FAKULTÄT FÜR !NFORMATIK

Vergleich von IT-Risikomanagement Tools anhand eines Business Cases

MASTERARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Masterstudium Wirtschaftsinformatik

eingereicht von

Chia-chang Lin
Matrikelnummer 0100745

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: O.Univ.Prof. Dipl.-Ing. Dr.techn. A Min Tjoa
Mitwirkung: Univ.Ass. Dipl.-Ing. Dr.techn. Mag.rer.soc.oec. Edgar Weippl

Wien, 23.09.2008 _____ _____
(Unterschrift Verfasser) (Unterschrift Betreuer)

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, 23.09.2008

Chia-chang Lin

Danksagung

An erster Stelle möchte ich mich an meine Familie bedanken für ihre Unterstützung während meiner ganzen Studienzeit. Ohne die Unterstützung der Familie habe ich das Masterstudium in Wirtschaftsinformatik nicht in zwei Jahre abschließen können.

Weiters bedanke ich mich bei Herrn Prof. Dr. Michael Huth von der Firma Hulocon GmbH für die Bereitstellung eines Testversions von Rimanis. Ein herzlicher Dank geht auch an Mag. (FH) Samuel Brandstätter, Geschäftsführer der avedos Business Solutions GmbH für die Bereitstellung eines Testzugangs für Risk2Value, auch wenn die Software nicht in die Evaluierung aufgenommen wurde aufgrund eines Fehlers von meiner Seite.

Ganz besonders möchte ich bei Herrn Rameder Stefan bedanken für die Unterstützung beim Korrekturlesen meiner Masterarbeit. Ohne seine Unterstützung wird das Korrekturlesen sicher viel länger dauern.

Abschließend möchte ich mich bei Andreas Tomek und Edgar Weippl für die Betreuung meiner Masterarbeit bedanken. Andreas Tomek und Edgar Weippl haben mir bei der Erstellung viele wertevolle Hilfe gegeben und zum Gelingen dieser Arbeit wesentlich beigetragen.

Kurzfassung

Das IT-Risikomanagement wird im Unternehmen oft durchgeführt und gewinnt aufgrund der rasanten Entwicklung im Bereich der Informationstechnologie immer mehr an Bedeutung. Die Unternehmen werden im IT-Bereich täglich von verschiedenen Gefahren/Risiken wie z.B. Spionage oder Hacker Angriffe ausgesetzt. Es ist daher notwendig, dass man die möglichen Risiken regelmäßig erfasst, bewertet, steuert und überwacht.

Die Masterarbeit ist in zwei Bereiche aufgeteilt: Der Theorieteil beinhaltet das Risikomanagement im IT-Bereich und die Evaluierung der Risikomanagement-Lösungen. Im ersten Teil wird zuerst die allgemeine Theorie im Risikomanagement vorgestellt. Dabei wird der Begriff Risiko beschrieben und auf die unterschiedlichen Kategorien von Risiko eingegangen. Außerdem wird auch der Risikomanagement-Prozess sowie einige dazugehörige Techniken vorgestellt. Anschließend werden einige Standards und Best Practice Ansätze kurz erklärt und einen Bezug zum IT-Risikomanagement hergestellt.

Im Evaluierungsteil sind insgesamt drei Softwareevaluierungen enthalten. Diese Software unterstützt das IT-Risikomanagement und basiert auf unterschiedliche Best Practice Ansätze. Der Schwerpunkt der Evaluierung liegt in der Unterstützung der Software im IT-Risikomanagement. Es kommt dabei nicht darauf an, welche Best Practice Ansätze das Programm unterstützt. Die Vorteile und Nachteile eines Best Practice Ansatzes spielen hier daher kaum eine Rolle.

Um die Evaluierung zu erleichtern, wurde ein Business Case erstellt. Im Business Case sind Informationen über den IT-Bereich eines fiktiven mittelständischen Unternehmens enthalten. Diese Informationen dienen als Ausgangspunkt für die Modellierung bei der Evaluierung. Der wichtigste Teil des Business Cases sind die Interviews mit den zuständigen Verantwortlichen des IT-Bereiches im fiktiven Unternehmen. Mit Hilfe des Interviews ist es möglich, den derzeitigen Prozessablauf zu erkennen sowie die derzeitige Vorgehensweise in verschiedenen Bereichen der IT zu identifizieren.

Neben dem Business Case wurde auch ein Katalog mit Evaluierungskriterien erstellt, um einen Anhaltspunkt bei der Evaluierung zu haben. Man muss hier dabei beachten, dass die evaluierten Risikomanagement-Produkte Softwareprogramme sind und Evaluierungsschwerpunkte analog zu den Qualitätskriterien einer Software gesetzt werden. Diese Schwerpunkte sind zum Beispiel die Softwarearchitektur oder die Bedienbarkeit der Software.

Die Zielsetzung der Arbeit ist nicht nur das Ergebnis der evaluierten IT-Risikomanagement-Software zu präsentieren, sondern die Arbeit zeigt auch, wie man eine IT-Risikomanagement Lösung evaluieren kann, egal auf welchen Standard oder Best Practice Ansatz das Programm basiert. Das Theorieteil über das IT-Risikomanagement gibt zusätzlich eine recht gute Einführung in die Materie und ist für Unternehmen interessant, die Interesse an der Einführung von IT-Risikomanagement haben.

Inhaltsverzeichnis

1. Einleitung

Im Privat- oder Berufsleben ist immer erforderlich Entscheidungen zu treffen, um dem Leben eine andere Wendung zu geben oder sich gegenüber negativen Konsequenzen abzusichern. Diese Entscheidungen stehen oft mit unterschiedlichen Ereignissen in Verbindung. In vielen Fällen geschieht es aber auch, dass unerwartete Ereignisse eintreten und wir als Menschen darauf rasch reagieren müssen, um keine Nachteile im Leben zu erfahren. Jede Entscheidung birgt aber auch ein Risiko, da wir die Folgen unseres Handelns nicht immer genau einschätzen können. Genauso verhält es sich mit dem Risikomanagement von IT-Systemen. Um sich abzusichern, sind gewisse Entscheidungen erforderlich, um einen Schaden oder größeren Verlust gering zu halten.

Carl Amery, ein deutscher Schriftsteller hat einmal gesagt:

Risiko ist die Bugwelle des Erfolgs.

Das bedeutet, dass die Risiken nicht nur Gefahren bringen, sondern auch Chancen, die zum Erfolg eines Unternehmens führen. Dabei spielt das Risikomanagement eine entscheidende Rolle. Es ist ein Verfahren zur Bewertung, Erfassung und Steuerung von Risiken. In dieser Arbeit wird das Thema IT-Risikomanagement behandelt.

Das Risikomanagement im Bereich IT gewinnt immer mehr an Bedeutung. Angesichts der zunehmenden Bedrohung durch Hacker, Saboteure und Computerviren wird die IT-Sicherheit immer bedeutender. (Junginger, et al., 2004) Es ist daher wichtig IT-Risikomanagement einzuführen, um dazu eine passende IT-Sicherheitsstrategie zu entwickeln, um die Wahrscheinlichkeit eines Risikoeintritts zu minimieren bzw. den Schaden bzw. Verlust nach einem Risikoeintritt zu minimieren.

Zurzeit gibt es auf dem Markt verschiedenen Anbieter von Software-Lösungen, die IT-Risikomanagement bzw. Compliance Management unterstützten. Durch die Anwendung dieser Lösungen ist eine Reduktion des Aufwands im Bereich des IT-Risikomanagements bis zu 50% vorstellbar. Die Architektur und die Funktionalitäten der Softwarelösungen variieren jedoch sehr stark, sodass vor der Anschaffung eine sorgfältige Evaluierung notwendig ist. Eine Möglichkeit der Evaluierung ist die Modellierung anhand eines Business Cases und der anschließende Vergleich der Ergebnisse. Bei der Modellierung ist es möglich, die Managementtechniken der Softwarelösungen zu bewerten und anhand des Modellierungsergebnis-

ses kann man feststellen, ob die Software den gewünschten Anforderungen des Unternehmens entspricht.

Contribution

Der Beitrag dieser Masterarbeit ist nicht nur einfach eine Evaluierung der IT-Risikomanagement Tools und eine anschließende Präsentation der Ergebnisse. Neben der Durchführung der Softwareevaluierung soll aber auch die Kernfrage beantwortet werden, wie man ein IT-Risikomanagement-Tool evaluieren kann. Die Bewertung solcher Tools ist nicht sehr einfach, da es keinen einen einheitlichen Standard für das IT-Risikomanagement gibt. Das IT-Risikomanagement oder ein Teil orientiert sich jedoch an verschiedenen Informationssicherheitsstandards oder Best Practice-Ansätzen wie .z.B. EBIOS oder ITIL.

Die meisten Risikomanagement Tools basieren auf einen Best Practice Ansatz oder auf eine eigene Methode eines Software-Anbieters, die von ihm selbst entwickelt wurde. Es gibt eher wenige Tools, die auf den allgemeinen Risikomanagement-Prozess basiert. Es ist nicht die Absicht dieser Masterarbeit, die Vor- und Nachteile eines Standards oder eines Best Practice Ansatzes zu beurteilen. Der Schwerpunkt des Evaluierungsteils in der Arbeit beschäftigt sich mit der Frage, wie gut das Programm die darauf basierten IT-Risikomanagement Ansätze unterstützt.

Das Theorieteil über das IT-Risikomanagement gibt zusätzlich eine recht gute Einführung in die Materie und ist für Unternehmen interessant, die Interesse an der Einführung von IT-Risikomanagement haben.

