IT-Risiko-Check: Das Wissen um geschäftskritische IT-Risiken

Joachim Stocker[1] · Sven Wenzel[2] · Jan Jürjens [3]

[1] Hochschule Albstadt - Sigmaringen
stocker@hs-albsig.de

[2] Fraunhofer-Institut für Software- und Systemtechnik ISST
Sven.Wenzel@isst.fraunhofer.de

[3] Fraunhofer-Institut für Software- und Systemtechnik ISST
und Technische Universität Dortmund
Jan.Juerjens@isst.fraunhofer.de

Zusammenfassung

Die Beantwortung der Frage, welche IT-Risiken nicht tolerierbar sind, beschäftigt die Unternehmen vor dem Hintergrund zahlreicher Angriffe aus dem Cyberspace aktuell in vielfacher Hinsicht. Insbesondere hochspezialisierte Unternehmen, deren Wettbewerbsvorteil auf der Geheimhaltung der Verfahren der Produktherstellung und -zusammensetzung beruht, suchen zu dieser Frage umsetzbare Lösungen. Der in diesem Papier vorgestellte, teilautomatisierte Ansatz leistet dazu einen Beitrag, indem geschäftskritische Risiken im Kontext der Informationssicherheit identifiziert, analysiert und bewertet werden. Unter Einbindung von Orientierungsmaßen und Entscheidungshilfen werden dazu verschiedene Phasen durchlaufen. In einem ersten Schritt werden jene Geschäftsprozesse bestimmt, deren Ausfall oder Störung als geschäftskritisch für die Erbringung vereinbarter Leistungen sowie der Geheimhaltung vertraulicher Informationen eingestuft werden. Die darin eingebundenen IT-/Informationsobjekte werden im nächsten Schritt auf Basis von Szenarien einer Schwachstellenanalyse unterzogen und entsprechend klassifiziert. Anschließend werden die Schwachstellen je Schadenszenario hinsichtlich ihrer Gefahrenlage bestimmt und bewertet. Die aus Gefährdung und Schwachstelle resultierenden, mit quantitativen Werten unterlegten Risiken werden im letzten Schritt bestimmt und in das unternehmensweite Risikomanagement überführt.

1 Motivation

Informationssicherheit motiviert sich im Kern ihrer Wichtigkeit für privatwirtschaftliche Unternehmen aus den nachfolgenden Aspekten. Einerseits muss die Sicherheit von Informationen als geschäftlicher Imperativ begriffen werden. Gelingt es nicht autorisierten Personen geschäftskritische Informationen zu entwenden, geht dies unumgänglich mit einer Schwächung der Wettbewerbsposition für das betroffene Unternehmen einher. Dies kann zu massiven Umsatzeinbrüchen führen, letztlich das Unternehmen in seiner Existenz bedrohen. Der Schutz

P. Schartner · N.N (Hrsg.) · DACH Security YYYY · syssec (YYYY) pp-pp.

sämtlicher geschäftskritischer Informationen und damit die Absicherung der virtuellen und physischen IT-Infrastrukturen liegen im originären Interesse der Organisation.

Andererseits ist das Risikomanagement im Kontext der Informationssicherheit mit haftungsrelevanten Aspekten der Leitungsebene in Unternehmen verbunden [WePM08, S. 14]. Das im Jahre 1998 in Kraft getretene Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) besitzt in diesem Kontext besondere Bedeutung. Es manifestiert verschiedene Änderungen im Aktiengesetz (AktG) und hat ebenfalls Ausstrahlungswirkung in die handelsrechtlichen Vorschriften. Konkret wird der Vorstand von Aktiengesellschaften zur Einrichtung eines „Frühwarnsystems“ verpflichtet. Der Annahme, das KonTraG finde nur Anwendung für börsennotierte Unternehmen, wird durch die entsprechenden Paragrafen im 2. Abschnitt des 3. Buches des Handelsgesetzbuch (HGB) widerlegt. Dieser Abschnitt schließt Kapitalgesellschaften, Gesellschaften mit beschränkter Haftung (GmbH) sowie Personengesellschaften, bei denen persönlich haftende Gesellschafter keine natürlichen Personen sind, in den erweiterten Anwendungsumfang mit ein [KeRS13, S. 2].

Trotz der genannten Relevanz wird das breite Themenspektrum der Informationssicherheit insbesondere in mittelständischen Unternehmen häufig stiefmütterlich behandelt (vgl. dazu [Pric14, S. 8], [Teut10, S. 78]). Fehlendes Wissen und knappe Ressourcen veranlassen Entscheidungsträger oftmals dazu, auf ihr „Bauchgefühl“ zu vertrauen oder notwendige Schritte schlicht zu unterlassen [Teut10, S. 87].

2 Zielsetzung

Vor diesem Hintergrund haben wir eine zu Teilen werkzeuggestützte Systematik entwickelt, um Transparenz für geschäftskritische IT-Risiken zu schaffen. Sie fokussiert auf Kernrisiken in der Informationssicherheit und basiert auf Erfahrungswerten, die im Rahmen von mehrjährigen Beratungs- und Forschungstätigkeiten gesammelt wurden. Insbesondere zielt der beschriebene Ansatz darauf ab,

- dem Prinzip der Wesentlichkeit zu folgen, so dass alle im Sinne der Geschäftskritikalität wesentlichen IT-Risiken bestimmt, analysiert, bewertet und damit einem Vergleich unterzogen werden können;
- den Zusammenhang zwischen geschäftskritischen Prozessen und damit verbundenen IT-Risiken zu verdeutlichen;
- Unternehmen mit wenig Erfahrung im IT-Risikomanagement einen Einstieg zu geben;
- für die Zielgruppe großer mittelständischer Unternehmen konzipiert zu sein; und
- offen für inhaltliche Vertiefungen und Erweiterungen zu sein.

