Management and Information Technology Solutions

Decker Consulting GmbH

Informationssicherheit – ohne methodische Risikoidentifizierung ist alles Nichts

Karsten M. Decker

Decker Consulting GmbH

Birkenstrasse 49

CH-6343 Rotkreuz

Revision 1.3

27.09.2017

öffentlich

Dieser Artikel ist eine erweiterte Version des Artikels

Informationssicherheit - ohne methodische Risikoidentifizierung ist alles Nichts

der im Springer Journal HMD Praxis der Wirtschaftsinformatik, 54(1), 21-36, 2017;

DOI 10.1365/s40702-017-0288-3 publiziert wurde.

Inhaltsverzeichnis

Zusammenfassung

Informationssicherheit ist kein IT-Problem und kann nicht auf die IT-Abteilung reduziert werden. Eine wirksame Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit muss in der ganzen Organisation verankert werden. Um dieser Herausforderung effizient zu begegnen, ist ein risikobasiertes Vorgehen erforderlich. Dazu muss zunächst der organisatorische Kontext bestimmt werden. Bei der Durchführung des Risikomanagementprozesses ist die Qualität der Risikoidentizfierung ausschlaggebend. Risiken, die hier nicht identifiziert werden, fehlen in der nachfolgenden Risikoanalyse und -bewertung und somit auch bei der Risikohehandlung. Für die methodische Risikoidentifizierung existieren verschiedene Ansätze, von denen zwei vorgestellt werden: der vorwiegend wirkungsorientierte Ereignis-basierte Ansatz und der ursachenorientierte auf Werten, Bedrohungen und Schwachstellen basierte Ansatz. Damit die Umsetzung der Risikoidentifizierung in der Praxis gelingt, müssen verschiedene Voraussetzungen erfüllt sein. Ausschlaggebend ist, dass die oberste Leitung ihre Führungsrolle umfassend und wirksam wahrnimmt. Die zentrale Herausforderung ist, den Umfang der Risikoidentifizierung handhabbar zu halten. Dazu haben sich in der Praxis die Vorgehensweisen der Fokussierung und Vergröberung bewährt. Unabhängig vom gewählten Ansatz zur Risikoidentifizierung ist auf jeden Fall ein fundiertes Beurteilungsvermögen unerlässlich. Mittels des Prozesses der fortlaufenden Verbesserung kann schliesslich ein anfänglich grobes, aber eindeutiges Bild der Informationssicherheitsrisiken Schritt für Schritt verfeinert und den aktuellen Anforderungen und Bedrohungen angepasst werden.

1 Einleitung

Es ist unbestritten, dass eine angemessene und wirksame Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information über Geschäftsprozesse, Unterstützungsprozesse, Beschäftigte, Kunden, Lieferanten, etc. für alle Organisationen von grosser Bedeutung ist. Dabei ist es unerheblich, in welcher Form die Information vorliegt oder greifbar wird: Sie kann auf Papier gedruckt oder geschrieben, elektronisch gespeichert, per Post oder E-Mail versandt, mit elektronischen Mitteln übertragen, auf Photos, in Videos oder Filmen gezeigt, in Besprechungen, am Telefon oder in der Öffentlichkeit gesprochen oder mittels eines Fotokopierers oder Faxgeräts verarbeitet oder übermittelt werden.

Gelangt Information in unbefugte Hände, kann dies sehr weitreichende Folgen für die Geschäftstätigkeit haben, wie etwa Reputationsschäden, Verlust von Wettbewerbsvorteilen, Verlust der Technologieführerschaft, Klagen und Strafen, die Verletzung vertraglicher Verpflichtungen in Service-Level Vereinbarungen, etc. - bis hin zur vollständigen Aufgabe der Geschäftstätigkeit.

Es stellt sich somit die Frage, wie Information am besten angemessen und wirksam geschützt werden kann. Dazu muss zunächst festgehalten werden, dass es sich hier nicht um ein IT-Problem handelt und schon gar nicht um eine Angelegenheit, die auf die IT-Abteilung beschränkt werden kann, weil so die Verantwortlichen für Geschäftsprozesse und Unterstützungsprozesse sowie die Risikoeigentümer aus den Überlegungen komplett ausgeblendet würden. Die Informationssicherheitsrisiken, denen die Organisation ausgesetzt ist, müssen also organisationsweit umfassend und ausreichend genau identifiziert werden. Erst danach können sie hinsichtlich ihrer Grösse analysiert und entsprechend ihrer Bedeutung für die Organisation bewertet werden.

Wenn eine Organisation ihre Informationssicherheitsrisiken nur dürftig identifiziert hat, besitzt sie eine mangelhafte Grundlage für die Auswahl geeigneter Informationssicherheitsmassnahmen. Und als Folge davon kann die vorgeschlagene Informationssicherheitsrisikobehandlung unwirksam oder ineffizient und damit unangemessen teuer sein.

Es ist das Ziel dieses Artikels, die Identifizierung von Informationssicherheitsrisiken aus methodischer Sicht darzulegen und Hinweise zu geben, wie dies praktisch umgesetzt werden kann.Für die weiteren Ausführungen treffen wir die folgenden Annahmen und Vereinbarungen zum Sprachgebrauch:

Den Betrachtungen liegt eine Organisation beliebiger Art zugrunde. Diese kann privatwirtschaftlicher oder öffentlicher Natur sein, oder Teile oder eine Kombination davon.

