2. Kapitel

2 Grundlagen

„Wenn Sie denken, Technologie kann Ihre Sicherheitsprobleme lösen, dann verstehen Sie die Probleme nicht und Sie verstehen die Technologie nicht."
-- Bruce Schneier

Voraussetzungen

Wenn Sie sich mit dem Management von Risiken für die Informationssicherheit auseinandersetzen wollen, müssen Sie sich vor allem einer Sache bewusst werden: Keine Technologie dieser Erde wird Ihre Sicherheitsprobleme lösen. Technologie verschafft Ihnen vielleicht an einer Stelle einen gewissen Vorsprung vor den Angreifern, an einer anderen Stelle jedoch reißt sie neue Lücken auf. Im schlimmsten Fall macht sie für einen Angreifer sogar den besonderen Reiz aus, gerade Ihre Systeme anzugreifen. Im Rahmen von Sicherheitsmanagement ist Technologie nur ein Mittel zum Zweck, ein Werkzeug. Ganz so, wie ein Bildhauer Hammer und Meißel benutzt – Hammer und Meißel stehen niemals im Mittelpunkt seines Schaffens. Die Aufgabe eines Künstlers ist es – zum Beispiel – eine Skulptur zu gestalten, sie mit

S. Klipper, *Information Security Risk Management,* Edition <kes>,
DOI 10.1007/978-3-658-08774-6_2, © Springer Fachmedien Wiesbaden 2015

Inhalt zu füllen. Wenn ihm die Ideen ausgehen oder den Besuchern seiner Galerie die Skulpturen einfach nicht gefallen, dann hilft es nichts, wenn er seine Werkzeuge austauscht. Um das Zitat vom Kapitelbeginn aufzugreifen: Wenn dieser Künstler denkt Werkzeuge könnten seine Probleme lösen, dann versteht er weder seine Probleme noch sein Werkzeug.

Was Sie in diesem Kapitel erfahren

In Kapitel 2 erfahren Sie die Grundlagen der Kunst, sich von der Technologie zu lösen und über die eigentlichen Probleme im Bereich der Sicherheit nachzudenken. Sie erhalten dazu einen Überblick über das Thema Management von Informationssicherheit im Ganzen und Sie bekommen das nötige Fundament, auf dem wir in den folgenden Kapiteln aufbauen, wenn wir uns mit den Herausforderungen des Risikomanagements beschäftigen.

2.1 Sprachgebrauch, Begriffe und Besonderheiten der Übersetzung

Bevor wir endgültig durchstarten können, müssen wir noch eine Sache erledigen, die gerne vernachlässigt wird: Wir müssen uns auf ein gemeinsames Vokabular verständigen. Das ist wichtig, damit wir nicht dieselben Worte für unterschiedliche Dinge verwenden. Dies ist umso wichtiger, wenn Sicherheitsexperten unter sich sind. Sie sprechen leider oft nicht dieselbe Sprache und verstehen sich nicht richtig, obwohl sie sich objektiv richtig ausgedrückt haben. Entscheidend ist jedoch, wie der Empfänger der Nachricht sie subjektiv verstanden hat. Selbst Sicherheitsexperten sprechen nicht immer vom selben Thema, obwohl sie dieselben Worte benutzen. Diesen Sachverhalt habe ich bereits in meinem ersten Buch näher beleuchtet, auf das ich Sie an dieser Stelle aufmerksam machen möchte:

Sebastian Klipper
Konfliktmanagement für Sicherheitsprofis
Auswege aus der Buhmann-Falle
für IT-Sicherheitsbeauftragte, Datenschützer und Co.
Springer Vieweg, 2. Auflage, 2015

Einheitliche Übersetzung

Einer der Gründe für diesen Begriffswirrwarr sind die Schwierigkeiten bei der Übersetzung aus dem Englischen. Da fast alle hier zitierten Standards ursprünglich in Englisch vorliegen, gilt es die Begriffe richtig ins Deutsche zu übertragen. Hierzu gehen wir die wichtigsten Begriffe der Normenreihe ISO/IEC 27000 systematisch durch. Insgesamt legt die ISO/IEC 27000 [6] fast 90 Begriffe fest, von denen wir hier etwa 30 genauer betrachten.