3 Grundlagen

3.1 Informationssicherheit

Informationssicherheit wird im Kontext dieser Ausarbeitung als der Schutz sämtlicher physischer, virtueller als auch geistiger Informationen verstanden. Bewusst wurde nicht der Begriff „IT-Sicherheit“ gewählt, da sich dieser hauptsächlich auf den Einsatz der Informationstechnik bezieht (siehe dazu auch [Bund01]). Er schließt beispielsweise die nicht-elektronische Form

von Informationen (z. B. physisch vorliegende Dokumente) aus und grenzt somit die Wertobjekte der Informationssicherheit auf die Objekte in der Informationstechnik ein [Koen13, S. 151].

3.2 IT-Risiko

In Literatur und Praxis existieren unterschiedliche Begriffe, wie IT-Risiko, Informations-Risiko, Informationssicherheits-Risiko, IT-Sicherheitsrisiko, die je nach Anwendungsbezug auch synonym verwendet werden (vgl. dazu [Koen13, S. 151f.], [Muel11, S. 116], [Iso/11b, S. 9]). Allgemein gefasst wird unter dem sicherheitsorientierten Risikobegriff ein Ereignis verstanden, das bei Eintritt eine negative Auswirkung auf die Ziele der Geschäftstätigkeit haben kann. Ein IT-Risiko stellt dabei die Möglichkeit dar, dass eine Bedrohung die Schwachstelle eines oder mehrerer schutzbedürftiger IT-/Informationsobjekte (Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze) ausnutzt, sodass in der Folge Schaden für die Unternehmung entsteht. Der vorliegenden Ausarbeitung liegt dieses Begriffsverständnis für IT-Risiken zugrunde.

4 Methodik

4.1 Bedarf und bestehende Ansätze

Diese Ausarbeitung geht der Frage nach, wie die Erhebung, Analyse und Bewertung von Risiken im Kontext der Informationssicherheit bei typischerweise gegebenen Ressourcenrestriktionen in mittelständischen Unternehmen ausgestaltet werden kann. Erfahrungswerte zeigen, dass die Inhalte der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf der einen Seite zu komplex für mittelständische Organisationen sind. Andererseits ist ein Standard wie ISO/IEC 27005 ([Iso/11a]) zu abstrakt und es mangelt an konkreten Handlungsanweisungen und Umsetzungshilfen, die angemessen für diese Zielgruppe sind.

Es existieren Ansätze, die in ihrer Lösung mitunter auf die Ressourcenrestriktionen kleiner und mittlerer Unternehmen eingehen (vgl. hierzu beispielsweise [CSYW07], [Pelt05]). Jedoch ist auch hier zu konstatieren, dass diese als abstrakter Leitfaden ohne Konkretisierung anzusehen oder in ihrem Umfang nicht auf die Bedürfnisse der Zielgruppe passend sind.

4.2 Zielsetzung

Die beschriebene Lücke wird durch den von uns entwickelten Good-Practice Ansatz geschlossen, der verschiedene Vorteile bestehender Ansätze kombiniert und wo notwendig ergänzt. Für die Zielgruppe wird eine ressourcenadäquate und belastbare Vorgehensweise mit Orientierungsmaßstäben und konkreten Entscheidungshilfen aufgezeigt. Tiefgreifende und langjährige Erfahrungen aus der Beratungs- und Forschungspraxis sind die Grundlage für den hier entwickelten zielgruppenorientierten Ansatz.

Grundsätzlich basiert der vorgeschlagene Ansatz auf dem Kriterium der Kritikalität. Er besitzt nicht den Anspruch sämtliche Risiken im Kontext der Informationssicherheit zu identifizieren. Sein Anspruch ist es, mit moderatem Aufwand die für den Geschäftserfolg entscheidenden Risiken in der Informationssicherheit zu adressieren. Hierzu werden einerseits Geschäftsprozesse bestimmt, die als geschäftskritisch im Sinne der operativen Leistungserbringung anzusehen

sind. Andererseits werden Geschäftsprozesse identifiziert, die Einsicht auf geschäftskritische Informationen ermöglichen. Diese Auswahl basiert auf den Erfolgsfaktoren vieler mittelständischer Unternehmen: die kundenspezifische Bereitstellung schwer zu kopierender Produkten und Dienstleistungen in der vereinbarten Quantität, Qualität und Zeit sowie der Geheimhaltung des Wissens über die Verfahren zur Produktherstellung und -zusammensetzung. Anzumerken ist, dass Geschäftsprozesse, die als „unkritisch“ im genannten Sinne einzustufen sind, ihre Wichtigkeit nicht verlieren, jedoch eine geringere Priorität für die genannte Zielsetzung besitzen.