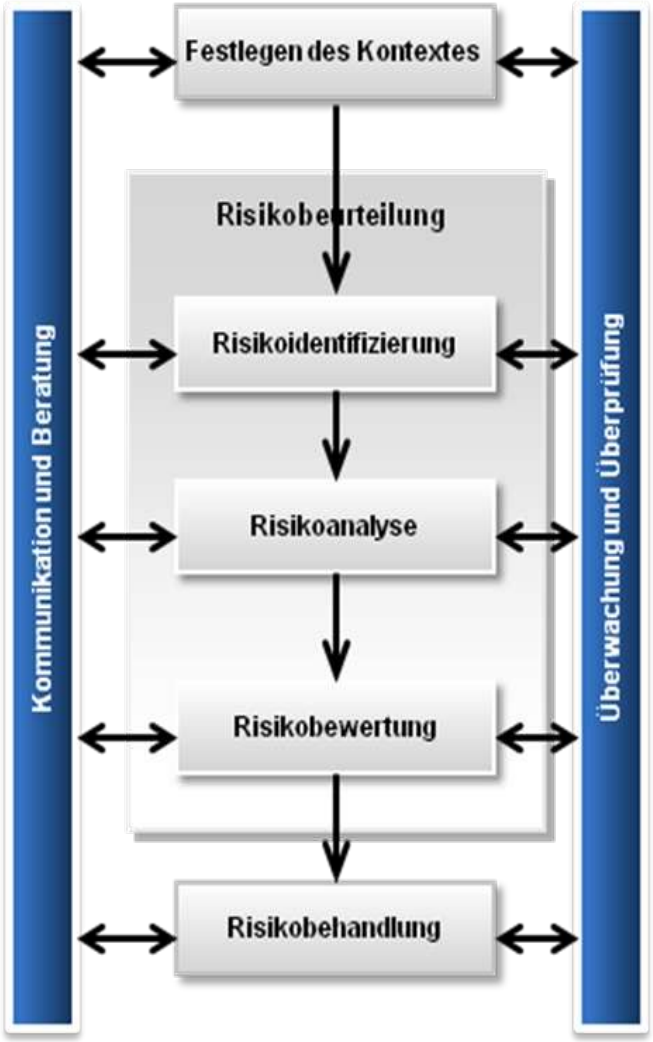
Diese Organisation hat ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet und umgesetzt, hält dieses ISMS aufrecht und verbessert es fortlaufend. Die Elemente des ISMS beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung, Betrieb, etc.

Der Anwendungsbereich des ISMS kann die ganze Organisation, bestimmte Funktionen der Organisation, bestimmte Bereiche der Organisation oder eine oder mehrere Funktionen über eine Gruppe von Organisationen hinweg umfassen. Zur Vereinfachung des Sprachgebrauchs benennen wir denjenigen Teil der Organisation, für den das ISMS anwendbar ist, im weiteren als *Organisation*.

2 Der Risikomanagementprozess im Überblick

ISO 31000:2009 [ISO 31000] beschreibt einen Risikomanagementprozess so wie er in Figur 1 dargestellt ist. Die Teilprozesse haben den folgenden Inhalt:

Figur 1 Der Risikomanagementprozess im Überblick



- **Kommunikation und Beratung:** Unterstützt während aller Phasen des Risikomanagementprozesses das Festlegen und Anpassen des Kontextes sowie die fortlaufende Verbesserung der anderen Teilprozesse.
- **Festlegen des Kontextes:** Legt die Ziele der Organisation für die Durchführung des Risikomanagementprozesses fest, bestimmt die externen und internen Themen sowie die Erfordernisse und Erwartungen extern-

er und interner interessierter Parteien, die bei der Handhabung von Risiken beachtet werden müssen, und legt den Anwendungsbereich sowie die Risikokriterien für die anderen Teilprozesse fest.

- **Risikoidentizierung:** Ermittelt die Informationssicherheitsrisiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Information innerhalb des Anwendungsbereichs des ISMS und identifiziert die Risikoeigentümer.
- **Risikoanalyse:** Schätzt die möglichen Folgen bei Eintritt der identifizierten Risiken ab, schätzt die realistischen Eintrittswahrscheinlichkeiten der identifizierten Risiken ab und bestimmt die Risikoniveaus.
- **Risikobewertung:** Vergleicht die Ergebnisse der Risikoanalyse mit festgelegten Risikokriterien und priorisiert die analysierten Risiken für die Risikobehandlung.
- **Risikobehandlung:** Wählt einer oder mehrerer angemessene Optionen zur Risikobehandlung unter Berücksichtigung der Ergebnisse der Risikobeurteilung aus und legt alle Massnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Risikobehandlung erforderlich sind, fest.
- **Überwachung und Überprüfung:** Erkennt Veränderungen bei den externen und internen Themen, den Erfordernissen und Erwartungen externer und interner interessierter Parteien, beim Anwendungsbereich sowie bei den Risikokriterien; stellt weitere Information zur Verfügung, um die Risikoidentifizierung, -analyse und -bewertung zu verbessern; analysiert und gewinnt Erkenntnisse aus Ereignissen, Veränderungen, Trends, Erfolgen und Fehlern; identifiziert neu aufkommende Risiken; erkennt die Wirksamkeit und Effizienz des gesamten Risikomanagementprozesses.

In den nachfolgenden Abschnitte wenden wir den Prozess gemäss Figur 1 an auf die Handhabung von Informationssicherheitsrisiken und beschränken uns gleichzeitig auf den Teilpozess der Risikoidentifizierung und alles, was für eine methodische Risikoidentifizierung erforderlich ist. Zur Vereinfachung des Sprachgebrauchs schreiben wir stets RisiikoXXX anstatt InformationssicherheitsrisikoXXX.

3 Vorbereitung des Risikoidentifizierungsprozesses

3.1 Festlegen des Kontextes

Zunächst muss der Kontext genau festgelegt werden. Dazu müssen alle für den Zweck der Organisation relevanten Themen, die für das ISMS relevanten interessierten Parteien sowie deren Anforderungen an die Informationssicherheit bestimmt werden. Werden diese Überlegungen zu eng oder zu oberflächlich angestellt, bleiben wesentliche Elemente unberücksichtigt und in Folge wird die Risikoidentizierung zwangsläufig lückenhaft sein.