2. Definition von IT-Risikomanagement

Bevor man mit dem Thema bzw. Begriff IT-Risikomanagement beschäftigt, soll man sich erst mit dem Begriff Risiko auseinandersetzen. Von diesem existieren noch verschiedene Definitionen. Eine allgemeine Definition gibt es jedoch nicht. Je nach Betrachtung und Rahmenbedingungen in dem Risikomanagement werden unterschiedliche Anforderungen an den Risikobegriff gestellt. In dieser Arbeit ist der Begriff Risiko aus Sicht der Informationstechnologie von Relevanz.

Risiko ist die Möglichkeit (Wahrscheinlichkeit) einer Abweichung des tatsächlichen Ergebnisses vom erwarteten Ergebnis. Diese Abweichung kann positiv oder negativ sein. Bei negativen Abweichungen besteht die Gefahr, dass unerwünschte Ergebnisse eintreten (z.B. Verluste) oder die Gefahr, dass erwünschte Ergebnisse nicht eintreten (z.B. verpasste Chancen). Positive Risiken (Chancen) drücken sich durch ein Eintreten unerwartet positiver Ergebnisse aus. (Seibold, 2005 S. 10)

Der obige Absatz versucht, den Begriff Risiko allgemein zu definieren. Man erkennt, dass man den Begriff Risiko mit Verlust bzw. Chancen beschreibt. Die beiden Begriffe sind sehr nah miteinander verbunden und man kann davon ableiten, dass das Risiko weder gut noch schlecht ist. Diese Aussage kann man als die wichtigste Botschaft des Risikomanagements verstanden werden.

Ein Risiko aus der Sicht der Informationstechnologie bezeichnet man als IT-Risiko. Unter dem Begriff IT-Risiko versteht man die Unfähigkeit, anforderungsgerechte IT-Leistungen effektiv und effizient erbringen zu könne. IT-Leistungen sind dabei der Betrieb und die Entwicklung von Systemlösungen, das Projektmanagement sowie das Management dieser Leistungen und die Beratung der Fachbereiche für deren Geschäftstätigkeit (Seibold, 2005 S. 11)

Wie bei dem Begriff Risiko gibt es auch verschiedene Definitionen vom Begriff Risikomanagement. Jeder Mensch praktiziert aktiv Risikomanagement täglich unbewusst. Ein simples Beispiel: Beim Verlassen der Wohnung wurde festgestellt, dass der Himmel bewölkt ist und folglich das Wetter nicht einschätzbar ist. Sicherheitshalb nimmt man einen Regenschirm mit. Dadurch ist man vor dem natürlichen Risiko geschützt, nass zu werden, falls es zu regnen anfängt. Wenn man keinen Regenschirm mitnimmt und es fängt an, zu regnen, dann muss man mit durchnässter Kleidung bzw. mit einer Erkältung rechnen.

Man bezeichnet das Beispiel oben als Risikomanagement im Alltag. Jeder praktiziert es unbewusst und täglich. Ein komplexes Managementsystem dafür aufzustellen ist notwendig, da wir gelernt haben mit dem Risiko umzugehen. (Ahrendts, et al., 2008 S. 8) Daraus abgeleitet kann man Risikomanagement so definieren:

Risikomanagement ist ein Verfahren der Umgang mit den Risiken.

Risikomanagement im Bereich Informationstechnologie ist jedoch viel komplizierter als Risikomanagement im Alltag. Ein komplexes Managementsystem ist notwendig, um mit allen Risiken umgehen zu können, die man bisher noch gut gelernt hat.

Beim IT-Risikomanagement unterscheidet man zwischen strategischem und operativem Risikomanagement. Das strategische Risikomanagement beinhaltet die Grundsätze zur Behandlung von Risiken, die Risikokultur sowie die Methodik. (Seibold, 2005 S. 11) Das operative Risikomanagement ist ein sich wiederholender Prozess, der aus folgenden Komponenten besteht:

- Identifizierung von Risiken sowie deren Klassifizierung
- Bewertung und Aggregation von Risiken
- Maßnahmen der Risikobewältigung festlegen und durchführen
- Überwachung der Risiken

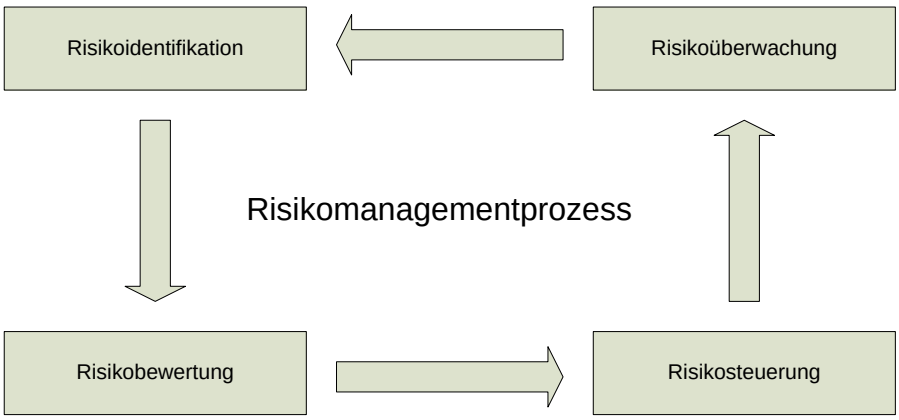


Abbildung 1: Risikomanagement Prozess, vereinfachte Darstellung

Am Beginn des Risikomanagementprozesses steht die Identifikation von Risiken. Vor der Risikoidentifikation soll zuerst der zu beobachtende Rahmen (Systemgrenze) festgelegt werden. Nach der Festlegung erfolgt anschließend die Erkennung von Risiken. Nach der Risikoidentifikation werden diese möglichst genau analysiert, um anschließend eine vollständige

Bewertung und Beschreibung erstellen zu können. An die Risikoanalyse schließt die Risikosteuerung an. In der Risikosteuerung werden Maßnahmen aufgrund der ermittelten Grundlagen in der Risikoanalyse erstellt. Die letzte Komponente des Risikomanagementprozesses ist die Risikoüberwachung. Hier wird mittels Risikoindikatoren überwacht, ob die Risiken noch evident sind oder sich verändert haben. Der Risikomanagement-Prozess wird später noch im einen eigenen Kapitel ausführlicher behandelt.

3. Die Mythen des IT-Risikomanagements

Es gibt verschiedene Mythen von IT-Risikomanagement. Um diese Mythen zu finden, hat die Firma Symantec Corporation über 400 IT-Fachleuten weltweit befragt und im Jänner 2008 den zweiten Band des IT-Risikomanagement Report (Symantec Corporation, 2008) veröffentlicht. Im Bericht wurde insbesondere vier Mythen erwähnt:

- IT-Risiko ist IT-Sicherheitsrisiko
- IT-Risikomanagement ist ein Projekt
- IT-Risiken könne mittels Technologie verhindert werden
- IT-Management ist eine Wissenschaft

Sehr häufig werden die Begriffe IT-Risiko und IT-Sicherheitsrisiko gleichgesetzt. Es existiert zwar ein direkter Zusammenhang zwischen IT-Security und IT-Risikomanagement, man sollte jedoch diese beiden Begriffe nicht gleichsetzten oder behaupten, dass IT-Risiken generell IT-Sicherheitsrisiken sind. Wer dies jedoch tut, kann mit einer sehr hohen Wahrscheinlichkeit unangenehme Überraschungen wie z.B. Systemfehlern oder Unterbrechungen im Geschäftsbetrieb erleben.

Die meisten IT-Experten, die an der Befragung teilnahmen, sind sich jedoch bewusst, dass die IT Risiken mehr umfassen als die IT-Sicherheitsrisiken. Im Bericht wurden die Experten über die Wichtigkeit der Risiken im Bereich Informationstechnologie befragt. Dabei erfolgt eine Beurteilung der Wichtigkeit von vier IT-Risikoarten (Sicherheit, Verfügbarkeit, Compliance und Performance) anhand von vier unterschiedlichen Wichtigkeitsstufen (Business Critical, Serious Risk, Some Risk und Minimal Risk). Folgende Abbildung zeigt das Ergebnis der Befragung dar.

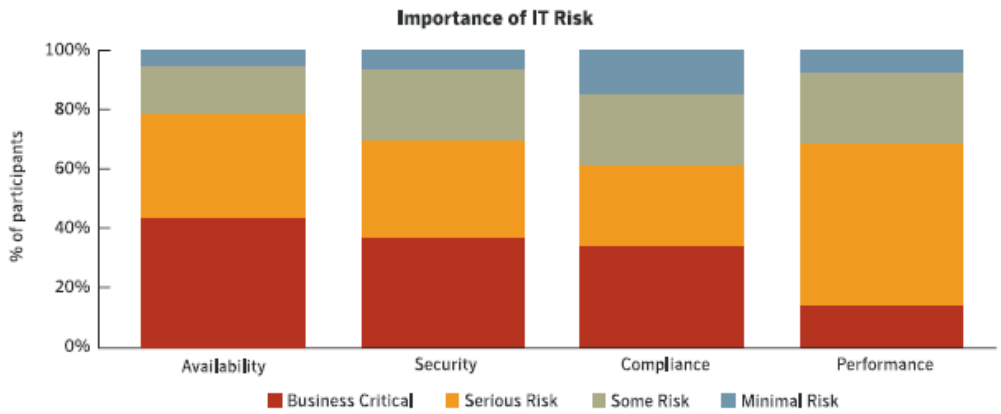


Abbildung 2: Wichtigkeitsbewertung von IT-Risiken (Symantec Corporation, 2008 S. 10)

Laut Bericht schätzen 78 Prozent der Befragten die Risiken über die Verfügbarkeit eines Systems kritisch oder schwerwiegend ein. Es kann somit als das wichtigste Risiko in der IT angesehen werden. Andere Risiken sind von den Befragten ebenfalls als sehr hoch eingestuft worden (Security 70 Prozent, Performance 68 Prozent, Compliance 63 Prozent). Wie man aus den Zahlen erkennt, liegen die Risiken nur 15 Prozent auseinander. Man kann deshalb daraus schließen, dass die Einstufung der Wichtigkeit recht ausgewogen ist. Viele Unternehmen erkennen, dass nicht nur die Sicherheits-Risiken im IT-Risikomanagement wichtig sind, sondern auch Risiken in den Kategorien Verfügbarkeit, Leistungsfähigkeit und Compliance.