In dieser Ausarbeitung wird von der Annahme ausgegangen, dass wenig Erfahrung im Umgang mit Informationssicherheit besteht. In diesem Maturitätsstadium sind Beurteilungen der Entscheidungsträger zu Eintrittswahrscheinlichkeiten und Schadenshöhen von Risiken erfahrungsgemäß eher qualitativ als quantitativ zu leisten (vgl. dazu auch [Bund02, S. 28]), weshalb auch externe Sachverständige in den Prozess einzubeziehen sind. Umso wichtiger ist es in dieser Phase die Akzeptanz in der Organisation zu gewinnen. Ein entscheidender Aspekt ist dabei, die Ergebnisse der Schritte im Rahmen des Managements von IT-Risiken in das unternehmensweite Risikomanagement zu integrieren [PaMK12, S. 130]. Demzufolge ist als Ausgangs- und Endpunkt der Bestimmung von geschäftskritischen IT-Risiken das unternehmensweite Risikomanagement unabdingbar.

4.3 Vorgehensweise und Inhalt

Im Folgenden wird eine qualitative Methode, gestützt durch quantitative Orientierungspunkte und Entscheidungsunterstützungsmodelle, aufgezeigt, deren Ausgangspunkt das unternehmensweite Risikomanagement ist (siehe hierzu auch die überblickhafte Darstellung der Vorgehensweise in Abbildung 4 sowie die Abbildung 1).

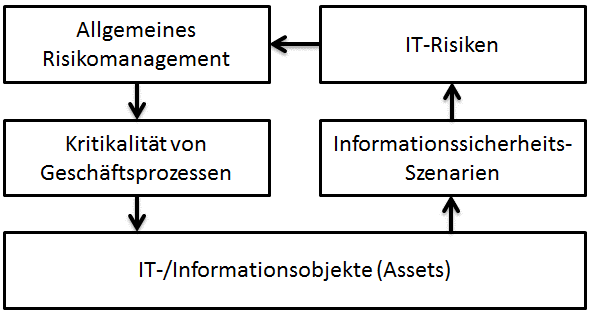

Abb. 1: Einbindung von IT-Risiken in das allgemeine Risikomanagement

(1) Das Fundament für die Methodik bildet die Festlegung des Geltungsbereiches (sog. „Scope“) [Hari12, S. 292], d.h. der Ausschnitt innerhalb des Unternehmens, in welchem geschäftskritische IT-Risiken vorkommen können. Der Ansatz des BSI (vgl. dazu [Bund03]) schließt dabei alle Geschäftsprozesse in den Umfang der Prüfung ein. Für unsere Zielgruppe ist dieser Umfang nicht realisierbar, da einerseits der Ressourcenaufwand für eine gesamtheitliche Prüfung nicht darstellbar ist. Andererseits ist die dafür notwendige Dokumentation aller Geschäftsprozesse in dieser Zielgruppe eher unwahrscheinlich. Darüber hinaus gibt es viele Prozesse, die stunden- oder sogar tagelang teilweise oder komplett ausfallen können ohne der Unternehmung essentiell zu schaden. Andere Ansätze grenzen die Prüfung auf bestimmte Unter-

nehmensbereiche (z. B. Forschung und Entwicklung) ein. Diese Eingrenzung läuft Gefahr wesentliche IT-Risiken, die nicht dediziert Geschäfts- oder Fachbereichen zugeordnet werden können, auszuklammern.

Im ersten Schritt wird die Bestimmung der geschäftskritischen Prozesse vorgenommen. Dafür existieren bestenfalls dokumentierte Prozessübersichten, alternativ wird das Wissen der Verantwortlichen um die Abläufe im Unternehmen herangezogen. Das erste Ziel ist, alle Geschäftsprozesse zu identifizieren, deren Ausfall oder Störung als geschäftskritisch angesehen werden müssen. Konkret formuliert gilt jeder Geschäftsprozess als kritisch, dessen Zeitspanne zwischen Ausfall oder Störung und geregeltem Wiederanlauf für die Unternehmung zu einer nicht tolerierbaren Unterbrechung des operativen Geschäftsbetriebes führt. Diese Anforderung muss vom Unternehmen selbst operationalisiert werden, d.h. welche Zeitspanne als tolerabel bzw. nicht tolerabel erachtet wird. Im produzierenden Gewerbe stehen dabei operativ-leistungserbringende Prozesse, die einen Output für Kunden generieren, im Fokus. Ein entscheidender Faktor ist dabei das Logistik- und Produktionsprinzip. Von diesem wird die Zeitspanne im Wesentlichen bestimmt. Werden beispielsweise Einzelstücke gefertigt, die bedarfssynchron angeliefert werden, so ist die Zeitspanne dabei vergleichsweise kurz.