3.1.1 Festlegen des externen Kontextes

Der externe Kontext umfasst alle relevanten Themen, interessierte Parteien sowie deren Anforderungen ausserhalb des Einflussbereichs der Organisation. Beispiele, die für Organisationen beliebiger Art gelten, sind etwa die Gesetzgebung und der Gesetzgeber, Lieferanten, Auftragnehmer, Konkurrenten und Kunden. Eine unfassendere Zusammenstellung findet sich in Tabelle 1. Die dort aufgeführten Themen und interessierten Parteien sind aber nicht als abschliessend zu betrachten und müssen für jede Organisation individuell angepasst werden.

3.1.2 Festlegen des internen Kontextes

Der interne Kontext umfasst alle relevanten Themen, interessierten Parteien sowie deren Anforderungen innerhalb des Einflussbereichs der Organisation. Beispiele, die für Organisationen beliebiger Art gelten, sind etwa Ziele, Strategien und Richtlinien zu deren Erreichung, Struktur und Führung, inkl. Rollen und Verantwortlichkeiten, Beschäftigte, Prozesse und Verfahren sowie Fähigkeiten in Form von Ressourcen und Wissen (Kapital, Zeit, Personen, Prozesse, Systeme, Technologien). Eine unfassendere Zusammenstellung findet sich in Tabelle 2. Wie beim externen Kontext sind die dort aufgeführten Themen und interessierten Parteien nicht als abschliessend zu betrachten und müssen für jede Organisation individuell angepasst werden.

Tabelle 1 Zusammenstellung möglicher Themen und interessierter Parteien ausserhalb des Einflussbereichs der Organisation

Gesellschaft und Kultur
Politisches Umfeld
Gesetzgebung und Gesetzgeber sowie regulatorischer Rahmen und Regulatoren
Normatives Umfeld
Gesamtwirtschaftliches Umfeld und Angebotsnachfrage
Technologischer Wandel
Umwelt
Wettbewerbssituation
Anteilseigner einschliesslich Eigentümer und Investoren
Lieferanten, Auftragnehmer und Auditoren
Konkurrenten
Kunden
Branchenverbände, Interessensgruppen und Aktivistengruppen
Öffentlichkeit

Tabelle 2 Zusammenstellung möglicher Themen und interessierter Parteien innerhalb des Einflussbereichs der Organisation

Kultur der Organisation
Ziele, Strategien und Richtlinien zu deren Erreichung
Aufsichtsgremium
Struktur und Führung, inkl. Rollen und Verantwortlichkeiten
Zuständige für Prozesse und Werte
Eigentümer von Risiken
Informationssicherheitsfachleute
Beschäftigte
Angewendete Normen, Leitfäden und Modelle
Prozesse und Verfahren
Fähigkeiten in Form von Ressourcen und Wissen (Kapital, Zeit, Personen, Prozesse, Systeme, Technologien)
Physische Infrastruktur
Informationssysteme und -flüsse
Audits und Risikobeurteilungen

3.2 Festlegen des Anwendungsbereichs

Auf der Basis der Überlegungen in den Abschnitten 3.1.1 und 3.1.2 muss genau beschrieben werden, wo der Risikomanagementprozess Anwendung finden soll und wo nicht. Dazu müssen:

- die Grenzen und Anwendbarkeit des ISMS bestimmt werden; das betrifft die:
  - Funktionen der Organisation (Produkte und Dienste);
  - Prozesse der Organisation;
  - Bereiche der Organisation;

– die Schnittstellen und Abhängigkeiten zwischen den Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten, die von anderen Organisationen durchgeführt werden, bestimmt werden; derartige Schnittstellen und Abhängigkeiten können sein:
  – rechtlich;
  – vertraglich;
  – physisch;
  – technisch.

Der Anwendungsbereich des Risikomanagementprozesses kann vom Anwendungsbereich des ISMS abweichen. Dies ist unter anderem dann der Fall, wenn eine externe Organisation eine Funktion, einen Prozess oder eine Tätigkeit ganz oder teilweise wahrnimmt bzw. durchführt. Diese Organisation befindet sich ausserhalb des Anwendungsbereichs des ISMS, obwohl die ausgliederte Funktion, der ausgliederte Prozess oder die ausgliederte Tätigkeit im Rahmen des ISMS Anwendungsbereichs liegt. Da die damit verbundenen Verantwortlichkeiten aber bei der Organisation verbleiben, müssen die mit der Ausgliederung einhergehenden Risiken Bestandteil des Risikomanagementprozesses sein.

3.3 Risikokriterien

Die Beschreibung der möglichen Folgen von Sicherheitsereignissen für die Geschäftstätigkeit der Organisation hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Information kann durch verschiedene Personen und bei Wiederholung des Risikoidentifzierungsprozesses grundsätzlich sehr unterschiedlich ausfallen. Um die Anforderungen der Konsistenz, Vergleichbarkeit und Reproduzierbarkeit der Ergebnisse an diesen Prozess gemäss Abschnitt 4.2 zu erfüllen, müssen diese Beschreibungen strukturiert und standardisiert werden. Dies geschieht mit Hilfe von Folgekriterien, die vor Beginn der Risikoidentifizierung detailliert und mit ausreichender Genauigkeit festgelegt werden müssen.

Ein Auszug aus einem Folgekriterienkatalog, gegliedert nach Folgen für die Vertraulichkeit, Integrität und Verfügbarkeit von Information, ist in Tabelle 3 dargestellt.

Die Folgekriterien sind für den Risikoanalyseprozess, der sich an den Risikoidentifizierungsprozess anschliesst, von zentraler Bedeutung.