Ein weiterer Mythos des IT-Risikomanagements (RM) ist die Aussage, dass das IT-Risikomanagement als ein einzelnes Projekt gehandhabt werden kann. Im vorherigen Kapitel wurden das IT Risikomanagement sowie der RM Prozess kurz vorgestellt. Ein Projekt ist ein einmaliges Vorhaben auf Zeit und hat einen Endzeitpunkt. Daher ist die Aussage, dass IT-Risikomanagement ein Projekt ist falsch, da ein RM Prozess nie ein Ende hat, was bei einem Projekt durchaus gegeben ist. Das IT-Risikomanagement soll daher als ein laufender Prozess verstanden werden, der mit einer Umgebung (Unternehmen), die sich ständig verändert, Schritt halten muss.

Die obige Aussage kann man ebenfalls durch das Ergebnis des Risikomanagementberichts widerlegen, ohne genau ins Detail zu gehen. Der Bericht zeigt, dass 69 Prozent der Befragten jeden Monat mit einer kleineren IT-Störung, 63 Prozent jedes Jahr mit einem schwerwiegenden IT-Ausfall rechnen. Ferner ändert sich das Umfeld des Risikomanagements ständig, so dass eine regelmäßige Risikoeinschätzung erforderlich ist.

Auch wenn Technologie eine entscheidende Rolle bei der Abfederung von IT-Risiken spielt, steht und fällt das IT-Risikomanagement mit den Personen und Prozessen, die involviert sind. Nach den Ergebnissen des aktuellen Reports sind 53 Prozent der IT-Störungen auf Prozesse im Unternehmen zurückzuführen. (Symantec Deutschland GmbH, 2008)

Die nächste Abbildung zeigt die Ursachen für IT-Störungen. Auf Platz eins sind, wie bereits erwähnt, Störungen, die auf Prozesse im Unternehmen zurückzuführen sind. Danach folgen Störungen, die aufgrund der Konfiguration in der Umgebung zurückzuführen sind. 41 Prozent der Störungen wurden durch mangelnde Fähigkeiten der Mitarbeiter verursacht. Die Summe der Ursachen ist größer als 100 Prozent da eine Störung mehrere Ursachen haben kann.

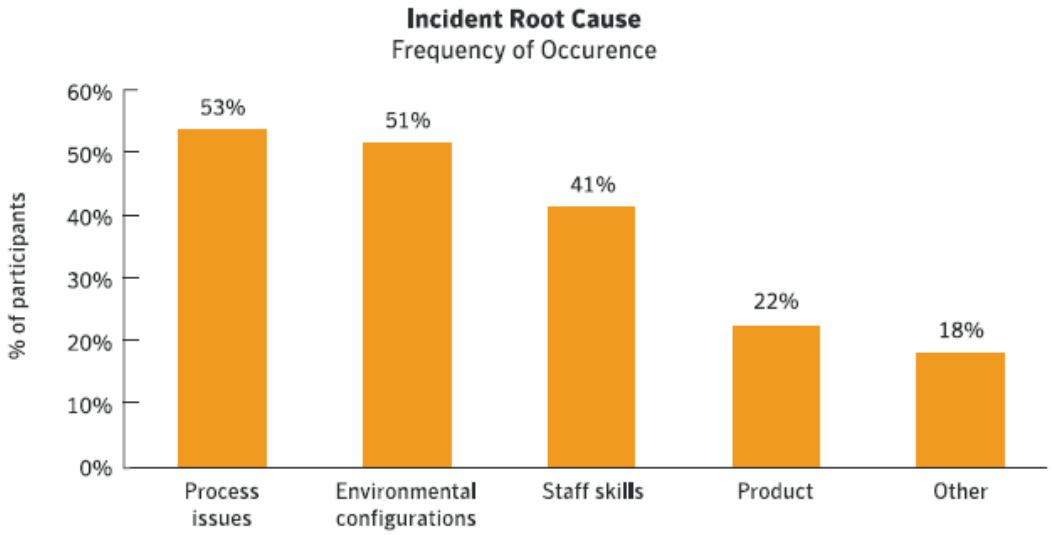


Abbildung 3: Ursache der IT-Zwischenfälle (Symantec Corporation, 2008 S. 30)

Aufgrund von Umfrageergebnisse und weitere Untersuchungen ist die Firma Symantec der Ansicht, dass IT-Risikomanagement eine Business Disziplin ist und keine eigene Wissenschaft. Wissenschaft hat mit Forschung und Experimente zu tun, was im Bereich des RM nicht gegeben ist.

4. Klassifizierung von Risiken

Im Kapitel zwei wurde definiert, was ein Risiko ist. Die Risiken lassen sich noch detaillierter in verschiedenen Kategorien aufteilen. Durch die Kategorisierung von Risiken wird das Zusammenfassen von gleichartigen Risiken und somit die Beherrschbarkeit dieser Risiken mittels gemeinsamer oder ähnlicher Risikoindikatoren und Risikoreduzierungsmaßnahmen ermöglicht. (Seibold, 2005 S. 15) Es gibt viele Möglichkeiten die Risiken zu kategorisieren. Üblicherweise werden sie jedoch in folgende Kategorie aufgeteilt:

- Ursache und Wirkung
- Zeiträume
- Eigenschaft

4.1. Kategorisierung nach Ursache und Wirkung

Die Risiken kann man unterteilen in ihrer Ursache sowie in ihrer Wirkung. Die Unterscheidung hinsichtlich der Risikoursache kann man z.B. am IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik Deutschland orientieren. In den IT-Grundschutz-Katalogen werden die Risikoursachen in höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technische Versagen und vorsätzliche Handlungen unterteilt. Eine andere Unterteilung der Risikoursache ist z.B. die Risikokategorie nach VÖB (Verband öffentlicher Banken).

Im Allgemein kann man die Ursachen eines Risikos unterteilen in

- Mensch,
- Technologie,
- Organisation,
- externe Einflüssen und höhere Gewalt.

Die Kategorie Mensch beinhaltet nur Risiken, die direkt einer Person zugeordnet werden können wie z.B. menschliches Versagen oder gesetzwidrige Handlungen. Ein Mensch ist nicht eine Maschine und macht Fehler. Menschliche Fehlhandlungen spielen daher eine wichtige Rolle bei der Risikoursache. Der Risikotreiber für Fehlverhalten im menschlichen Bereich sind Faktoren wie z.B. Motivation oder Ausbildungsstand. Ein Mitarbeiter ist nicht an der Ausübung seiner Tätigkeit interessiert, wenn er gering oder gar nicht motiviert ist. Folglich führt es zur Unachtsamkeit, die wiederum zu einer menschlichen Fehlhandlung führt. Die

Ausbildung ist hier ebenfalls ein Risikotreiber. Wenn man einen Mitarbeiter an eine Stelle einsetzt, für die laut Stellenbeschreibung nicht geeignet ist, kann dies zu falschen oder sogar gesetzwidrigen Handlungen führen.

Die Kategorie Technologie birgt Risiken aus der Informationstechnologie, welche durch fehlerhafte Verarbeitung oder mangelnde Verfügbarkeit entstehen können. Außerdem beinhalt sie auch Risiken über die technische Infrastruktur eines Unternehmens wie z.B. die Versorgung von Strom, Wasser oder Gas. Die Risikotreiber in dieser Kategorie sind z.B. die hohe Komplexität eines Systems oder Kosteneinsparungen bei der Wartung aufgrund des finanziellen Drucks. Im IT-Risikomanagement spielen die Risiken in der Technologie eher eine weniger bedeutende Rolle, da sie nur ein Teil von IT-Risiken abdeckt. Die meisten Risiken im Bereich IT sind in der Kategorie Mensch zu finden und werden als Anwender-IT-Risiken bezeichnet, weil sie durch Anwender, also dem Menschenverursacht werden.

Die Kategorie Organisation beinhaltet alle Risiken, die mit dem Aufbau bzw. mit den Geschäftsprozessen eines Unternehmens zu tun haben. Die typischen Risikotreiber in dieser Kategorie sind die Schwäche in den Prozessen wie z.B. eine unvollständige Prozessdefinition, unzureichende Kontrollmechanismen oder mangelnde Rollendefinitionen. Das Nichtvorhandensein eines Prozesses (z.B. Nichtdurchführung von IT-Risikomanagement) soll man ebenfalls als einen Risikotreiber einzustufen.

Die höhere Gewalt ist ein von außen einwirkendes, nicht vorhersehbares und nicht beeinflussbares Ereignis. Selbst bei bester Sorgfalt kann der Betroffene solche Ereignisse nicht abwenden. Die Beispiele für höhere Gewalt in der Natur sind z.B. Überschwemmung, Erdbeben oder Orkan. Beispiele für höhere Gewalt im Betrieb sind z.B. Personalausfall, Totalausfall des IT Systems usw. Die höhere Gewalt ist ein Teil der Risikoursache „Externe Einflüssen“. Sie treten jedoch meistens nur mit einer geringen Eintrittswahrscheinlichkeit auf. Viel wichtiger sind Risikoursachen wie Betrug, Sabotage oder rechtliche Gegebenheiten wie z.B. die Gesetzgebung sowie deren Auslegung.