Für die Bestimmung der kritischen Geschäftsprozesse eignet sich ein Workshop, der mit den Bereichs- und Geschäftsprozessverantwortlichen abzuhalten ist. Letztere sind wichtig, da in dieser Phase gute Kenntnisse über die Geschäftsprozesse gefragt sind. Jeder Teilnehmer hat im Vorgang zum Workshop die Geschäftsprozesse, die er als kritisch erachtet, zu identifizieren. Innerhalb des Workshops werden diese dann zur Diskussion gestellt, ausreichend skizziert und abschließend von der Gruppe hinsichtlich ihrer Geschäftskritikalität bewertet. Die Granularität der Geschäftsprozesse sollte dabei den Mittelweg zwischen einer zu detaillierten Betrachtung und einer zu starken Komprimierung finden. Die Anwendung einer anerkannten Notation für die Visualisierung der Prozesse ist in diesem Stadium nicht zwingend erforderlich. Um die Diskussion auf einer gemeinsamen Abstraktionsebene anzusetzen, ist jedoch eine beispielhafte Darstellung der Visualisierung und Granularität für die Geschäftsprozesserhebung im Vorgang zum Workshop bereitzustellen. Dabei sind In- und Output, vor- und nachgelagerte Prozesse sowie die Abhängigkeiten zu unterstützenden Prozessen in einer Prozesslandkarte darzustellen (siehe hierzu auch die beispielgebende Abbildung 2). Die Auflistung der vor- und nachgelagerten Prozesse hat die Wertkette innerhalb des Unternehmens abzubilden. So wird sichergestellt, dass die Verortung der Diskussion und die Abhängigkeiten zwischen Geschäftsprozessen für alle Teilnehmer verständlich sind. Die Erfassung der unterstützenden Prozesse ist ebenfalls wichtig, da diese für die Aufrechterhaltung der Kernprozesse von vitalem Interesse sein können. Erfahrungswerte zeigen, dass in einem ersten Schritt die Bestimmung von maximal 15 Prozessen nicht zu überschreiten ist.

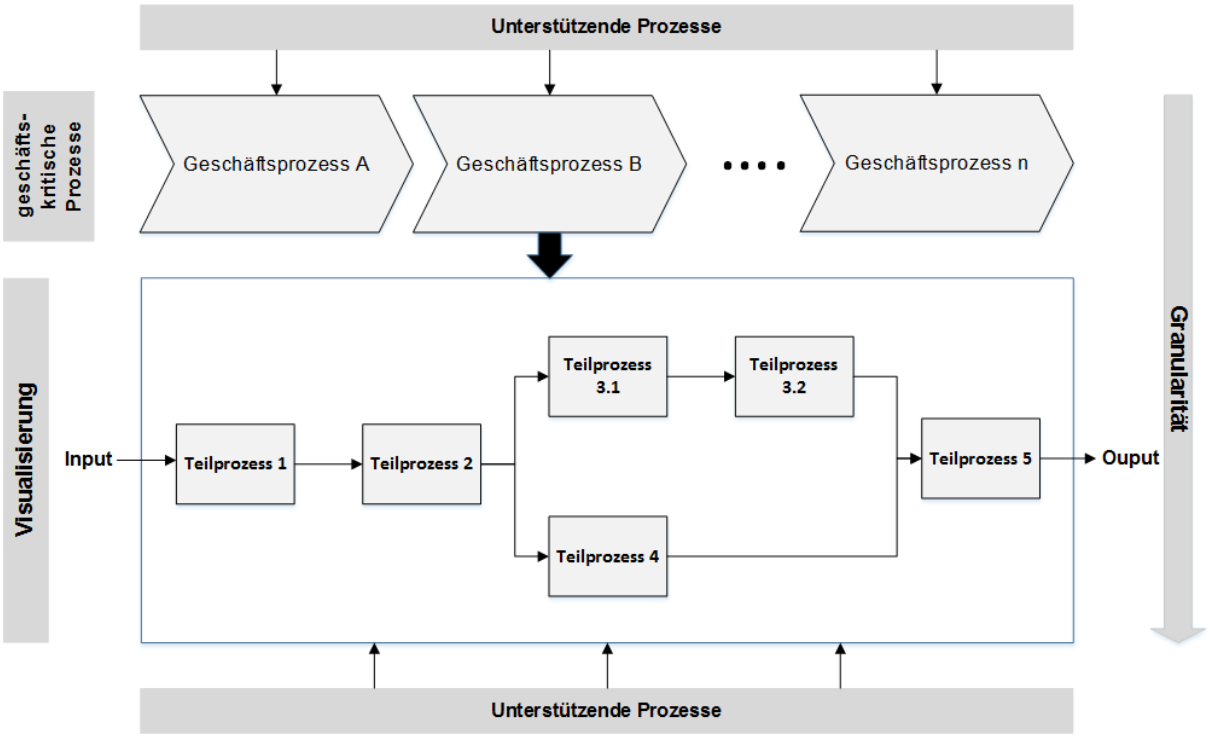

Abb. 2: Visualisierung und Granularität der Geschäftsprozesserhebung

Weiterhin sind Geschäftsprozesse zu identifizieren, die Einsicht auf geschäftskritische Informationen ermöglichen. Als geschäftskritische Informationen sind alle virtuell und physisch vorliegenden Informationen zu werten, deren Verlust, Beschädigung oder nicht-autorisierter Besitz zu Wettbewerbsnachteilen für das betroffene Unternehmen führen. Konkret bedeutet dies, die Auffindung der in der Geschäftsprozessdurchführung verarbeiteten Daten, die vertrauliche Informationen (z. B. Herstellungsverfahren) enthalten.

Physisch vorliegende Informationen sind vergleichsweise leicht identifizierbar. Sie befinden sich oftmals in einem Dokumentenablagesystem, dessen Ort von den Verantwortlichen benannt werden kann. In den meisten Fällen sind streng vertrauliche Dokumente bereits klassifiziert und ihrer Vertraulichkeitsstufe entsprechend abgelegt. Die Erhebung der vertraulichen Dokumente wird mittels strukturierter Befragung der Archiv- und Dokumentationsverantwortlichen durchgeführt.