Tabelle 3 Auszug aus einem Folgekriterienkatalog

Folgen für die Vertraulichkeit	Folgen für die Integrität	Folgen für die Verfügbarkeit
Verletzung der Privatsphäre von internen oder externen Benutzern	Fehllieferung infolge widersprüchlicher Daten	Leistungsabbau von Diensten
Verlust von Wettbewerbsvorteilen	Unmöglichkeit, einen korrekten Jahresabschluss zu erstellen	Nichtverfügbarkeit von Diensten
Verlust der Technologieführerschaft	Unfähigkeit, gesetzliche Verpflichtungen zu erfüllen	Betriebsunterbrechung

4 Der Risikoidentifizierungsprozess

4.1 Ziel

Die Risikoidentifizierung ist der Prozess zum Finden, Erkennen und Beschreiben von Risiken. Dabei ist Risiko definiert als die Auswirkung von Ungewissheit auf Ziele (ISO 31000:2009 [ISO 31000]). Ziel der Risikoidentifizierung ist es basierend auf denjenigen Ereignissen, die das Erreichen von Zielen verursachen, verbessern, verhindern, vermindern, beschleunigen oder verzögern, eine umfassende Liste von Risiken zu erstellen.

4.2 Anforderungen

Um Vertrauen in die Aussagekraft und Qualität der Risikoidentifizierung zu schaffen, muss der Risikoidentifizierungsprozess auf ausreichend detaillierte Methoden und Werkzeuge gestützt sein, sodass wiederholte Risikoidentifizierungen zu konsistenten, vergleichbaren und reproduzierbaren Ergebnissen führen.

Wiederholte Anwendungen des Risikoidentifizierungsprozesses können dabei helfen, Probleme mit den gewählten Methoden und Werkzeugen (die sich in Form von Inkonsistenzen oder Unstimmigkeiten manifestieren) zu identifizieren.

Unabhängig von den gewählten Methoden und Werkzeugen muss der Risikoidentifizierungsprozess sicherstellen, dass:

- alle Risiken mit dem erforderlichen Detaillierungsgrad betrachtet werden;
- die Ergebnisse konsistent und reproduzierbar sind, d.h. sie können durch Dritte verstanden werden;
- seine Ergebnisse die gleichen sind, wenn verschiedene Personen die Risiken im gleichen Kontext identifizieren;
- die Ergebnisse von wiederholten Risikoidentifizierungen vergleichbar sind.

4.3 Ausgangspunkt

Unabhängig vom gewählten Ansatz zur Risikoidentifizierung sind die Ausgangspunkte die für die Organisation festgelegten Informationssicherheitsziele, der Kontext der Risikoidentifizierung gemäss Abschnitt 3.1 und deren Anwendungsbereich gemäss Abschnitt 3.2

4.4 Ansätze zur Risikoidentifizierung

Zwei Ansätze werden üblicherweise für die Identifizierung von Risiken gebraucht:

- ein Ereignis-basierter Ansatz;
- ein Ansatz, der auf der Identifizierung von Werten, Bedrohungen und Schwachstellen beruht.

Beide Ansätze sind mit den Prinzipien und allgemeinen Leitlinien zur Risikobeurteilung von ISO 31000:2009 konsistent. Andere Ansätze können benutzt werden, sind aber nur empfehlenswert, wenn sie die Anforderungen in Abschnitt 4.2 sicherstellen können. Ist ein ISMS das Ziel, welches den Anforderungen von ISO/IEC 27001:2013 genügt, ist das Sicherstellen dieser Anforderungen unabdingbar.

4.4.1 Der Ereignis-basierte Ansatz

4.4.1.1 Übersicht

Beim Ereignis-basierten Ansatz werden Risiken durch die Betrachtung von Ereignissen und ihren Folgen identifiziert. Betrachtete Ereignisse können in der Vergangenheit geschehen sein oder können für die Zukunft erwartet werden. Im ersten Fall können sie historische Daten umfassen, im zweiten Fall können sie auf theoretischen Analysen, sachkundigen Meinungen und Expertenmeinungen sowie Bedürfnissen von interessierten Parteien beruhen.

4.4.1.2 Ereignisse und ihre Ursachen

Zunächst werden durch Betrachtung der Fragen "Wer?", "Was?", "Wo?", "Wann?" und "Warum?" mögliche Ereignisse beschrieben. Um die Ermittlung der Ereignisse zu unterstützen, werden in der Praxis Ereigniskataloge herangezogen. Durch den Basler Ausschuss für Bankenaufsicht wurde z.B, ein ausführlicher Katalog für den Bankensektor erstellt [Basel II]. Ein Auszug aus einem Ereigniskatalog ist in Tabelle 4 dargestellt.

Danach werden die Ursachen für diese Ereignisse ermittelt, um ein tiefergehendes Verständnis für die Risiken zu erreichen und so Hinweise auf die unterliegenden Bedrohungen und Schwachstellen zu erhalten.

Tabelle 4 Auszug aus einem Ereigniskatalog

Ereignistyp	Ereignis
Interner Betrug	Fälschung von Daten oder Dokumenten
	Ausführung einer unbefugten Transaktion
Externer Betrug	Diebstahl durch Drittpersonen
	Hacking
Beschäftigungspraktiken	Fehler bei der Beendigung der Beschäftigung
	Verletzung von Sicherheitsregelungen
Kunden, Produkte und Geschäftspraktiken	Verletzung der Privatsphäre
	Missbrauch von vertraulicher Information
Beschädigung physischer Werte	Zerstörung durch terroristische Angriffe
	Zerstörung von Geräten und Einrichtungen
Betriebsstörung und Systemfehler	Ausfall eines Imformationssystems
	Zerstörung der Stromversorgung
Ausführung, Erfüllung und Handhabung von Prozessen	Vereinbarte Leistung wurde nicht erbracht
	Unvollständige Kundenaufzeichnungen

4.4.1.3 Folgen

Schliesslich werden für alle Ereignisse die möglichen Folgen beschrieben. Folgen, die den Zielen der Organisation nicht zugeordnet werden können, tragen nicht zu den Risiken bei und können daher ignoriert werden. Falls derartige Folgen jedoch so wahrgenommen werden, dass sie tatsächlich zu Risiken beitragen, deutet dies an, dass es in der Liste der Ziele der Organisation Auslassungen gibt, die korrigiert werden sollten.