Falls ein Risikofall eintritt, hat er unterschiedliche Auswirkungen, positiv oder negativ, auf das Unternehmen. Daher können die Risiken nach ihrer potentiellen Auswirkungen unterschieden werden. Nach Seibold (Seibold, 2005 S. 18-19) werden drei Arten nach der Kategorie Auswirkung unterschieden:

- Monetäre Risiken/Effizienzrisiken
- Qualitative Risiken

- Image-Risiken

Die monetären Risiken wirken sich direkt auf das Gewinn-und-Verlust (GuV) Konto der Buchhaltung aus. Beim Eintritt eines monetären Risikos geht der Gewinn für das Unternehmen verloren oder es findet ein erhöhten Verlust statt. Die Abschreibung eines Gerätes aufgrund eines Schadens innerhalb der Nutzungsdauer wirkt sich ebenfalls auf den Erfolg des Unternehmens aus. Beispiel für ein monetäres Risiko ist. die frühzeitige Abschreibung eines Geräts aufgrund einer Fehlbedienung eines Mitarbeiters.

Bei den Qualitativen Risiken drückt sich der Schaden ein einer verringerten Leistung aus. Dies kann in einem geringeren quantitativen oder qualitativen Umfang bestehen. (Seibold, 2005 S. 19)

Das Ausmaß der Image-Risiken ist sehr schwierig zu quantifizieren. Falls solches Risiko eintritt, hat es eine Auswirkung auf die Reputation eines Unternehmens. Die öffentliche Meinung über das gesamte Unternehmen ändert sich, obwohl nur ein Teil des Unternehmens davon betroffen ist. Ein gutes Beispiel für die Image-Risiken ist die Liechtensteiner Steueraffäre, obwohl man sie nicht direkt mit dem IT-Risikomanagement im Zusammenhang bringen kann. Der Bundesnachrichtendienst kaufte für mehrere Millionen die Kundendaten der liechtensteinischen IGT Bank und startet anschließend einige Ermittlungsverfahren wegen Steuerhinterziehung, die dann für großes Aufsehen sorgte. Die Liechtensteiner Steueraffäre ist das größte bisher in der Bundesrepublik Deutschland eingeleitete Ermittlungsverfahren wegen Steuerhinterziehung. Durch die Steueraffäre hat die Bevölkerung jetzt eine andere Meinung vom Finanzplatz Liechtenstein und die Schäden dadurch sind kaum abzuschätzen.

Die Tabelle unten fasst noch einmal alle Risiken in der Kategorisierung nach Ursache und Prinzip zusammen.

Einteilung nach Ursache	Einteilung nach Wirkung
Menschliches Versagen	Monetäre Risiken
Technische Risiken	Effizienzrisiken
Organisatorische Risiken	Qualitative Risiken
Externe Einflüssen und höhere Gewalt	Image-Risiken

Tabelle 1: Kategorisierung der Risiken nach Ursache und Wirkung

4.2. Kategorisierung nach Zeit

Eine andere Möglichkeit der Risikokategorisierung ist die Einteilung der Risiken nach Zeit. Dabei werden sie eingeteilt nach der Dauer der Relevanz. Die Einteilung kann dabei frei erfolgen, jedoch werden sie normalerweise in drei Kategorie unterteilt: kurzfristige, mittelfriste und langfristige Risiken.

Die langfristigen Risiken sind meistes immer von Relevanz und ein schneller Wegfall eines solchen Risikos ist nicht zu erwarten. Die Beispiele für langfristige Risiken sind entweder das Risiko einer Sabotage oder das Risiko eines Terroranschlags. Diese Risiken kann man nie ausschließen und sie bleiben daher dauerhaft relevant. Das Potential eines Risikos variiert über den Risikolebenszyklus mit einer sehr hohen Wahrscheinlichkeit. Die Variation des Risikopotentials kann man mit einem Beispiel sehr einfach darstellen: Die Wahrscheinlichkeit eines Terroranschlags sinkt wenn ein hohes Mitglied der Terrororganisation gefasst wurde. Nach einiger Zeit reorganisiert sich die Terrororganisation und ihre Handlungsfähigkeit steigt wieder. Die Wahrscheinlichkeit eines Anschlags steigt daher wieder nach oben.

Die Kategorie mittelfristiger Risiken beinhaltet alle Risiken, die das Ende bzw. der Wegfall des Risikos vorhersehbar ist. Sie fängt alle Risiken ab, die nicht zu den Kategorien langfristige und kurzfristige Risiken gehören. Das Potential eines Risikos variiert über den Risikolebenszyklus variieren, jedoch mit einer niedrigeren Wahrscheinlichkeit als bei den langfristigen Risiken. Beispiele für mittlere Risiken sind die Risiken eines Projekts oder Gewährleistungsrisiken aufgrund der Gewährleistung.

Risiken, die spontan auftreten oder eine sehr kurze „Lebensdauer“ haben, gehören zur Kategorie kurzfristige Risiken. Sie beziehen sich zumeist auf einmalige Situationen, die sich oftmals erst kurzfristig ergeben und schwierig vorauszusehen sind. (Seibold, 2005 S. 20) Beispiele für kurzfristige Risiken sind unter anderem plötzlicher Stromausfall, kurzfristig steigende Bedarf an Ressourcen usw. Da sie meistens spontan auftreten, werden sie meistens durch Improvisation gemanagt.

Eine andere Möglichkeit der Kategorisierung nach Zeit ist die Verknüpfung der Risiken mit den Unternehmenszielen. Die Ziele eines Unternehmens kann man unterteilen in strategische und operative Ziele. Strategische Ziele sind langfristige Ziele des Unternehmens wie z.B. „*Wir sollen in fünf Jahren europäische Marktführer werden“* oder *„In fünf Jahren werden wir die umweltfreundlichste IT-Unternehmens sein“*. Die operativen Ziele sind kurzfristig und können innerhalb eines kurzen Zeitraums erreicht werden.

Um die Ziele eines Unternehmens zu erreichen, müssen Entscheidungen getroffen werden. In der Einleitung wurde bereits erwähnt, dass Entscheidungen zu Risiken führen. Um strategische Ziele eines Unternehmens zu erreichen, werden strategische Entscheidungen getroffen. Die Risiken bei solchen Entscheidungen sind daher lang- bzw. mittelfristig und decken die Kategorie langfristige Risiken und zum Teil die der mittelfristigen Risiken ab. An den Beispielen von strategischen Zielen erkennt man, dass sie ziemlich abstrakt formuliert sind. Um die strategischen Zielen zu erreichen, werden daher operative Ziele formuliert. Operative Ziele führen zu Entscheidungen, die operative Risiken beinhalten. Die operativen Risiken decken die Kategorie kurzfristige Risiken und ein Teil der mittelfristigen Risiken ab.

Die untere Abbildung fasst die beiden Möglichkeiten der Risikoeinteilung nach Zeit sowie deren Beziehungen noch einmal zusammen.

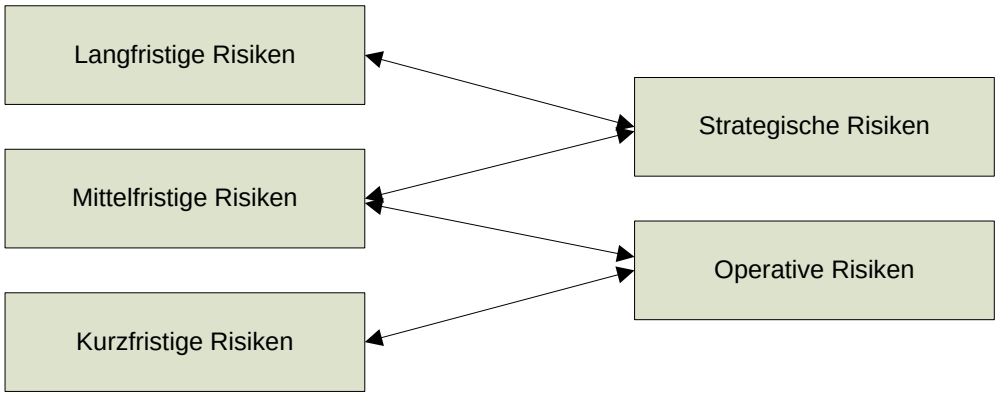


Abbildung 4: Einteilung der Risiken nach Zeit

4.3. Kategorisierung nach Eigenschaften

Ein Risiko hat verschiedene Eigenschaften, daher ist eine Einteilung nach Risikoeigenschaften durchaus sinnvoll. Die Risiken können zum Beispiel unterteilt werden in

- Eintrittswahrscheinlichkeit,
- Höhe der Schaden,
- Schadensverlauf und
- Risikotransparenz.

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt wie oft ein Risiko in einem bestimmten Zeitraum auftritt. Dabei soll man diese nicht mit der Kategorisierung nach der Zeit ver-

wechseln. Die Kategorisierung nach Zeit beschreibt, wie lange ein Risiko von Relevanz ist bzw. wann ein Ende absehbar ist. Die untere Tabelle stellt eine mögliche Einteilung der Risiken nach Eintrittswahrscheinlichkeit dar.

Risikoklasse	Eintrittswahrscheinlichkeit
Sehr häufig	Einmal pro Woche oder häufiger
Häufig	Einmal pro Monat
Selten	Einmal pro Jahr
Sehr selten	Einmal in 5 Jahren oder seltener

Tabelle 2: Kategorisierung nach Eintrittswahrscheinlichkeit

Falls ein Risiko eintritt, verursacht es auch Schaden. Die Tabelle unten zeigt eine mögliche Einteilung der Risiken nach den Schadensaumaß.

Risikoklasse	Schadensausmaß
sehr gering	bis € 1.000
gering	€ 1.000 bis € 10.000
mittel	€ 10.000 bis € 100.000
groß	€ 100.000 bis € 1.000.000
katastrophal	über € 1.000.000

Tabelle 3: Risikoeinteilung nach Schadensausmaß

Eine weitere Möglichkeit der Kategorisierung der Risiken nach ihren Eigenschaften ist die Einteilung über den Verlauf der Schäden nach dem Risikoeintritt. Die Abbildung auf der nächsten Seite stellt zwei Arten von Schadensverläufe dar: rasanter und schleichender Schadensverlauf.