Um geschäftskritische Informationen aufzufinden, die in IT-gestützten Geschäftsprozessen verarbeitet werden, wird eine Analyse der Geschäftsprozessbeschreibungen vorgenommen. Hierzu werden die Prozessbeschreibungen mit unserem Werkzeug RiskFinder analysiert. Der RiskFinder extrahiert die Texte und gleicht sie systematisch mit einer Ontologie ab, die geschäftskritische Informationen geeignet klassifiziert. Das Analyseverfahren haben wir bereits in [PHJB11, HWP14] eingeführt. Hier wird es mittels dedizierter Ontologien für verschiedene Unternehmensbereiche oder Branchen zur Klassifikation der verarbeiteten Informationen eingesetzt. Eine Anpassung der abgestimmten Suchanforderungen (z. B. Ausweitung oder Eingrenzung) ist ebenfalls jederzeit durch Verändern der Ontologie möglich und bedarf keiner zusätzlichen Ressourcenbelastung. Im Anschluss ist das Ergebnis von den Verantwortlichen in Plenum zu

verifizieren. Insgesamt bietet dieser Automatisierungsschritt den Vorteil der Zeitersparnis, reduziert Auslassungen, die oftmals auf Basis des ausschnittweisen Wissens der Verantwortlichen basieren, und bietet eine belastbare Basis für eine effiziente Verifizierung der Ergebnisse.

(2) In einem zweiten Schritt sind zuerst die IT-/Informationsobjekte zu bestimmen und in Verbindung zu setzen, die für die Funktionsfähigkeit der geschäftskritischen Prozesse relevant sind. Anschließend ist deren Schadensausmaß als Ergebnis der Verletzung von Vertraulichkeit, Integrität und Verfügbarkeit darzustellen.

Zuerst sind IT-Systeme und die damit in direktem Zusammenhang stehenden Anwendungen zu identifizieren. Viele Unternehmen pflegen dazu Datenbanken, in welchen das IT-Inventar gelistet ist. Jedoch kann bei wenig Erfahrung in diesem Bereich nicht davon ausgegangen werden, dass derartige Übersichten vollumfänglich existieren. Um einen Überblick der vorhandenen IT-Systeme zeit- und ressourcensparend zu generieren, können IT-Inventare mittels entsprechender Scansoftware (nmap, OpenVAS, PS-Tools, Secunia CSI, …) automatisiert erzeugt werden. Hiermit lässt sich neben den Systemen auch die darauf installierte Software erfassen. Die manuelle Prüfung im Anschluss stellt durch Plausibilitätsprüfungen sicher, dass alle im Netzverbund befindlichen IT-Systeme und Softwarekomponenten einschließlich deren Version gelistet sind, die einen Beitrag für die Funktionsfähigkeit der geschäftskritischen Prozesse leisten. Da sich der Netzverbund aus meist vielen Einzelobjekten zusammensetzt, können ähnliche Objekte, die gleichen Gefährdungen ausgesetzt sind, zu Gruppen zusammengefasst werden (z. B. konfigurationsgleiche Client-Rechner). Anschließend sind pro IT-System die damit zusammenhängenden Anwendungen und Informationen festzulegen. Dies garantiert eine eindeutige Zuweisung der Informationen und Anwendungen zu IT-Systemen.

Um die dabei vorzufindende Komplexität zu meistern, ist eine Sitzung der im Fachbereich arbeitenden Mitarbeiter und Prozessmanager, der Verantwortlichen für die Anwendungen sowie der betreuenden IT-Mitarbeiter für Administration und Sicherheit einzuberufen. Als Grundlage für diesen Workshop sowie notwendiger Bestandteil der Informationssicherheit ist eine Klassifizierungsmatrix zu erstellen, die die Einstufung möglicher Schäden im Hinblick auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit abstrakt beschreibt (siehe hierzu auch Tabelle 1). In einem fortgeschrittenen Maturitätsstadium können weitere Schutzzeile (z.B. Authentizität, Nichtabstreitbarkeit) ebenfalls in die Betrachtung integriert werden. Die Einstufung basiert dabei auf einer Ordinalskala, wobei für die quantifizierbare Bewertung numerische und monetäre Werte (gemessen in lokaler Währung, z. B. Euro) anzusetzen sind. Die monetären Werte sind als Ergebnis der Verletzung von Vertraulichkeit, Verfügbarkeit und Integrität von IT-/Informationsobjekten zu verstehen. Sie stellen Orientierungsbreiten für die Erfassung des „direkten“ finanziellen Aufwands (personelle und technische Ressourcen für die Behebung des Schadens) sowie des „indirekten“ finanziellen Aufwands (Folgekosten aus der Verletzung von Integrität, Vertraulichkeit und Verfügbarkeit) dar. Der Maßstab für die Einschätzung der monetären Schadensauswirkung ist grundsätzlich individuell festlegbar. Erfahrungsgemäß empfiehlt sich die Anlehnung an eine sondereffektfreie, durchschnittliche betriebliche Größe vergangener Perioden. Beispielhaft ist das Betriebsergebnis der letzten 5 Jahre als Extremwert (Wert „d“ in der Tabelle 1) zu nennen. Tritt ein derartiger Schaden ein, steht das Unternehmen vor einer existenzgefährdenden Situation. Die Abkürzung GE steht in Tabelle 1 für Geldeinheiten und repräsentiert die lokale Währung.

