und Vermögenswerten eingeleitet werden,
- Problemsituationen schnell und zuverlässig bewältigt werden,
- Risiken identifiziert und an die Verantwortlichen berichtet werden und
- Sicherheit ein Element der Unternehmensphilosophie wird.

Aufgrund von thematischen Überschneidungen zum Gebäudemanagement, das für den Gebäudeschutz zuständig ist, sind insbesondere auch diese Sicherheits- und Verhaltenshinweise bindend.

2.5 Umsetzung

2.5.1 Sicherheitsarchitektur

Ziel der Sicherheitsarchitektur ist es festzulegen, wie die Sicherheit im Unternehmen umgesetzt wird (siehe Abb. 1). Die **Sicherheitsgrundsätze** bilden die oberste Ebene der Sicherheitsarchitektur und legen allgemeine Sicherheitsgrundsätze und Verantwortlichkeiten fest. Die Sicherheitsgrundsätze gelten für das gesamte Unternehmen.

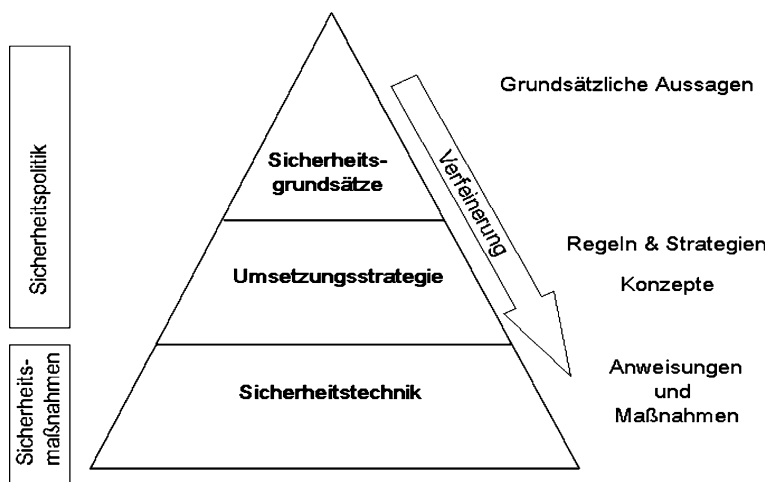


Abb. 1 Sicherheitsarchitektur

Durch die **Umsetzungsstrategie** mit ihren Regelungen werden grundsätzliche Sicherheitsanforderungen und Sicherheitsmaßnahmen beschrieben. Die Regelungen und Strategien gelten ebenfalls für das gesamte Unternehmen.

Die Umsetzungsstrategie wird durch die **Sicherheitsmaßnahmen** ergänzt; wobei in Konzepten und Anweisungen detailliert die Sicherheitsanforderungen und technische bzw. organisatorische Maßnahmen festgelegt werden, die sich auf die aktuelle System-Plattform, IT-Anwendungen oder auch auf die organisatorische Struktur des Unternehmens beziehen.

Da wegen der Kurzlebigkeit von Software und IT-Systemen häufiger mit einer Änderung und damit mit einer kürzeren Lebensdauer von Sicherheitsmaßnahmen zu rechnen ist, wird eine Trennung von Umsetzungsstrategie und Sicherheitsmaßnahmen empfohlen.

Für spezifische Sicherheitsanforderungen ist die Erstellung von zugeschnittenen Sicherheitskonzepten notwendig, weil sich die abgeleiteten Schutzmaßnahmen von Fall zu Fall unterscheiden.

Sicherheitskonzepte werden in der Regel projekt-, bzw. entwicklungsbegleitend erstellt. Stellt sich heraus, dass bei bestehenden Anwendungen oder Systemen keine ausreichende Sicherheitskonzeption vorhanden ist, so ist diese nachträglich innerhalb einer mit dem Sicherheits-Team abgestimmten Übergangsfrist zu entwickeln und zu implementieren. Bei der Erstellung von Sicherheitskonzepten ist insbesondere auf den betriebswirtschaftlichen Aufwand zur Risikominimierung zu achten und das mögliche Restrisiko darzustellen.

2.5.2 Aufgabengebiete

Sicherheit ist in nahezu allen Bereichen des Unternehmens ein Aspekt, wobei der Fokus primär auf der Informationstechnologie liegt. Speziell hier kann entsprechend nur durch kontinuierliche Bearbeitung, Verbesserung und Anpassung eine angemessene IT-Sicherheit aufrechterhalten werden.

Neben den bereits definierten Aufgabengebieten sind im Folgenden als Ausblick wichtige Themen der Sicherheit genannt, die durch die Geschäftsführung, das Management, die Sicherheitsorganisation und die jeweils verantwortlichen Mitarbeiter entsprechend der ihnen übertragenen Verantwortung bearbeitet werden müssen:

- Plattform- und Netzwerksicherheit,
- Sicherheits-Reviews und Auditing,
- IT-Risikomanagement,
- Infrastruktursicherheit,
- Zugangs- und Zugriffskontrolle,
- Sicherheitsberatung,
- Betriebssicherheit,
- Sicherheitsbewusstsein des Personals,
- Sicherheitstechnologie und -grundlagen,
- Anwendungssicherheit.

In den Umsetzungsstrategien werden die Aufgabengebiete jeweils separat und detaillierter beschrieben.

2.5.3 Kontrolle

Nach dem Grundsatz der Nachvollziehbarkeit ist der Umgang mit sicherheitsrelevanten IT-Systemen und -Anwendungen so zu gestalten, dass Verstöße gegen dokumentierte und freigegebene Sicherheitsregelungen feststellbar und ihren Verursachern zuordenbar sind. Die durchgeführten Maßnahmen dienen ausschließlich der Aufrechterhaltung der Sicherheit sowie der Einhaltung der gesetzlichen und aufsichtsrechtlichen Vorgaben und der internen Regelungen. Ein Missbrauch für andere Zwecke, insbesondere hinsichtlich der systematischen Überwachung der Mitarbeiter, ist nicht erlaubt.

Nachweisliche Verstöße gegen Sicherheitsregelungen können je nach Schwere zu Disziplinar-, arbeits- wie auch zivilrechtlichen Maßnahmen oder strafrechtlicher Verfolgung führen. Die entsprechenden Maßnahmen regelt der Bereich Personal. Bei mitbestimmungsrelevanten Themen ist der Betriebsrat mit einzubinden.

Verstöße gegen die Sicherheitsregelungen basieren unter anderem auf:

- der Nichtbeachtung sowie Verletzung gesetzlicher Vorgaben,
- dem Nichtbeachten oder Verletzen von Sicherheitsvorschriften,

- der Manipulation oder Umgehung bestehender Sicherheitseinrichtungen,
- der vorsätzlichen Schädigung des Unternehmens durch Nichterfüllung von Sicherheitsmaßnahmen,
- der Schädigung der Sicherheit von Kunden, Geschäftspartnern und Mitarbeitern durch Nichterfüllung von Sicherheitsmaßnahmen,
- der unautorisierten Preisgabe von Geschäftsgeheimnissen und vertraulichen Interna,
- der unautorisierten Veränderung sicherheitsrelevanter IT-Anwendungen, -Systeme oder anderer Vorrichtungen,
- der Nutzung von IT-Anwendungen und -Systemen für unzulässige Zwecke,
- der Verletzung der Informationspflicht beim Auftreten sicherheitsrelevanter Vorfälle.

Management operationaler IT- und Prozess-Risiken

Methoden für eine Risikobewältigungsstrategie

Thies, K.H.W.

2008, XI, 148 S. 31 Abb., Hardcover

ISBN: 978-3-540-69006-1