Bei einigen Begriffen ist es möglich, die englischen Begriffe beizubehalten. So ist es durchaus sinnvoll, auch im Deutschen von *„Controls“* statt von *„Maßnahmen“* zu sprechen. Die Grenzen sind hier sicher fließend. Ein weiteres Beispiel wären die Worte Incident und Vorfall, die beide verwendet werden können.

Offizielle Übersetzung

Auch ist es möglich, die deutschen Übersetzungen der Standards zu verwenden. Man sollte sich jedoch nicht zu viel von diesen Übersetzungen erwarten. Da wird *„normative references“* schon mal mit *„normative Verweisungen“* übersetzt und Risiken werden mal *„abgeschätzt“*, mal *„eingeschätzt“* und mal *„bewertet“*, wobei *„estimation“* und *„assessment“ wiederum* jeweils mit *„einschätzen“* übersetzt wird. Die deutsche Übersetzung kann das Original daher zwar formell ersetzen, sorgt stellenweise aber für Verwirrung. Ich empfehle stets die Verwendung des englischen Originals.

Im folgenden Abschnitt werden die wichtigsten Begriffe – ausgehend von den englischen Standards – übersetzt und festgelegt. Am Seitenrand finden Sie in alphabetischer Reihenfolge die englischen Originalbegriffe und im Text daneben die jeweilige Übersetzung, bei der die Verständlichkeit jeweils im Vordergrund stand. Insbesondere soll dadurch die Anzahl der ähnlich klingenden Begriffe reduziert werden. Gleichzeitig wird dieser Abschnitt bereits dazu genutzt, die Bedeutung der Begriffe transparent zu machen.

Wandel der Begriffe

Gehen wir nun im folgenden Abschnitt die Begriffe durch, die in den Standards jeweils verwendet werden.[3] Man muss hierbei wissen, dass sich die Begriffe im verlauf der Zeit in ihrer Definition wandeln. Noch vor wenigen Jahren wurden sie in unterschiedlichsten Standards definiert und sind erst in der Version von 2014

[3] Falls nicht anders angegeben, werden die Begriffe in ISO/IEC 27000 definiert [6].

an einer zentralen Stelle zusammengefasst. Viele wichtige Begriffsdefinitionen gehen zusätzlich auf ISO Guide 73 [7] zurück.

2.1.1 Mindmap und Definition wichtiger Begriffe

Mindmap

Die von der ISO für den Risikomanagement-Prozess wichtigen und auch formell eingeführten Begriffe sind in Abbildung 2 in einem Vorschlag für eine Mindmap dargestellt.

Als Ursprung dient der Begriff der Informationssicherheit, von dem aus zu den drei Punkten Werte, Informationssicherheits-Risiko-Management und Vorfall verzweigt wird. Die auch als Schutzziele der Informationssicherheit bezeichneten Begriffe Verfügbarkeit, Integrität und Vertraulichkeit finden sich bei den Werten und zu einem Vorfall gehören Bedrohungen, Schwachstellen, Ereignisse, Auswirkungen und Maßnahmen.

Abbildung 2: Mindmap zur Informationssicherheit mit den verwendeten Begriffen aus den Standards

Alle anderen Begriffe finden sich direkt unterhalb des Knotens Informationssicherheits-Risikomanagement. Die gezeigte Mindmap ist als Vorschlag zu verstehen. Es entspricht durchaus dem Ziel des Mindmappings, dass Sie sich bei Bedarf eine eigene Mindmap zeichnen, anhand derer Sie die Begriffe ordnen.

2.1.1.1 Oberbegriff Informationssicherheit

Information Security

Mit **Informationssicherheit** bezeichnen die Standards den Erhalt von Vertraulichkeit, Integrität und Verfügbarkeit. Darüber hinaus werden jedoch auch Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit unter dem Begriff zusammengefasst.

Information Security Management System

Ein **Managementsystem für Informationssicherheit ISMS** ist der Teil eines übergreifenden Managementsystems, der Informationssicherheit unter Berücksichtigung von Risiken

- ⇒ plant,
- ⇒ einrichtet, betreibt,
- ⇒ überwacht, überprüft,
- ⇒ aufrechterhält und verbessert[4].

Bestandteile dieses Managementsystems sind die Aufbauorganisation, Richtlinien, Planung, Verantwortlichkeiten, Verfahrensweisen, Prozesse und Ressourcen [4].