Bei der Beschreibung der Folgen werden die in Abschnitt 3.3 festgelegten Folgekriterien herangezogen.

4.4.1.4 Vor- und Nachteile

Von Vorteil dieses vorwiegend wirkunsorientierten Ansatzes ist, dass seine Verwendung mit vergleichsweise geringem Aufwand verbunden ist. Damit eignet er sich, um ein erstes, grobes Bild der Informationssicherheitsrisiken zu erstellen. Man kann argumentieren, dass so eine Fokussierung der Risikoidentifizierung auf die kritischen Risiken unterstützt wird.

Nachteilig ist, dass bestehende Bedrohungen und Schwachstellen als mögliche Ursachen der Ereignisse nicht notwendigerweise systematisch ermittelt werden. Das erschwert im später erfolgenden Risikobehandlungsprozess die zielorientierte Auswahl von Massnahmen. Ebenfalls nachteilig ist, dass Risiken übersehen werden können.

4.4.2 Der auf Werten, Bedrohungen und Schwachstellen basierte Ansatz

4.4.2.1 Übersicht

Bei diesem Ansatz werden Risiken durch die Betrachtung von Werten, Bedrohungen, Schwachstellen und dazugehörigen Folgen identifiziert. Diese Folgen ergeben sich, wenn Bedrohungen Schwachstellen eines Werts oder einer Gruppe solcher Werte ausnutzen und damit einer Organisation Schaden zufügen.

4.4.2.2 Identifizierung von Werten

Ein Wert ist alles, was für eine Organisation von Wert ist und daher Schutz benötigt. Zwei Arten von Werten können unterschieden werden: primäre Werte und unterstützende Werte.

Die primären Werte setzen sich zusammen aus den Geschäftsprozessen und -tätigkeiten sowie derjenigen Information, die für den Zweck der Organisation von zentraler Bedeutung ist. Dies sind daher die Werte, die bei der Risikoidentifizierung als erstes betrachtet werden müssen.

Die unterstützenden Werte können in Hardware, Software, Netzwerk, Personal, Standort und Organisation klassifiziert werden. Sie können als Behältnisse im weiteren Sinne betrachtet werden, um die primären Werte zu verarbeiten, speichern, archivieren oder anderweitig zu bearbeiten oder handzuhaben. Unterstützende Werte besitzen in der Regel Schwachstellen, die durch Bedrohungen ausgenutzt werden können, welche darauf abzielen, die primären Werte zu schädigen.

Für jeden Wert sollte ein Zuständiger benannt werden, der für den Umgang mit dem Wert sowie dessen Instandhaltung und Sicherheit verantwortlich ist. Dieser Zuständige ist oft auch die geeignetste Person, um die Werthaftigkeit des Wertes zu bestimmen.

4.4.2.3 Identifizierung von Bedrohungen

Eine Bedrohung ist eine mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder einer Organisation führen kann.

Bedrohungen können die Schwachstellen von einem oder mehreren Werten ausnutzen. Sie können auf Naturereignissen basieren, zufälliger, versehentlicher oder aber absichtlicher und damit bewusster und vorsätzlicher Herkunft sein.

Bedrohungen können nach Typen klassifiziert werden. ISO/IEC 27005:2011 [ISO/IEC 27005] schlägt z.B. die folgende Klassifizierung vor:

- physische Schäden;
- Naturereignisse;
- Verlust von Versorgungseinrichtungen;
- Störung infolge Strahlung;
- Kompromittierung von Information;
- technische Ausfälle;
- unbefugte Handlungen;
- Kompromittierung von Aufgaben.

Bei der Bestimmung der Bedrohungen kann mithilfe dieses Klassifizierungsschemas sichergestellt werden, dass wichtige Bedrohungen nicht vergessen werden.

Ein Auszug aus einem Bedrohungskatalog ist in Tabelle 5 dargestellt.

4.4.2.4 Identifizierung von Schwachstellen

Eine Schwachstelle ist eine Schwäche eines Wertes oder einer Massnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann.

Schwachstellen sind damit wesentliche Eigenschaften von Werten oder Massnahmen. Diese Eigenschaften müssen nicht ausschliesslich negativer Art sein. So ist z.B. die grosse Beweglichkeit von Mobilgeräten jeder Art (Laptops, Netbooks, Tablets, Smartphones, etc.) gewünscht. Auf der negativen Seite macht diese Beweglichkeit diese Geräte aber leichter ausnutzbar für Bedrohungen wie Diebstahl, Abhören oder Fernspionage. Ähnliches gilt für Werte wie Wechseldatenträger.

Analog kann bei Massnahmen z.B. eine schwache Zugangssteuerung genannt werden. Während diese den Zutritt zu Räumlichkeiten und den Zugriff auf Systeme oder Anwendungen erleichtert, sind auf der negativen Seite die Ausnutzbarkeit durch Bedrohungen wie Diebstahl oder Zerstörung von Datenträgern, Dokumenten oder

Tabelle 5 Auszug aus einem Bedrohungskatalog

Bedrohungstyp	Beispiele
Physische Schäden	Feuer
	Wasser
Naturereignisse	Erdbeben
	Überschwemmung
Verlust von Versorgungseinrichtungen	Versagen der Klimaanlage
	Stromausfall
Störung durch Strahlung	Elektromagnetische Strahlung
	Thermische Strahlung
Kompromittierung von Information	Abhören
	Diebstahl von Dokumenten
Technische Ausfälle	Ausfall von Geräten
	Sättigung des Informationssystems
Unbefugte Handlungen	Unbefugte Benutzung von Geräten
	Gebrauch gefälschter Software
Kompromittierung von Funktionen	Missbrauch von Rechten
	Fälschung von Rechten

Geräten, die unbefugte Benutzung von Geräten, die Verfälschung von Daten oder das Leugnen von Tätigkeiten zu nennen.