Anhand der Abbildung erkennt man beim rasanten Schadensverlauf deutlich, dass die kumulierte Schadenshöhe bereits nach dem Eintritt des Schadensereignisses sehr hoch ist und den größten Teil des Gesamtschadens bildet. Danach steigt die kumulierte Schadenshöhe nur noch im geringen Ausmaß. Als Beispiele für solche Schadensverläufe können. Stromausfälle oder Brandunfälle angeführt werden.

Falls die kumulierte Schadenshöhe nach dem Eintritt des Schadensereignisses gering ist und mit der Zeit immer mehr steigt, spricht man vom schleichenden Schadensverlauf. Wenn

man bereits am Anfang wirkungsvolle Maßnahmen einsetzt, wird der Schadensverlauf beeinflusst und die Höhe der Schäden bleibt niedrig. Bleibt der Schaden jedoch unentdeckt oder wird ignoriert, kann der Schaden eine enorme Auswirkung haben. Beispiele von Risiken mit schleichenden Schadensverläufen findet man sehr oft im Projekte. Ein Fehler beim Design im einen Softwareprojekt kann enormen Schaden verursachen, falls er unentdeckt bleibt. Dieser Fehler erst in der letzten Projektphase zu beheben würde erhebliche Kosten verursachen und das Projektergebnis verändern oder sogar das Projekt zum Scheitern bringen.

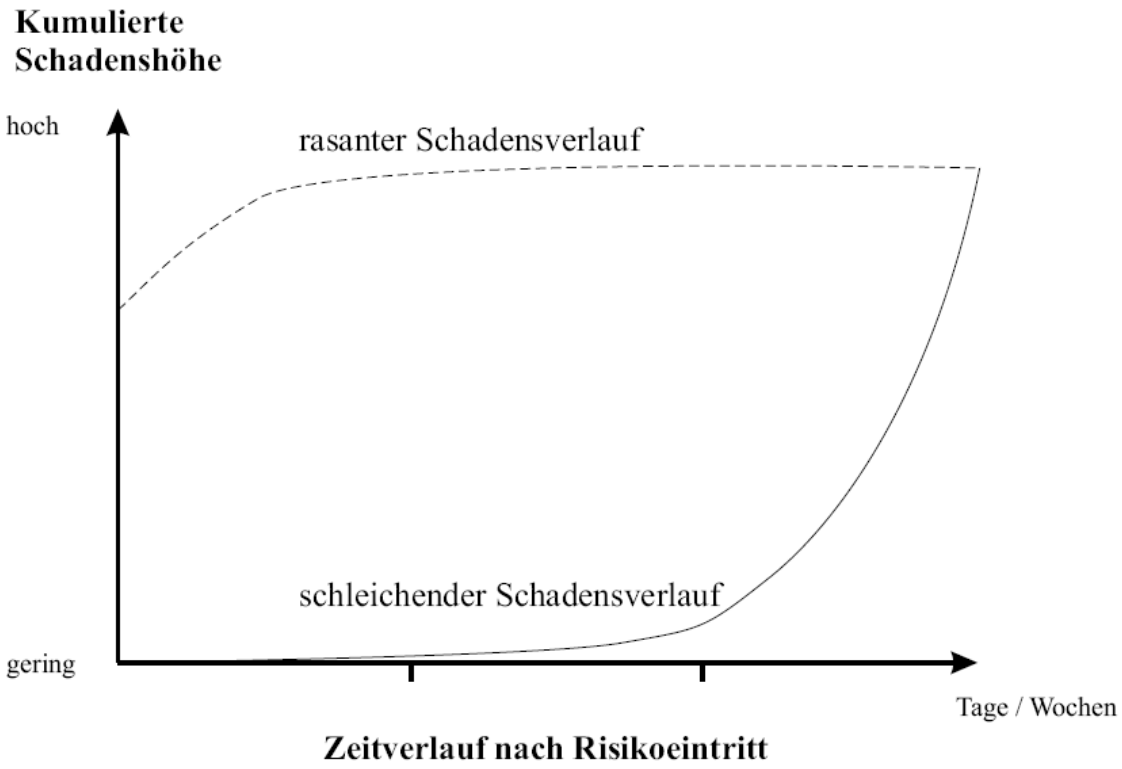


Abbildung 5: Schadensverläufe für Risikokategorisierung (Seibold, 2005 S. 24)

Die Klassifizierung der Risiken bezüglich Risikotransparenz kann grundsätzlich erst in der Nachschau erfolgen. Der Sinn dieser Einteilung liegt in der Qualitätssicherung des eigenen Risikomanagements. (Seibold, 2005 S. 24) Bei der Kategorisierung nach Risikotransparenz unterscheidet man drei Arten von Risiken:

- Unerkannte Risiken,
- Versteckte Risiken und
- Erkannte Risiken.

Unter der Kategorie „Unerkannte Risiken“ findet man Risiken, die man beim Risikoidentifizierungsprozess nicht entdeckt hat. Folglich werden diese Risiken nicht gemanagt und trifft das

Unternehmen vollkommen unvorbereitet. Falls ein solches Risiko eintritt, wird meistens improvisiert, um den Auswirkungen entgegenzuwirken.

Versteckte Risiken wurden bei der Risikoanalyse nicht oder nicht im gesamten Umfang als eigenständige Risiken identifiziert bzw. deren Risikopotential deutlich fehlgeschätzt. Deshalb wurden keine konkreten oder in der Wirkung nicht ausreichenden, adäquaten Risikoreduzierungsmaßnahmen abgeleitet. Diese Risiken sind zumeist Teile anderer Risikoszenarien. (Seibold, 2005 S. 25)

Erkannte Risiken sind Risiken, die bei der Risikoinventur vollständig erfasst, bewertet und anschließend ihrer Bedeutung angemessen gemanagt wurden. Diese Risiken sind aus Risikomanagementsicht unproblematisch, da sie beeinflusst werden können. Das Restrisiko nach Steuerung dieser Risiken wird bewusst akzeptiert. (Seibold, 2005 S. 25)

Nach der Einteilung der Risiken nach Risikotransparenz kann man die Wirksamkeit des vorhandenen Risikomanagement (RM) Systems beurteilen. Falls die Anzahl der unerkannten und verstecken Risiken hoch ist, muss man sich Gedanken über die Verbesserung des Risikomanagementprozesses machen. Die Anzahl solcher Risiken soll so gering wie möglich sein.

5. Risikomanagement Prozess

Der Risikomanagement Prozess (RM-Prozess) ist das Kernstück eines Risikomanagementsystems. Dieser Prozess kann je nach dem Tätigkeitsbereich eines Unternehmens angepasst werden. Generell kann man den RM-Prozess in vier Komponenten zusammenfassen, die bereits kurz im Kapitel „Definition von IT-Risikomanagement“ beschrieben wurden. Im diesen Kapitel werden diese Komponenten und einige Techniken sowie Methoden der Anwendung im Bezug auf das IT-Risikomanagement kurz vorgestellt.

5.1. Definition Risikomanagement-Kontext

Bevor man mit dem Risikomanagement Prozess beginnt, soll zuerst das System auf dem IT-Risikomanagement durchgeführt wird, definiert werden. Der erste Schritt der Kontextdefinition ist die Abgrenzung des Systems. Dabei legt man fest, welche Gegenstände ein System besitzen und somit zum Betrachtungsgebiet von IT-Risikomanagement gehören. Neben der Abgrenzung des Systems sollen auch wichtige Einschränkungen und Randbedingungen hier festgehalten werden.

Wichtig ist auch die Beschreibung wesentlicher Aspekte der externen und internen Umgebung des betrachteten Gegenstandes. Ist der zu betrachtende Gegenstand ein Unternehmen, dann gehören zur externen Umgebung beispielsweise Aspekte wie Gesellschaft, Natur, Technologie und Wirtschaft. Zu den internen Aspekten gehören Normen, Werte, Ressourcen sowie die internen Anliegen und Interessen. Zum Kontext gehören auch Führungs-Aspekte und organisatorische Festlegungen, wie organisatorische Strukturen und zugeordnete Verantwortlichkeiten, Aktivitäten, Budgetbeschränkungen und wichtige Termine. Und nicht zuletzt sind die für den Behandlungsgenstand relevanten wichtigen Ziele der Geschäfts- und Support-Prozesse (z.B. IT-Prozess) einschließlich der Risiko-Ziele aufzuführen. (Königs, 2006 S. 29)

5.2. IT-Risikoidentifizierung

Nach der Kontextdefinition folgt nun die Identifizierung der Risiken. Die Risikoidentifizierung sowie deren Einschätzung können als die schwierigsten Teile des Risikomanagementprozesses angesehen werden. Die Ergebnisse dieser Phase dienen als Input für weitere Komponente im Risikomanagementprozess. Es ist deshalb notwendig, dass möglichst viele Risiken korrekt identifiziert und eingeschätzt werden.

Man unterscheidet bei der Risikosuche grundsätzlich zwei Arten von Ansätzen der Analyse: Top-Down- und Bottom-Up-Ansätze. Bei den Top-Down Ansätzen werden allgemeinen Daten, die bekannt sind auf potentielle Risiken untersucht. Die Wahrscheinlichkeit eines Schadenseintritts wird aus bereits vorhandenen Daten geschätzt. Die Top-Down Ansätze sind relativ leicht durchzuführen und der Fokus liegt dabei auf den Risikoauswirkungen. Diese Ansätze liefern jedoch nicht viele Informationen über die Zusammenhänge und Ursachen eines Risikos. Die Bottom-Up Ansätze sind im Vergleich zu den Top-Down Ansätzen aufwendiger. Der Fokus der Bottom-Up Ansätze liegt auf den Ursachen der Risiken. Bei diesen Ansätzen werden die Risiken aufgrund der Ursachen, möglichen Schäden und deren Konsequenzen geschätzt und liefern dabei noch die Anhaltspunkte zum Setzen der notwendigen Sicherheitsmaßnahmen.