Tab. 1: Klassifizierungsmatrix

Schadensstufe (ordinal)	Wert (kardinal)	Schaden* (monetär)	Vertraulichkeit	Integrität	Verfügbarkeit
niedriger Schaden	1	<= a (GE)	Deskriptiver Klassifizierungsbereich: Festlegung und Beschreibung der Kriterien Vertraulichkeit, Integrität und Verfügbarkeit für die jeweilige Schadenseinstufung		
mittlerer Schaden	2	> a (GE); <= b (GE)			
hoher Schaden	3	> b (GE); <= c (GE)			
sehr hoher Schaden	4	> c (GE); <= d (GE)			

* = gemessen an einer betrieblichen Größe (z. B. durchschnittlicher Umsatz oder Betriebsergebnis der letzten x Jahre)

Mittels der vorgenommenen Zuweisung von Anwendungen und Informationen zu IT-Systemen können im Rahmen eines Workshops realitätsgetreue Schadenszenarien beschrieben werden (siehe dazu auch Abbildung 3). Das Zusammenspiel von Mitarbeitern, als Benutzer der Anwendungen, und den Verantwortlichen leistet erfahrungsgemäß eine belastbare Vorstellung darüber, welche Schäden in den einzelnen Szenarien entstehen können. Pro Schadenszenario ist die Bewertung anhand der Klassifizierungsmatrix, d. h. auf Basis der Verletzung der Kriterien Vertraulichkeit, Integrität und Verfügbarkeit vorzunehmen. In Summe ergeben diese den anzusetzenden Schadenswert pro Schadenszenario.

		Geschäftsprozess B			Bewertung
IT-/Informations-objekt	**Beschreibung Schadenszenario**	*Vertraulichkeit*	*Integrität*	*Verfügbarkeit*	*Summe aus…*
IT-System A	Schadenszenario X	Bewertung der Verletzung von Vertraulichkeit, Integrität und Verfügbarkeit (V/I/V) des Schadenszenario X anhand Schadensstufen (1-4)			V/I/V
Anwendung A					
Anwendung B					
IT-System B	Schadenszenario Y	Bewertung der Verletzung von Vertraulichkeit, Integrität und Verfügbarkeit (V/I/V) des Schadenszenario Y anhand Schadensstufen (1-4)			V/I/V
Anwendung C					
Anwendung D					

Abb. 3: Bewertung von Schadenszenarien

Im Ergebnis wird eine Liste geführt, die die IT-Systeme sowie die damit in Verbindung stehenden Anwendungen und Informationen zu Schadenszenarien zusammenführt und diese bewertet.

(3) Für die Bestimmung der Schadenswerte wie auch der Eintrittswahrscheinlichkeiten ist die Erhebung der Komponenten im Netzwerk in Form eines Netzplanes hilfreich. Im Netzplan sind die eingesetzten Informations- und Kommunikationskomponenten der geschäftskritischen Prozesse und deren Vernetzung graphisch im Überblick dargestellt. Zumeist sind Netzpläne mindestens in rudimentärer Form in Unternehmen elektronisch abgelegt und können bedarfsbezogen vervollständigt oder ausgebaut werden. Im Zuge der Gefährdungsanalyse sind Kommuni-

kationswege zu kennzeichnen die Außenverbindungen darstellen, d. h. ins Internet oder öffentlich zugängliche Netze führen. Weiterhin sind Kommunikationsverbindungen hervorzuheben, über die hoch sensible Daten im Sinne der definierten Geschäftskritikalität übertragen werden und ebenfalls jene, die für diesen Zweck auszuschließen sind. Neben diesen als kritisch eingestuften Pfaden im Netzwerk sind die IT-Komponenten und deren Abhängigkeiten zu veranschaulichen. Kenntnisse über Abhängigkeiten der IT-Komponenten im Netzwerk besitzen eine hohe Wichtigkeit, da aus ihnen Wissen zu sog. „Single Point of Failures“ hervorgehen kann. Ist für die störungsfreie Durchführung eines Geschäftsprozesses eine Anwendung notwendig, die Zugriff auf eine bestimmte Datenbank benötigt, so ist zu prüfen, ob diese Datenbank ein „Single Point of Failure“ darstellt. Abhängigkeit bedeutet in diesem Sinne, dass sämtliche IT-/Informationsobjekte für die störungsfreie Durchführung geschäftskritischer Prozessen bekannt sein müssen.