Schwachstellen können wie Bedrohungen nach Typen klassifiziert werden. ISO/IEC 27005:2011 [ISO/IEC 27005] schlägt z.B. eine Klassifizierung nach unterstützenden Werten vor:

- Hardware;
- Software;
- Netzwerk;
- Personal;
- Standort;
- Organisation.

Ein Auszug aus einem Schwachstellenkatalog ist in Tabelle 6 dargestellt.

Tabelle 6 Auszug aus einem Schwachstellenkatalog

Schwachstellentyp	Beispiele
Hardware	Ungenügende Instandhaltung
	Portabilität
Software	Fehlen einer Zugriffsprotokollierung
	Komplizierte Benutzeroberfläche
Netzwerk	Fehlen von Verschlüsselung
	Fehlen von Redundanz
Personal	Ungenügendes Sicherheitstraining
	Fehlen von Aufsicht
Standort	Instabiles Stromnetz
	Lage in einem Überschwemmungsgebiet
Organisation	Fehlen einer Aufgabentrennung
	Fehlen einer Arbeitsplatzbeschreibung

Es entspricht der Logik des auf Werten, Bedrohungen und Schwachstellen basierten Ansatzes zur Risikoidentifizierung, dass eine Schwachstelle für sich genommen keinen Schaden verursachen kann, weil eine Bedrohung existieren muss, um diese Schwachstelle auszunutzen. Derartige Schwachstellen müssen aber identifiziert und überwacht werden, weil infolge Veränderungen des internen oder externen Umfelds passende Bedrohungen neu in Erscheinung treten können.

Analoges gilt umgekehrt für festgestellte Bedrohungen, zu denen es keine entsprechenden Schwachstellen gibt. Auch diese Bedrohungen müssen identifiziert und überwacht werden, weil im Laufe der Zeit Werte oder bereits umgesetzte Massnahmen passende Schwachstellen entwickeln können.

4.4.2.5 Identifizierung von Folgen

Wird die Schwachstelle eines Wertes oder einer Massnahme durch eine Bedrohung ausgenutzt, wird zunächst eine unmittelbare Auswirkung auf die Informationssicherheit verursacht. So wird etwa vertrauliche Information unbefugten Personen bekannt, verfälschte Dokumente werden in Umlauf gesetzt oder ein Informationssystem fällt aus. Derartige Ereignisse können schliesslich Folgen für die Geschäftstätigkeit der Organisation auslösen. In den genannten Beispielen können diese z.B. sein die Verletzung vertraglicher Vereinbarungen oder anwendbarer Gesetze, der Leistungsabbau oder die Nichtverfügbarkeit von Diensten oder eine komplette Betriebsunterbrechung.

Die Unterscheidung zwischen unmittelbaren Auswirkungen auf die Informationssicherheit und Folgen für die Geschäftstätigkeit der Organisation infolge eines Verlusts der Vertraulichkeit, Integrität oder Verfügbarkeit von Information ist wesentlich. Die Auswirkungen und Folgen müssen für jedes einzelne Ereignis, bei dem eine Bedrohung eine Schwachstelle eines Wertes oder einer Massnahme ausnutzt, identifiziert und mit ausreichender Genauigkeit beschrieben werden. Bei der Beschreibung der Folgen werden die in Abschnitt 3.3 festgelegten Folgekriterien herangezogen.

4.4.2.6 Vor- und Nachteile

Wichtigster Vorteil ist, dass dieser ursachenorientierte Ansatz es erlaubt, die Folgen von Ereignissen systematisch mit den Schwachstellen von Werten und Massnahmen in Verbindung zu setzen. Das schafft die Voraussetzungen dafür, dass im später erfolgenden Risikobehandlungsprozess die Massnahmen sehr spezifisch und zielgerichtet ausgewählt und deren erforderliche Umsetzungsbreite und -tiefe genau bestimmt werden können. Damit wird sowohl die Wirksamkeit als auch die Effizienz des ISMS sichergestellt. Auch kann dieser Ansatz besser sicherstellen, dass alle relevanten Risiken berücksichtigt werden.

Von Nachteil ist der potentiell grosse Aufwand für diesen Ansatz. Die Identifizierung der relevanten Werte ist nicht immer einfach. Jeder Wert kann eine oder mehrere Schwachstellen besitzen, die jede für sich durch eine oder mehrere Bedrohungen ausgenutzt werden kann. Darum kann die Anzahl der Ereignisse kombinatorisch recht schnell anwachsen.

4.4.3 Identifizierung der Risikoeigentümer

Für die der Risikoidentifizierung nachfolgenden Prozessschritte ist es wichtig für jedes identifizierte Risiko einen Risikoeigentümer zu bestimmen. Diese Personen sind verantwortlich für die Handhabung dieser Risiken, die auch prozessübergreifend sein können. Um dieser Verantwortung nachkommen zu können, müssen ihnen durch die Prozessverantwortlichen die erforderlichen Ressourcen zugewiesen werden.

5 Risikoidentifizierung in der Praxis

5.1 Voraussetzungen

Bevor mit der praktischen Umsetzung der Risikoidentifizierung begonnen werden kann, sind verschiedene Voraussetzungen zu erfüllen.

5.1.1 Führung und Verpflichtung

Die oberste Leitung, d.h. die Person oder Personengruppe, welche die Organisation auf der obersten Ebene führt und steuert, muss dafür sorgen, dass die Verantwortlichkeiten für den Risikomanagementprozess und dessen Anwendung dem Anwendungsbereich dieses Prozesses entsprechend in der Organisation positioniert und eingegliedert wird.

Die oberste Leitung muss auch die Bedeutung der Wirksamkeit dieses Prozesses für den Erfolg der Organisation vermitteln. Will man Glaubwürdigkeit und Nachhaltigkeit sicherstellen, ist dies keine delegierbare Tätigkeit.