2.1.1.2 Werte

Asset

Als Asset wird alles bezeichnet, was für eine Organisation einen Wert hat [8]. Laut ISO/IEC 27000 gehören hierzu z.B. Bankdaten, geistiges Eigentum, Mitarbeiterdaten, oder Daten von Kunden. Vereinfacht handelt es sich also um die **Werte** der Organisation. Vielfach hört man jedoch auch den englischen Originalbegriff. Beide Begriffe sind möglich und erlaubt. Auch in diesem Buch werden sie synonym verwendet.

Availability

Verfügbarkeit ist die Eigenschaft, auf Verlangen einer berechtigten Entität zugänglich und nutzbar zu sein.

Integrity

Integrität ist die Eigenschaft, richtig und vollständig zu sein.

Confidentiality

Vertraulichkeit ist die Eigenschaft einer Information, niemals gegenüber einem unberechtigten Individuum, einer Entität oder

---

[4] Entsprechend den vier Phasen des Plan-Do-Check-Act-Zyklus (siehe Abschnitt 2.3.2 auf Seite 18).

einem Prozess verfügbar gemacht oder offengelegt wird. Vertraulichkeit beschränkt also die Verfügbarkeit.

2.1.1.3 Informationssicherheits-Risiko-Management

Risk

Als **Risiko** bezeichnet man Unsicherheiten bei der Erreichung der Ziele der Organisation. Risiko wird häufig als Kombination aus Wahrscheinlichkeit und Konsequenzen eines Ereignisses dargestellt.

Risk Management

Unter **Risikomanagement** versteht man die koordinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken.

External Context

Als **äußerer Kontext** wird das **Umfeld** verstanden, in dem eine Organisation arbeitet.

Internal Context

Als **interner Kontext** werden organisationsinterne Einflussgrößen bezeichnet.

Risk Assessment

Das **Risko-Assessment** bezeichnet den Prozess aus Risiko-Identifikation, Risikoanalyse und Risikobewertung/ Priorisierung.[5]

Risk Identification

Mit **Risikoidentifikation** bezeichnet man den Prozess, bei dem Risiken gesucht, aufgelistet und charakterisiert werden.

Risk Analysis

Risikoanalyse ist der Prozess, die Art des Risikos zu verstehen und das Risiko-Level zu bestimmen.

Risk Evaluation

Während der **Risikobewertung/ Priorisierung** (offizielle Übersetzung lautet nur Risikobewertung[6]) werden die zuvor identifizierten und analysierten Risiken mit den Basiskriterien abgeglichen, um deren Bedeutung bewertet.

Risk Treatment

Mit **Risikobehandlung** wird der Prozess bezeichnet, bei dem Maßnahmen ausgewählt und eingerichtet werden, die sich auf die Risiken auswirken.

---

[5] Hierbei handelte es sich in der Vergangenheit um einen der Fälle, wo die deutsche Übersetzung Missverständnisse aufwarf. In den aktuellen Standards ab 2011 wird der Begriff Risiko-Analyse anders verwendet. Eigentlich sollte das Wort *„assessment“* mit *„einschätzen“* oder *„abschätzen“* übersetzt werden, was zu Überschneidungen mit *„estimation“* führte und damit zu ziemlich gestelzten Übersetzungen.

[6] Gemäß Standard liegt am Ende dieses Schritts eine priorisierte Liste mit Risiken vor.

Unter **Risikomodifikation**[7] versteht man die Reduzierung der Wahrscheinlichkeit und/ oder der Konsequenzen eines Risikos [7]. Risk Modifikation

Unter **Risikoübernahme** versteht man gemäß [7] allgemein die Übernahme des Schadens oder des Gewinns, der sich aus einem Risiko ableitet. Im Kontext von Informationssicherheitsrisiken im Speziellen sollen jedoch nur Schäden berücksichtigt werden. Beachte: Risikoübernahme und Risikoakzeptanz bezeichnen unterschiedliche Aktivitäten im Prozessverlauf. Risk Retention

Die Entscheidung, sich einem Risiko gar nicht erst auszusetzen oder es durch Maßnahmen zu vermeiden, bezeichnet man als **Risikovermeidung** [7]. Risk Avoidance