Im Anschluss an die Analyse der Schadenszenarien ist die Wahrscheinlichkeit des Eintritts einer Gefährdung festzulegen. Die Gefährdung ist somit der Wahrscheinlichkeitswert einer Bedrohung bei Eintritt und setzt eine notwendige Anfälligkeit eines IT-/Informationsobjektes (Schwachstelle) voraus. Die Betonung der Notwendigkeit ist an dieser Stelle ausschlaggebend, da eine Bedrohung erst dann Schaden verursachen kann, wenn eine Schwachstelle für diese existiert [KeRS13, S. 127]. Die Schwachstellen der in Schritt 2 modellierten IT-/Informationsobjekte können automatisiert bestimmt werden. Hierzu gleicht unser Analysewerkzeug die Inventarlisten, welche die auf den Systemen installierte Software samt Versionen und z. T. Konfigurationen beschreiben, mit bestehenden Schwachstellendatenbanken (z. B. der National Vulnerability Database, NVD) und geeigneten Risikokatalogen ab. Die Datenbanken und Kataloge beschreiben Schwachstellen für gängige Software und erlauben eine Abschätzung der technischen Folgen von entsprechenden Exploits. Anschließend sind die Wahrscheinlichkeits- und Anfälligkeitswerte gemeinsam mit den IT-Sicherheitsfachkräften sowie ggf. vertrauten, externen Sachverständigen zur Diskussion zu stellen und einer Bewertung zu unterziehen. Die Einbindung externer IT-Sicherheitsexperten bringt den Vorteil, das oftmals fehlende umfassende Wissen in die Diskussion einfließen zu lassen und mögliche Angriffspfade aus Erfahrungswerten effektiv bestimmen zu können. Als Orientierungshilfe für die systematische Bestimmung der Wahrscheinlichkeiten ist es empfehlenswert Bewertungstabellen wie Tabelle 2 (Auszug) in den Gesprächen zu nutzen.

Im Ergebnis sind die Wahrscheinlichkeiten der Gefährdungen, die auf geschäftskritische Prozesse und deren IT-/Informationsobjekte einwirken können, bestimmt.

Tab. 2: Wahrscheinlichkeitswerte von Gefährdungen (Auszug)

Wahrscheinlichkeit einer Bedrohung	gering				mittel				...	sehr hoch
Anfälligkeit des Objekts für Bedrohung	gering	mittel	hoch	sehr hoch	gering	mittel	hoch	sehr hoch	...	sehr hoch
Wert	1	2	3	4	2	3	4	5	...	7
Wahrscheinlichkeits-spanne des Eintritts einer Gefährdung	0 - 0.14	0.14 - 0.28	0.28 - 0.42	0.42 - 0.57	0.14 - 0.28	0.28 - 0.42	0.42 - 0.57	0.57 - 0.71	...	0.86 - 1

(4) Der letzte Schritt führt die Ergebnisse aus den Schritten (2) und (3) zusammen. Die IT-Risiken werden aus der Wahrscheinlichkeit des Eintritts einer Bedrohung (Gefährdung) und dem möglichen Schadensmaß bestimmt. Sie können im Anschluss in qualitativer oder quantitativer Ausprägung in das unternehmensweite Risikomanagement überführt werden. Erfahrungswerte zeigen, dass IT-Risiken in einer separaten Risikokategorie zu führen sind. Dies bringt deren stark verwobenen technischen und organisatorischen Eigenschaften mit sich, was sie letztlich wesentlich von weiteren Risikoarten (z. B. Marktrisiken, Finanzrisiken) unterscheidet und nach einer eigenständigen Steuerung verlangt.

5 Fazit

Der Nutzen dieser Methodik liegt in der systematischen, mit moderatem Aufwand erzielbaren und durch Entscheidungsmodelle gestützten Herleitung von IT-Risiken, die als geschäftskritisch einzustufen sind. Diese können qualitativ, z. B. auf Basis von Ordinalskalen bewertet werden, oder mittels Anwendung mathematischer Umrechnungsprinzipien quantitativ ihren Ausdruck finden. Letzteres ist insbesondere relevant, wenn es um die Harmonisierung der Bewirtschaftung von IT-Risiken mit weiteren Risikoarten des unternehmensweiten Risikomanagements geht. Letztlich führt der Ansatz durch seine schrittweise Konkretisierung zu Verständnis und Akzeptanz im Umgang mit IT-Risiken und stellt die Grundlage für ein angemessenes Informationssicherheitsmanagement dar, vor allem für Organisationen mit knapper Ressourcenausstattung und wenig Erfahrung in der Informationssicherheit.