Schliesslich muss die oberste Leitung die erforderlichen Ressourcen in Form von Personen, Zeit, finanziellen Mitteln und Information für die Entwicklung des Prozesses, dessen Anwendung sowie dessen fortlaufender Verbesserung bereitstellen.

5.1.2 Ausbildung und Schulung

Risiko ist in den Medien, in der Öffentlichkeit und im Alltag von Organisationen jeder Art ein oft gebrauchter Begriff. In der Regel basiert dessen Verwendung auf einem intuitiven Verständnis der mit dem Begriff im Zusammenhang stehenden Konzepte. Daraus zu schliessen, dass allein deswegen die erforderlichen Voraussetzungen gegeben sind, um eine Risikoidentifizierung erfolgreich durchzuführen, ist ein weit verbreiteter Irrtum.

Ebenso gilt, dass wer befähigt ist, Finanzrisiken oder unternehmerische Risiken erfolgreich zu beurteilen, nicht notwendigerweise das Wissen und die Fertigkeiten besitzt, um Informationssicherheitsrisiken kompetent zu identifizieren (sowie danach zu analysieren, bewerten und behandeln).

Eine angemessene Ausbildung und Schulung für alle diejenigen Personen, welche an der Durchführung der Risikoidentifizierung direkt beteiligt sind, ist daher eine unabdingbare Voraussetzung.

Risikoidentifizierung ist keine exakte Wissenschaft oder etwas, das durch das Abarbeiten einer Checkliste erledigt werden kann. Vielmehr ist unabhängig vom gewählten Ansatz immer wieder fundiertes Beurteilungsvermögen gefragt, angefangen bei der Festlegung des Kontextes über die Bestimmung der relevanten Ereignisse, Werte, Bedrohungen und Schwachstellen bis hin zur Festlegung der Folgekriterien für Ereignisse.

Es muss daher ein wichtiges Ausbildungs- und Schulungsziel sein, dass die o.g. Personen sich dieses Beurteilungsvermögen aneignen und allgemein die Fertigkeit erwerben, mit Unschärfe und Ungewissheit kompetent umgehen zu können.

5.1.3 Sensibilisierung und Bewusstsein

Eine wirksame Risikoidentifizierung setzt voraus, dass neue Ursachen von Risiken und andere relevante Information zeitgerecht für die Durchführung des Risikoidentifizierungsprozesses erschlossen und diesem zugänglich gemacht werden. Alle Beschäftigten auf allen Hierarchiestufen der Organisation müssen sich bewusst sein, dass sie ständig Informationssicherheitsrisiken ausgesetzt sind und jederzeit selbt zu deren Vermeidung beitragen müssen. Alle müssen sich bewusst sein, dass weder IT-Mittel noch die IT-Abteilung ein universell wirksames Schutzschild sein können. Um das zu erreichen, muss das Thema Informationssicherheit in der ganzen Organisation wirksam verankert werden, um alle internen Informationsquellen zu erschliessen. Dies kann mit entsprechenden Massnahmen zur Sensibilisierung und Bewusstseinsbildung erreicht werden.

Beispiele für interne und externe Informationsquellen sind in Tabelle 7 zusammengestellt.

Tabelle 7 Beispiele für interne und externe Informationsquellen

Quellen	Bedrohungen	Schwachstellen
Intern		
Oberste Leitung	x	
Leitende Angestellte	x	
Business Continuity Management	x	
Interne Fachexperten aller Art	x	x
Zuständige für Werte	x	x
Risikoeigentümer	x	
Internes ISMS Audit		x
Management von Informationssicherheitsvorfällen	x	x
Patch Management		x
Extern		
Externe Informationssicherheitsexperten	x	x
Computer Emergency Response Teams	x	x
Spezielle Interessensgruppen	x	x
Meldestellen für Informationssicherheit	x	x
Geheimdienste	x	
Anbieter von Informationssicherheitsdiensten	x	x
Versicherungsgesellschaften	x	
Fachmedien	x	x
Massenmedien	x	
Technische Sicherheitsaudits		x
Lieferanten von Hardware und Software		x

5.2 Herausforderungen

Die Identifizierung der einzelnen Ereignisse, Werte, Bedrohungen und Schwachstellen bis hin zur Festlegung der Folgekriterien ist nicht einfach. Auf der Basis der in Abschnitt 5.1.2 beschriebenen Ausbildung und Schulung haben sich in der Praxis moderierte Expertengespräche bewährt. An den Gesprächen sollten Personen mit fundiertem Wissen über die Tätigkeiten der Organisation sowie über Hardware-, Software- und Netzwerktechnologien, Personalwesen, Standortsicherheit und Organisation teilnehmen. Diese Gespräche können durch Hilfsmittel wie Kataloge aller Art unterstützt werden. Die Moderation dieser Gespräche sollte durch eine unabhängige interne oder externe Person erfolgen.

Die zentrale Herausforderung ist, den Umfang der Risikoidentifizierung überschaubar und handhabbar zu halten. Das trifft insbesondere zu, wenn der auf Werten, Bedrohungen und Schwachstellen basierte Ansatz zum Einsatz gelangt. Gleichzeitig muss sichergestellt werden, dass die Risikoidentifizierung die wesentlichen Verhältnisse in der Organisation angemessen widerspiegelt. Unabhängig vom gewählten Ansatz ist auf jeden Fall ein fundiertes Beurteilungsvermögen unerlässlich.

Zwei Vorgehensweisen haben sich in der Praxis bewährt: Fokussierung und Vergröberung:

– Bei der Fokussierung kommt das Konzept der Materialität zum Einsatz. Welche Ereignisse oder welche primären Werte sind wirklich für die Organisation von Bedeutung? Das bedeutet, dass die Anzahl der berücksichtigten Prozesse eingeschränkt wird.

– Bei der Vergröberung werden je nach Ansatz Ereignisse oder aber Werte und/oder Bedrohungen gruppiert. Beispiele sind hier etwa die Zusammenfassung von Hardware, Software- und Netzwerkkomponenten zu einem Informationssystem, das einem bestimmten Zweck dient. Oder die Beschränkung, bei den Bedrohungen nur nach Bedrohungstypen zu unterschieden, anstatt einzelne Bedrohungen innerhalb eines Typs separat zu betrachten.