Die folgende Abbildung zeigt die möglichen Methoden zur Identifizierung der IT-Risiken mit einer anderen Kategorisierung als vorhin erwähnten.

Kollektions-methoden	Suchmethoden	
	Analytische Methoden	Kreativitätsmethoden
Checkliste SWOT-Analyse / Self-Assessment Risiko-Identifikations-Matrix (RIM) Interview, Befragung	Fragenkatalog Morphologische Verfahren Fehlermöglichkeits- und Einflussanalyse Baumanalyse	Brainstorming Brainwriting Delphi-Methode Synektik

Abbildung 6: Methoden zur Risikoidentifizierung (Romeike, et al., 2003 S. 174)

Da das Hauptthema die Evaluierung von IT-Risikomanagement Tools ist, werden hier nicht alle Methoden der Risikoidentifizierung behandelt. Im diesem Abschnitt werden lediglich die derzeit gängigen Methoden kurz vorgestellt:

- Bedrohungs- und Risikokataloge aus Best Practices
- Austausch von Erfahrungen
- Self Assessment
- Analyse der Schadensfälle

Bedrohungs- und Risikokataloge aus Best Practices

Manche Best-Practices Ansätze wie z.B. der IT-Grundschutz liefern bereits einen Bedrohungskatalog mit, den man für die Risikoidentifizierung verwenden kann. Der Umfang solcher Kataloge ist meistens sehr unterschiedlich. Die Gefährdungskataloge der IT-Grundschutz-Kataloge haben über 500 Seiten. Im nächsten Kapitel werden einige Standards von Best Practice Ansätzen sowie deren Zusammenhang zwischen IT-Risikomanagement vorgestellt.

Austausch von Erfahrungen

Die Identifizierung der Risiken kann durch einen Austausch der Erfahrungen erfolgen. Der Erfahrungsaustausch kann zwischen zwei oder mehreren Personen bzw. Unternehmen auf verschiedenen Wegen (formal, inoffiziell, u.a.) erfolgen. Die Methoden dieser Techniken sind beispielsweise. Benchmarking und Herstellerbefragung.

Die Herstellerbefragung ist eine sehr effektive Methode, um neue Kenntnisse bzw. Risiken über ein eingesetztes Produkt zu erfahren. Große Unternehmen haben meistens Verträge für die Wartung und Support mit dem Hersteller der erworbenen Produkte. Dabei kann der „Kunde“ auf eine große Sammlung von Dokumenten, z.B. über mögliche Gefährdungen oder das Knowhow des Herstellers, zurückgreifen. Die Erfahrungen der Kunden über die Risiken bzw. die eingetretenen Schaden fließen ebenfalls zurück an den Hersteller des Produktes und beeinflussen somit die Weiterentwicklung der betroffenen Produkte. Falls man nicht über solche Verträge verfügt, gibt es im Internet Foren, in denen auch Hersteller vertreten sind. Man kann dort gemeinsam mit dem Hersteller und anderen Käufern eines bestimmten Produktes über ein Problem diskutieren. Die gewonnenen Erkenntnisse kann man in die Risikoidentifizierung einfließen lassen, um. die Aktualität oder die Vollständigkeit eines Risikos zu erhöhen.

Unter Benchmarking versteht man ein Prozess dass nicht anderes macht als das Erkennen, Verstehen und Übernahmen von Arbeitsweisen und Prozessen. Als Referenz dienen andere Organisationen. Der Organisationsbegriff wird dabei aus Systemsicht neutral gehalten. D.h. es kann sich um unternehmensinternen Benchmarking (zwischen zwei Abteilungen, die fast identische Aufgaben durchführen) oder unternehmensübergreifendes Benchmarking handeln. Ziel des Benchmarking Prozesses ist die Leistungsfähigkeit der eigenen Organisation zu erhöhen, dabei werden erfolgreiche Arbeitsweisen/Prozesse adaptiert, sofern möglich. [vgl. (Seibold, 2005 S. 68)]

Self Assessment

Self Assessment bedeutet übersetzt Selbsteinschätzung. Man kann ansatzweise daraus schon ableiten, was diese Methode bedeutet. Konkret bedeutet dieser Begriff im Bezug auf IT-Risikomanagement die Einschätzung der Risiken mit vorhandenem Expertenwissen im Unternehmen und ist eine sehr oft benutzte Methode zur Risikoidentifizierung.

Der große Vorteil der Selbsteinschätzung ist, dass interne Experten besser als andere die Risiken kennen und diese einzuschätzen wissen. Nachteile können durch Betriebsblindheit oder einer für das Risikomanagement ungeeigneten Unternehmenskultur entstehen. Dies hat eine unvollständige bzw. unrichtige Selbsteinschätzung zur Folge. Die Selbsteinschätzung wird mit Experten des IT-Bereichs durchgeführt. Zusätzliche Einschätzungen können von den Fachbereichen, insbesondere bei IT-nahen Key-Usern und IT-Beauftragten, eingeholt werden. Diese Fachbereichseinschätzungen können zur Qualitätssicherung verwendet werden. (Seibold, 2005 S. 56)

Es gibt sehr viele Methoden für Self Assessment Technik. Um den Rahmen der Arbeit nicht zu sprengen, werden hier lediglich die zwei wohl bekanntesten Methoden vorgestellt: Befragungen und Workshops.

Bei der Befragung werden die erforderlichen Informationen von den Mitarbeitern des Unternehmens zur Verfügung gestellt. Die Befragung kann auf verschiedene Wege erfolgen: persönlich, schriftlich oder elektronisch. Bei den schriftlichen und elektronischen Befragungen wird meistens ein standardisiertes Formular verwendet, das der Mitarbeiter ausfüllen muss. Die elektronische Befragung ist jener der schriftlichen vorzuziehen, falls die notwendige Infrastruktur (z.B. jeder Mitarbeiter hat eine E-Mail Adresse oder es existiert ein unternehmensinternes Befragungsportal) vorhanden ist. Der wichtigste Vorteil der elektronischen Befragung ist die automatische Bearbeitung der Fragebogen und man spart dadurch viele Arbeitsstunden bei der Auswertung. Außerdem schont man damit die Umwelt, da man weniger Papier braucht. Eine persönliche Befragung, oder Interview genannt, ist im Vergleich zu den restlichen Befragungsarten individueller. Solche Befragungen sind nicht so an einer standardisierten Form gebunden und lasen Spielraum für Kreativität zu.

Eine weitere beliebte Methode von Self Assessment ist der Workshop. Dabei beschäftigt man sich intensiv mit dem Thema Identifizierung der IT-Risiken. Dabei wird miteinander intensiv über Risikosachverhalte diskutiert. Ein sehr wichtiger Faktor für einen erfolgreichen Workshop mit einem brauchbaren Ergebnis sind die Fachkenntnisse des Mitarbeiters. Der teilnehmende Mitarbeiter soll über die notwendigen Kenntnisse ihres Fachgebiets sowie über

ergänzendes Fachwissen verfügen. Außerdem soll man auch auf die Anzahl der Workshop-Teilnehmer achten. Die Anzahl soll dabei zwischen vier und zehn Teilnehmer liegen. Bei einer Überschreibung kann es vorkommen, dass man die Übersicht schnell verliert und dadurch ein effizientes Arbeiten verhindert wird.

Analyse der Schadensfälle

Eine sehr interessante Methode zur Risikoidentifizierung ist die Analyse der Schadensfälle. Man definiert den Begriff „Schadensfall“ als ein bereits eingetretenes Risiko, das ein Unternehmen bereits mit „Lehrgeld“ bezahlt hat. Man soll dabei zwischen internen Schadensfälle und externe Schadenssammlungen unterscheiden.

Die Analyse der externen Schadenssammlungen ist für das Unternehmen wohl die angenehmste Vorgehensweise, da man das „Lehrgeld“ für den eingetretenen Schaden nicht selbst bezahlen muss. Es gibt Firmen, die darauf spezialisiert haben, Datenbanken mit Schadensfällen anzubieten. Sie sammeln Schadenfällen auf, bearbeiten sie und stellen anschließend die Daten zur Verfügung. Jedoch muss man sagen, dass solche Firmen auf die öffentlich zugänglichen Medien angewiesen sind, d.h. ein großer Teil der Schadenssammlungen sind medienwirksame Schadensfälle.

Bei den internen Schadensfällen muss man zuerst anschauen, um welche Arten von Schadensfällen es sich handelt. Dabei unterscheidet man generell zwei Arten: Schadensfälle im Rahmen der Geschäftstätigkeit und Schadensfälle im IT-Bereich. Bei der Analyse der Schadensfälle aus der Geschäftstätigkeit soll man zuerst herausfinden, ob die IT des Unternehmens für den Schaden (mit-) verantwortlich ist. Der Schadensfall ist nicht relevant für IT-Risikomanagement, wenn der Schaden nicht aufgrund eines Fehlers im IT verursacht wurde. Falls die IT beim Schaden eine Rolle spielt, sollen die originären IT-Risiken identifiziert und dem spezifischen IT Risikomanagement Prozess zugeordnet werden.

5.3. IT-Risikobewertung

Risiken, die bei der Identifizierungsphase entdeckt wurden, werden anschließend in der Risikobewertung nach unterschiedlichen Kriterien wie Schadenshöhe, Eintrittswahrscheinlichkeit und Schadensfolgen bewertet. Wichtig ist es hier nur die Risiken zu evaluieren, die auch einen Bezug zum IT-Risikomanagement haben.