Man spricht davon **Risiken zu Teilen**[8], wenn der mögliche Schaden eines Risikos mit einer anderen Organisation geteilt wird. Auch hier werden mögliche Gewinne – wie in [7] vorgegeben – nicht berücksichtigt. Risk Sharing

Das nach der Risikobehandlung verbleibende Risiko nennt man **Restrisiko**. Residual Risk

Risikoakzeptanz ist die Entscheidung ein bekanntes Risiko zu akzeptieren. Beachte: Risikoakzeptanz und Risikoübernahme bezeichnen unterschiedliche Aktivitäten im Prozessverlauf. Risk Acceptance

Unter **Risikokommunikation und Beratung** versteht man den Austausch von Informationen zu Risiken zwischen den Entscheidungsträgern und anderen Prozessbeteiligten. Risk Communication and Consultation

Bei der **Überwachung** geht es um die Bestimmung des aktuellen Status des Risikomanagementprozesses. Monitoring

Hierunter versteht man die **Überprüfung** der Eignung, Angemessenheit und Wirksamkeit des Risikomanagementprozesses. Review

2.1.1.4 Vorfälle

Eine mögliche Ursache für einen unerwünschten Vorfall, der negative Auswirkungen auf ein System oder die Organisation haben kann, wird als **Bedrohung** bezeichnet. Threat

---

[7] Früher: Risikoreduktion

[8] Früher: Risikotransfer

Vulnerability

Eine **Schwachstelle** bezüglich eines Werts oder mehrerer Werte, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann [8]. Auch im Deutschen wird vielfach von Vulnerabilities beziehungsweise von Vulnerability-Management gesprochen.

Information Security Event

Ein **Informationssicherheitsereignis** ist ein identifiziertes Ereignis, dass auf eines der folgenden Dinge hindeutet:

- ⇒ einen möglichen Bruch der Informationssicherheits-Leitlinie,
- ⇒ einen Fehler der Schutzmaßnahmen oder
- ⇒ eine bisher unbekannte Situation, die sicherheitsrelevant sein könnte.

Information Security Incident

Ein **Informationssicherheitsvorfall** besteht aus einem oder mehreren unerwünschten oder unvorhergesehenen Informationssicherheitsereignissen, die mit einer hohen Wahrscheinlichkeit eine Beeinträchtigung der Geschäftstätigkeit bedeuten oder die Informationssicherheit bedrohen.

Impact

Unter einem Impact versteht man die **Auswirkung** auf die erreichte Höhe der Unternehmensziele [5].

Control

Controls sind **Maßnahmen** zur Modifikation von Risiken. *„Control“*, *„Measure“*, *„Safeguard“* und *„Countermeasure“* werden in den Standards synonym als Begriff für Maßnahmen verwendet. Der englische Begriff **Control** wird immer dann empfohlen, wenn es um ein explizites Control aus einem Standard geht.

Also zum Beispiel beim Zitieren von Punkt 12.5.5 aus ISO/IEC 27002:

> *ISO/IEC 27002*
> ***12.5.5 Outsourced software development***
> *Control*
> *Outsourced software development should be supervised and monitored by the organization.*

Bei einem solchen Zitat geht es konkret um das dort beschriebene Control und nicht um die aufgrund dieser Anforderung konkret ergriffenen Maßnahmen.

2.2 Entscheidend ist die Methodik

Es geht um die Methodik…

Nachdem nun die wichtigsten Begriffe geklärt sind, können wir uns an die Arbeit machen und inhaltlich durchstarten. *„Inhaltlich“*, das bedeutet beim Thema Risikomanagement *„methodisch“*.

…nicht um die Details

Wie bei allen Managementthemen stehen Detailfragen im Hintergrund. Es geht nicht darum, wie die Firewall zu konfigurieren ist; es geht nicht darum, welchen Kriterien eine Virenschutzlösung entsprechen muss und es geht auch nicht darum, welche Skills ein Risikomanager mitbringen muss. Das wäre auch von Unternehmen zu Unternehmen viel zu unterschiedlich, als dass es sich lohnen würde, darüber Bücher zu schreiben. Man bräuchte für jede Branche, für jede Behördenform und für unterschiedlichste Organisationsgrößen jeweils ein eigenes Buch.