5.3 Fortlaufende Verbesserung

Es ist nicht empfehlenswert, die Risikoidentifizierung im ersten Zyklus der Risikobeurteilung zu detailliert durchzuführen. Ein grobes, aber eindeutiges Bild der Informationssicherheitsrisiken zu haben ist weit besser als gar kein Bild. Der Detaillierungsgrad kann in weiteren Zyklen im Rahmen der fortlaufende Verbesserung des ISMS Schritt für Schritt verfeinert werden.

Eine mögliche Herangehensweise an die Risikoidentifizierung könnte z.B. die folgende sein:

1. Zyklus: Grober Überblick durch Anwendung des Ereignis-basierten Ansatzes;
2. Zyklus: Anwendung des (Werte, Bedrohungen, Schwachstellen)-basierten Ansatzes, um dann in der nachfolgenden Risikoanalyse unter Nichtberücksichtigung der möglichweise bereits umgesetzten Massnahmen die inhärenten Risiken zu bestimmen und zu verifizieren, ob die bereits getroffenen Massnahmen angemessen oder aber bereits zu umfangreich sind;
3. Folgende Zyklen: Anwendung des (Werte, Bedrohungen, Schwachstellen)-basierten Ansatzes unter Berücksichtigung der aktuell umgesetzten Massnahmen, um den risikobasierten Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Information schrittweise zu verbessern und den aktuellen Anforderungen und Bedrohungen anzupassen.

6 Zusammenfassung

Die Bedeutung der methodischen Risikoidentifizierung für ein wirksames Management von Informationssicherheitsrisiken wird in den meisten Fällen nicht erkannt. Sie ist aber für einen wirksamen Risikomanagementprozess wesentlich. Ohne eine solche, die auf die spezifischen Bedürfnisse der Organisation exakt zugeschnitten ist, hat der ganze Prozess nur wenig Wert. Jedes Risiko, das in diesem Prozessschritt nicht identifiziert wird, bleibt in den nachfolgenden Prozessschritten unberücksichtigt.

Es gibt verschiedene Ansätze zur Risikoidentifizierung deren jeweilige Stärken und Schwächen berücksichtigt werden müssen, wenn man den Prozess festlegt. Bei der praktischen Umsetzung ist die Erfüllung verschiedener Voraussetzungen ausschlaggebend für den Erfolg.

Wird die Risikoidentifizierung jedoch mit der erforderlichen Sorgfalt ausgeführt, ergeben sich unmittelbar mindestens zwei gewichtige Vorteile. Einerseits werden die notwendigen Voraussetzungen geschaffen, um in den nachfolgenden Prozessen der Risikoanalyse, -bewertung und -behandlung nicht nur die Auswahl von Massnahmen jeglicher Art vorzubereiten und zu steuern, sondern insbesondere auch deren Umsetzungsbreite und -tiefe zu bestimmen, genau in dem Umfang, wie er für die Organisation erforderlich ist. Die Kosteneffizienz der so umgesetzten Massnahmen kann damit (deutlich) höher liegen, als wenn man sich einfach ohne weitere Überlegung und Differenzierung auf die vielfach angepriesene gute fachliche Praxis (best practices) verlässt. Andererseits schafft eine solide Risikoidentifizierung auch die Voraussetzung für eine Diskussion mit Lieferanten von Hardware- und Software Sicherheitslösungen auf gleicher Augenhöhe. Dies kann helfen, unnötige Kosten zu sparen.

Die Handhabung von Informationssicherheitsrisiken ist in der Praxis nicht immer einfach. Es können schnell mehrere hundert Ereignisse zusammenkommen, die über den fortlaufenden Verbesserungsprozess verwaltet werden müssen. Die Konsistenz, Reproduzierbarkeit und Vergleichbarkeit ist dann mithilfe einer einfachen Tabelle nur schwer aufrechtzuerhalten. Daher arbeiten wir derzeit zusammen mit den Unternehmen Glue Software Engineering AG und fenceIT AG an einem Werkzeug, das eine bessere und einfachere Verwaltung und Handh-

abung des gesamten Risikoprozesses erlaubt und insbesondere die Umsetzung und Verifizierung der Einhaltung der Prozessanforderungen gemäss ISO/IEC 27001:2013 unterstützt.

Weitere Information zum praxisorientierten Management von Informationssicherheitsrisiken findet sich im lesenswerten Buch von Hans-Peter Königs [Königs].

Danksagung

Mein Dank gilt meinen Kollegen vom Normenkomitee INB NK 149 UK 7 der Schweizerischen Normen-Vereinigung (SNV): Hans-Peter Königs, IT Risk KM Consulting GmbH, Markus Soland, UBS AG und Peter Weiss, Swiss Re Management Ltd, für die stets ausgezeichnete Zusammenarbeit bei der Neuauflage von ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27006 sowie bei der Überarbeitung von ISO/IEC 27003 und ISO/IEC 27005 im Rahmen von ISO JTC 1/SC 27 und Hans Halstrick, Swiss TS Technical Services AG, für viele anregende Diskussionen zum Thema der Risikobeurteilung und -behandlung in der Praxis eines Zertifizierungsauditors.

Referenzen

[Basel II] Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards; A Revised Framework, comprehensive Version, June 2006, Bank for International Settlements

[ISO 31000] ISO 31000:2009, Risk management - Principles and guidelines

[ISO/IEC 27000] ISO/IEC 27000:2016

[ISO/IEC 27001] ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements

[ISO/IEC 27005] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

[Königs] Hans-Peter Königs, IT-Risikomanagement mit System. Praxisorientiertes Management von Informationssicherheits- und IT Risiken. Springer Verlag, 4. Auflage, 2013.