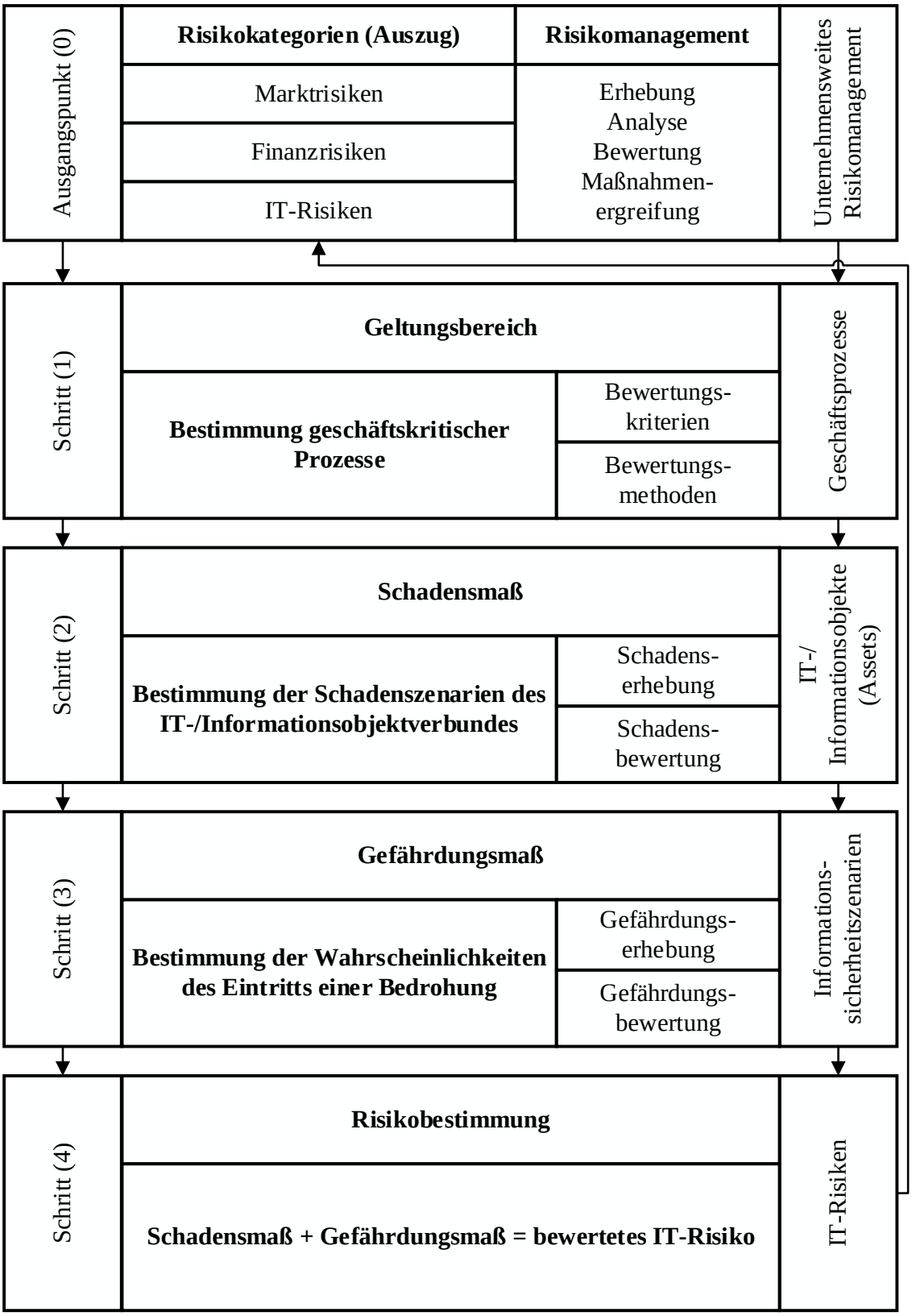

Abb. 4: Bestimmung geschäftskritischer IT-Risiken

Literatur

[Bund01] Bundesamt für Sicherheit in der Informationstechnik: Glossar und Begriffsdefinitionen, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (Zugriff 2015-03-10, 20:00 MEZ).

[Bund02] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (Zugriff 2015-03-10; 14:00 MEZ).

[Bund03] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4: IT-Grundschutz-Vorgehensweise, Version 2.0, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (Zugriff 2015-03-10; 14:00 MEZ).

[CSYW07] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (No. CMU/SEI-2007-TR-012), Carnegie-Mellon University, Software Engineering Institute, Pittsburgh (2007).

[Hari12] T. W. Harich: IT-Sicherheitsmanagement: Arbeitsplatz IT Security Manager, mitp (2012).

[HWP14] T. Humberg, C. Wessel, D. Poggenpohl, S. Wenzel, T. Ruhroth, J. Jürjens: Using Ontologies to Analyze Compliance Requirements of Cloud-Based Processes. In: Cloud Computing and Services Science (selected best papers), Springer, Communications in Computer and Information Science, vol. 453, pp. 1-16, 2014.

[Iso/11a] ISO/IEC 27005:2011: Information technology - Security techniques - Information security risk management.

[Iso/11b] ISO/IEC 27000:2009: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie.

[KeRS13] H. Kersten, J. Reuter, K.-W. Schröder: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung, Springer Vieweg (2013).

[Koen13] H.-P. Königs: IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits- und IT-Risiken, Springer Vieweg (2013).

[Muel11] K.-R. Müller: IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sicherheitspyramide - Standards und Practices - SOA und Softwareentwicklung, Vieweg+Teubner (2011).

[PaMK12] S. B. Paquet, C. Müller, B. Kühle: Effizienzgewinne durch vollständige Integration der IT-Governance in die Corporate Governance am Beispiel des IT-Risikomanagement. In: P. Ratzer, U. Probst (Hrsg.): IT-Governance, UVK Verlagsgesellschaft GmbH (2012), S. 123 - 137.

[Pelt05] T. R. Peltier: Information security risk analysis, Taylor & Francis Group (2005).

[PHJB11] M. Peschke, M. Hirsch, J. Jürjens, S. Braun: Werkzeuggestützte Identifikation von IT-Sicherheitsrisiken. In: D-A-CH Security 2011, Oldenburg, 2011. Gemeinsame Arbeitskonferenz der GI, OCG, BITKOM, SI, TeleTrusT.

[Pric14] PricewaterhouseCoopers Aktiengesellschaft Wirtschaftsprüfungsgesellschaft: Wie steht es um die Informationssicherheit im deutschen Mittelstand?, ohne Verlag (2014).

[Teut10] F. Teuteberg: IT-Risikomanagement - Eine Studie zum Status quo in deutschen Unternehmen. In: F. Keuper, F. Neumann (Hrsg.): Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien, Gabler (2010), S. 69 - 89.

[WePM08] W. Wellhöfer, M. Peltzer, W. Müller: Die Haftung von Vorstand Aufsichtsrat Wirtschaftsprüfer mit GmbH-Geschäftsführer, Beck (2008).