Der Weg ist das Ziel

Viel wichtiger ist die Frage, wie man zu diesen branchen-, behörden- und organisationsspezifischen Kriterien kommt. Wir werden es daher im Verlauf dieses Buchs immer mit Prozessen zu tun haben und nur selten mit Projekten. Das ist ein schwieriger Punkt, da heute fast alles in Projekten abgewickelt wird – sogar Prozesse. Im Zweifelsfall wird mit dem Projekt dann eben ein Prozess implementiert.

Projekte

Projekte verlaufen linear. Es gibt ein Anfang und ein Ende und dazwischen einen Projektplan. Die Projektbeteiligten befinden sich dabei an irgendeiner Stelle des Plans und schreiten dem Ende entgegen. Dabei kommt es vor allem darauf an, die Arbeitsschritte abzuschließen. (Abbildung 3).

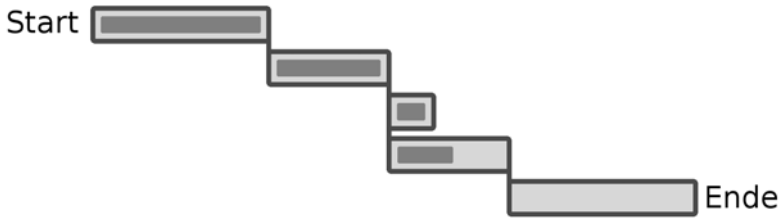


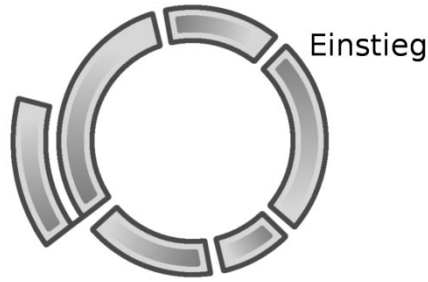
Abbildung 3: Einfacher Projektplan

Prozesse

Projektpläne sehen es nicht vor, einen Schritt immer wieder neu starten zu müssen. Der Unterschied bei Prozessen liegt darin, dass die einzelnen Schritte immer wieder gestartet werden und eigentlich permanent laufen und auf Input warten. Natürlich gibt es auch hier mindestens einen Einstiegspunkt, mit dem man beginnen kann. Das muss aber nicht sein. Es können auch mehrere

Einstiegspunkte sein oder man startet den Prozess quasi ausgehend von einer virtuellen Keimzelle und baut ihn nach und nach aus (Abbildung 4).

Abbildung 4: Beispiel für einen Prozess



Ausgehend vom Standpunkt einer üblichen Definition von Geschäftsprozessen ist das nicht ganz richtig. Dort werden Prozessbeschreibungen oft in der Art von Projektplänen verstanden, an deren Ende ein Pfeil zum Start eingezeichnet wird.

Risikomanagementprozess

Das kann im Sinne des Risikomanagements jedoch fatale Folgen haben. Stellen Sie sich vor, Sie würden ein sehr komplexes Risikomanagementsystem betreiben und auf diese Weise vorgehen und schaffen pro Jahr einen Prozessdurchlauf. Immer im Mai des Jahres überprüfen Sie zwei Wochen lang, ob es neue Bedrohungen für Ihr Informationssystem gibt. Ist das sinnvoll? Was machen Sie, wenn im Juni eine neue Bedrohung auftaucht? Warten Sie dann erst bis zum Mai des nächsten Jahres? Natürlich nicht. Man muss immerzu nach neuen Bedrohungen Ausschau halten und sofort reagieren, wenn sie auftauchen. In den Standards wird dieser Punkt unter dem Begriff *„Monitoring“* zusammengefasst.

Das Projekt „Einführung Risikomanagementprozess“

Der Risikomanagementprozess hat also gewisse Eigenschaften, die bei anderen Prozessen nicht so wichtig sind oder gar keine Relevanz haben. Will man die Etablierung eines Risikomanagements unbedingt als Projekt aufsetzen, so muss klar sein, dass an dessen Ende der Start des Prozesses steht. Gewissermaßen startet der Ingenieur am Ende der Entwicklungsphase den Motor.

http://www.springer.com/978-3-658-08773-9

Information Security Risk Management
Risikomanagement mit ISO/IEC 27001, 27005 und 31010
Klipper, S.
2015, XIV, 198 S. 28 Abb., Softcover
ISBN: 978-3-658-08773-9