Es gibt verschiedene Techniken, um ein Risiko zu bewerten. Folgende Techniken werden im Rahmen dieser Masterarbeit kurz vorgestellt:

- Expertenschätzung
- Delphi-Methode
- Value-at-Risk
- Simulation
- EVT – Extrem-Value-Theorie

Expertenschätzung

Die Expertenschätzung ist eine sehr einfache, jedoch äußerst effiziente Methode bei der Bewertung von Risiken. Die Bewertung der Risiken wird in diesen Fall einfach von einem Experten durchgeführt. Wichtig bei der Expertenschätzung ist die genaue Beschreibung der Ausgangsdaten, sonst ist eine Fehleinschätzung durchaus möglich. Eine weitere wichtige Voraussetzung ist, dass der beauftragte Experte kein Eigeninteresse an der Schätzung hat. Ferner unterscheidet man noch zwischen der internen und externen Expertenschätzung. Bei der internen Schätzung wird sie durch einen Experten im Haus durchgeführt. Eine externe Schätzung wird dabei von fremden Experten durchgeführt. Die externe Expertenschätzung soll man bevorzugen, wenn eine objektivere Einschätzung erwünscht bzw. erforderlich ist.

Delphi-Methode

Bei der Delphi-Methode werden die Risiken von mehreren Experten geschätzt. Sie ist ein iteratives, mehrstufiges Schätzverfahren und es gibt davon zwei Arten: Standard-Delphi-Methode (SD) und Breitband-Delphi-Methode (BD). Vor Beginn der Delphi-Methode wird der Sachverhalt genau beschrieben und der zu schätzende Parameter definiert. Bei der Delphi-Methode wird wie folgt vorgegangen:

1. Formulierung der Themen sowie zu schätzenden Werte
2. Experten erhalten die Dokumente
3. (BD) Diskussion
4. Experten schätzen den Umfang anonym
5. Auswertung
    a. (SD) Gravierende Abweichungen werden kommentiert
    b. (BD) Ergebnis wird zusammengefasst
6. Die Ergebnisse gehen an die Experte
7. (BD) Diskussion über die Abweichungen
8. Experten korrigieren (Wiederholung Pkt. 4-8 solange bis Korrelation vorhanden)
9. Ergebnis ist der Mittelwert der Schätzungen

Bei beiden Delphi-Methoden ist die Schätzung anonym, jedoch ist die Diskussion im Anschluss bei der Breitband-Delphi-Methode nicht anonym. Generell versucht die Delphi-Methode die Fehleinschätzungen der Experten durch mehrstufiges Design zu reduzieren. Dennoch können hier auch nicht alle Probleme der Expertenschätzung beseitigt werden. Außerdem kann eine solche Bewertungsmethode sehr lange dauern.

Value-at-Risk Methode

Die Value-at-Risk (VaR) Methode ist ein quantitativer Ansatz zur Bewertung von Risiken. Der Begriff wird auch öfters als Money-at-Risk oder Capital-at-Risk genannt.

> *Der „Value at Risk"-Wert ist der maximal erwartete Schaden, der unter üblichen Bedingungen innerhalb einer bestimmten Zeit-Periode mit einer bestimmten Wahrscheinlichkeit, dem sog. Konfidenz-Niveau, eintreten kann.*

Die Methode Value-at-Risk wurde von J.P. Morgan entwickelt und ist zurzeit ein Standardrisikomaßverfahren im Finanzsektor. Diese Methode wird mittlerweise auch in anderen Sektoren wie Industrie oder Handel zur Quantifizierung der Risiken eingesetzt. Die folgende Abbildung zeigt Value-at-Risk nochmal graphisch dar.

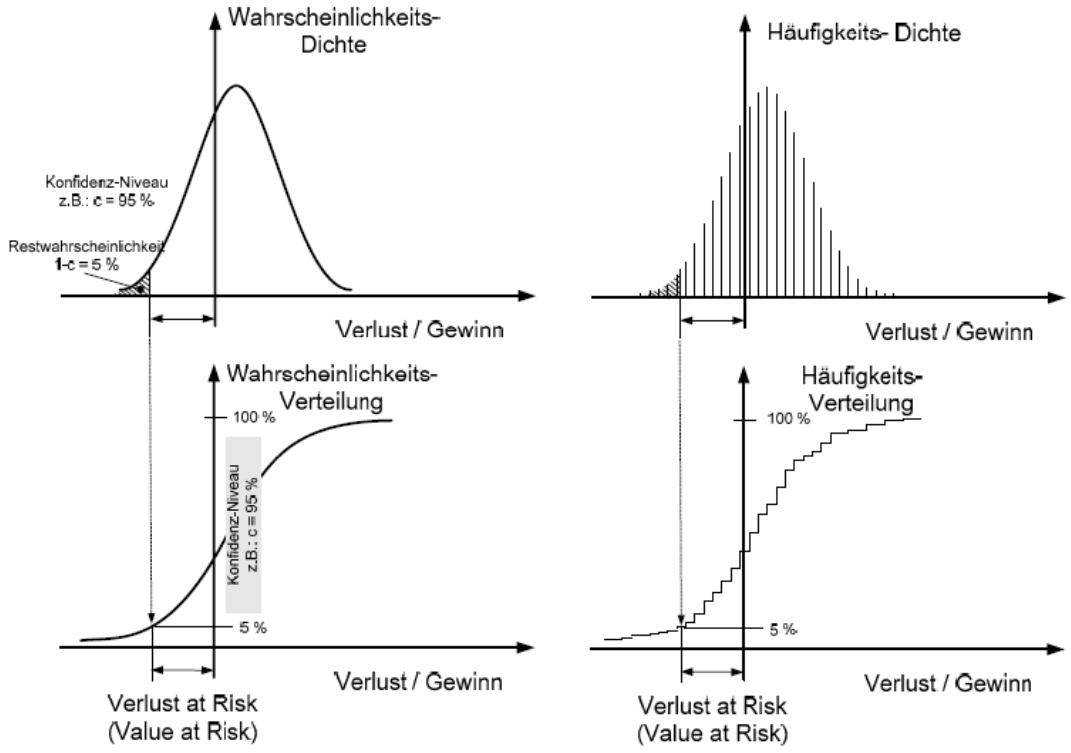


Abbildung 7: „Verlust at Risk" mit Konfidenz-Niveau 95 % kontinuierlich und diskret verteilt (Königs, 2006 S. 35)

Man unterscheidet zwei Arten von VaR Ansätzen: parametrisierter Ansatz und simulierter Ansatz. Den parametrisierte VaR-Ansatz soll man eher nicht im Bereich der operationellen Risiken bzw. im Bereich der IT-Risiken anwenden. Der Grund dafür ist recht einfach: die parametrisierten VaR Modelle liegen zumeist einer Normalverteilung zugrunde. Die Wahrscheinlichkeitsverteilung der IT-Risiken schaut dabei anders als eine Normalverteilung aus. Es ist allgemein bekannt, dass im operationellen bzw. IT-Bereich kleine bis mittlere Verluste mit verhältnismäßig hoher Wahrscheinlichkeit eintreten. Schäden mit großen Verlusten kommen hierbei weniger vor. Aufgrund der hier vorliegenden Erkenntnisse ist die Normalverteilung bei der Bewertung von IT-Risiken nicht geeignet. Die Wahrscheinlichkeitsverteilung soll hier in der Regel rechtsschief sein. Eine mögliche Wahrscheinlichkeitsverteilung für den IT-Bereich ist Log-Normal-Verteilung, dargestellt in der folgenden Abbildung.

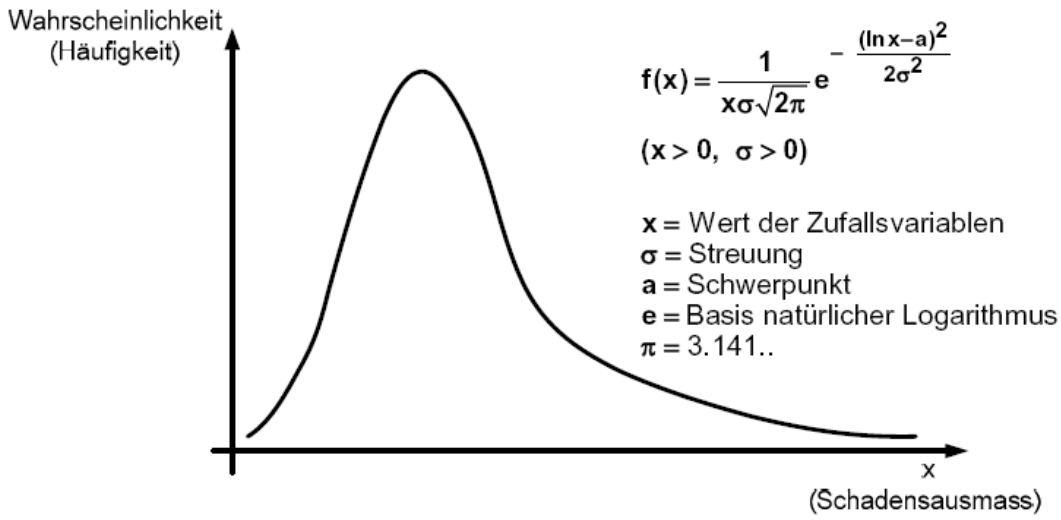


Abbildung 8: Dichtefunktion der Log-Normal-Verteilung (Königs, 2006 S. 36)

Die Value-at-Risk Methode kann grundsätzlich auf IT-Risiken angewendet werden. Allerdings lassen sich aus diesem Ansatz, aufgrund der benötigten Datenmengen, nur schwer Rückschlüsse auf einzelne Risikoszenarien ziehen. Für die Quantifizierung einzelner IT-Risikoszenarien ist ein hoher Initialaufwand erforderlich. [Vgl. (Seibold, 2005 S. 101)]

Simulation

Die Simulationsmethoden zählen wie die VaR-Methode ebenfalls zu den quantitativen Ansätzen der Risikobewertung. Aufgrund der vorhandenen Daten werden die künftigen Entwicklungen anhand von mathematischen Formeln berechnet und analysiert.

EVT – Extreme-Value-Theorie

Die EVT Methode wird bei den Risiken, die zwar sehr selten vorkommen, jedoch deren Folgen fatale Schadenssummen ergeben, verwendet. Beim Value-at-Risk Ansatz wurde erwähnt, dass die Schadensverteilung im operationellen Bereich rechtsschiefe Eigenschaften besitzt. Aufgrund der seltenen Eintrittswahrscheinlichkeit kann die maximale Größe des Auswirkungsmaßes meistens nur geschätzt werden.

Die EVT verwendet zur Berechnung eines maximalen Schadensniveaus spezielle Extremwertverteilungen, die aus empirischen Untersuchungen/Schätzwerten resultieren und bedient sich der Eigenschaft, dass lange, rechtsschiefe Verteilungen einen annähernd linearen Funktionsverlauf nehmen. Der Einsatz von EVT ist, insbesondere bei der Schätzung von Auswirkungsmaßen bei Produktivitäts-/Abhängigkeitswerten, von Bedeutung. Sie kann gut bei Infrastrukturkomponenten oder Basistechnologien bzw. auf Seiten der Fachbereiche bei den Anwender-IT-Risiken eingesetzt werden. (Seibold, 2005 S. 102)

Ein Beispiele für den Einsatz von EVT Methode ist die Berechnung der Höhe der Deiche, die Holland vor Überschwemmungen schützen. Dabei wird die Höhe der Deiche berechnet, die erforderlich ist, um eine Katastrophe zu verhindern. Zugegeben das Beispiel hat nichts mit IT-Risikomanagement zu tun. Jedoch zeigt das Beispiel die wichtige Bedeutung der EVT-Methode im Risikomanagement.

5.4. IT-Risikosteuerung und -überwachung

In der IT-Risikoidentifikation wurde erwähnt, dass die Identifizierung der IT-Risiken als den schwierigsten Teil des RM-Prozesses gesehen werden kann, da sie die Daten für weitere Phasen des Risikomanagementprozesses liefern. Somit kann man die Risikoidentifizierung als die Basis bezeichnen. Im Gegensatz zur Identifizierung der IT-Risiken kann die IT-Risikosteuerung als das Herzstück betrachtet werden. Am Anfang dieses Kapitels werden die Steuerungsmaßnahmen, anschließend wird das Thema Risikoüberwachung im IT kurz vorgestellt. Am Ende des Kapitels werden dann die Risikoindikatoren kurz erwähnt.

5.4.1. Steuerungsmaßnahmen

Durch die Steuerungsmaßnahmen werden die relevanten IT-Risiken beeinflusst. Beeinflussbar sind zum Beispiel die Eintrittswahrscheinlichkeit oder die Höhe des Schadens. Man unterscheidet generell vier Arten von Steuerungsmaßnahmen:

- Risikovermeidung
- Risikoverminderung
- Risikoübertragung
- Risikoakzeptanz

Risikovermeidung

Die Risikovermeidung ist eine sehr einfache und äußerst effiziente Maßnahme zur Reduzierung der Risiken. Dabei geht man einfach kein Risiko ein. Es existiert keine Gefahr für einen Schaden, wenn man kein Risiko eingeht. Es bedeutet jedoch auch, dass die Chancen auf einen Erfolg verhindert werden.

Ein Beispiel für eine risikovermeidende Maßnahme ist der Verzicht auf die Einführung eines bestimmten IT-Services wie etwa. Internet Banking oder Online-Shop. Wenn man auf die Einführung verzichtet, vermeidet man Risiken, die das bestimmte IT-Service nach der Einführung mit sich bringen. Risiken für einen Online-Shop sind unter anderem gefälschte Bestellungen oder Angriffe von Hackern. Allerdings wird ein Erfolg oft dadurch verhindert, wenn man auf das Eingehen eines Risikos verzichtet.

Es ist hier auch möglich, Risikobegrenzung durchzuführen: Das Unternehmen geht solange das Risiko ein, bis eine festgelegte Verlust-Obergrenze überschritten wird. Danach zieht sich das Unternehmen aus dem Geschäft zur Gänze zurück. (Löbl, 2008 S. 40) Die Risikobegrenzung ist im Finanzgeschäfte üblich und hat im Bereich IT-Risikomanagement eher wenig Bedeutung.

Risikoverminderung

Bei der Risikoverminderung werden Maßnahmen zur Verminderung eines Risikos durchgeführt. Dabei nimmt man gezielt auf die Eintrittswahrscheinlichkeit oder das Ausmaß eines Schadens Einfluss.

Ein Beispiel für Risikoverminderung bei einem Online-Shop ist die Einführung der gesicherten Datenübertragung. Durch die Verschlüsselung der Daten erschwert man z.B. den Hackern das Herausfinden von empfindlichen Geschäftsdaten wie etwa die Kreditkartenummer. Als Beispiel hierfür kann im Bereich des Internet Banking. die Einführung mobiler TAN-Nummer angeführt werden. Das bedeutet, dass bei jedem Auftrag eine TAN-Nummer vom System generiert und per SMS an den Auftraggeber geschickt wird. Diese TAN-Nummer ist

nur für eine bestimmte Transaktion gültig. Dadurch schützt man Personen mit wenigen IT-Kenntnissen z.B. vor Phishing Attacke, die eine enorme Schadenssumme verursachen kann.

Maßnahmen, die die IT-Risiken vermindern, werden in vielen Bereichen des Unternehmens eingesetzt. Folgende Auflistung zeigt einige Beispiele:

- IT Security: Standards oder Best Practices wie z.B. die ISO 27000 Reihen oder der IT-Grundschutz
- IT-Controlling: Einführung von IT-Controlling als Stabbereich zur Unterstützung von IT-Management bzw. IT-Risikomanagement.
- IT-Projektmanagement: Die gewonnenen Erkenntnisse über die Risiken im verschiedenen Typen von IT-Projekte sollen in einer Datenbank gesammelt werden, damit sie nicht verloren gehen.
- Personalmanagement: Das Personalmanagement leistet einen sehr großen Beitrag zur Reduzierung der IT-Risiken. Mitarbeiter mit wenig oder gar keiner Motivation produzieren (absichtlich) Fehler. Bei einer Neueinstellung soll man auf die Qualifikation des Bewerbers achten.
- Qualitätsmanagement: Einhaltung von Qualitätsstandards helfen die Risiken zu vermindern.
- RZ-Betrieb: Große Firmen oder Anbieter von IT Dienstleistungen wie z.B. Servern/VPS oder Webhosting Pakete betreiben meistens ein eigenes Rechenzentrum. Hier kann man durch die Anwendung von Standards oder Best-Practice Ansätze wie z.B. ITIL die IT-Risiken reduzieren.

Risikoübertragung

Unter Risikoübertragung versteht man eine Abwälzung der Risiken sowie des Schaden an einen Dritten. Die bekannteste Form der Risikoübertragung ist der Abschluss von Versicherungen. Im Falle eines Risikoeintritts zahlt die Versicherung den entstandenen Schaden und das Unternehmen geht ohne oder nur mit geringem Schaden heraus. Man muss jedoch anmerken, dass die Höhe der Versicherungsprämie von der Eintrittswahrscheinlichkeit sowie vom Schadensausmaß abhängig ist. Die Prämie wird wohl sehr hoch sein, wenn man alle Risiken versichern möchten. Die Höhe der Versicherungsprämie variiert bei unterschiedlichen Versicherungsgesellschaften. Man soll daher in regelmäßigen Intervallen die Verträge mit der Versicherung überprüfen.

Eine weitere Form der Risikoübertragung ist die Übertragung auf den Geschäftspartnern. Man lagert hier bestimmte Bereiche wie z.B. IT-Security an einen Spezialisten aus und vereinbart eine Konventionalstrafe. Falls das Unternehmen aufgrund der Fahrlässigkeit des Geschäftspartners einen Schaden erleidet, kann der Geschäftspartner zur Verantwortung gezogen werden. Ein Beispiel für diese Risikoübertragungsform ist die Einrichtung eines Security Proxy-Servers, der beispielweise von Security Spezialisten der Firma Ikarus Security Software GmbH angeboten wird.

Risikoakzeptanz

Bei der Risikoakzeptanz trägt das Unternehmen selbst den Schaden im Falle eines Risikoeintritts. Man „akzeptiert" das Risiko einfach. Im diesen Fall wird in der Buchhaltung des Unternehmens eine Rückstellung gebildet, d.h. man reserviert einen bestimmten Geldbetrag für die Begleichung eines eingetretenen Schadens.

Der Nutzen, für den das Risiko eingegangen wird, muss höher als das Risikopotenzial sein und zugleich müssen die vorhandenen alternativen Steuerungsmaßnahmen nicht möglich bzw. nicht sinnvoll sein. [vgl. (Seibold, 2005 S. 33)] Bei dieser Steuerungsmaßnahe ist es sehr wichtig, dass die Risiken und deren Folgen richtig eingeschätzt werden.

5.4.2. IT-Risikoüberwachung

Ziel der Risikoüberwachung ist, den Status der zu beobachtenden Risiken und den der Gegenmaßnahmen zu dokumentieren. Mithilfe der festgelegten Risikoindikatoren können Abweichungen festgestellt werden. Weichen die Risikoindikatoren von ihrem Wert ab und/oder ist bereits ein Trend zu sehen, dass sie noch mehr abweichen werden und dadurch die vorgegebene Grenze überschritten werden könnte, wird dies dokumentiert und im Risikomanagementbericht als Frühwarnung entsprechend angezeigt. Über die Risikosteuerung können umgehend Maßnahmen vorbereitet oder auch eingeleitet werden. Der Einsatz der Maßnahmen wird bei Überschreiten des Grenzwertes unmittelbar durchgeführt, um entweder den Eintritt des Risikos verhindern oder zumindest noch die Schadenhöhe minimieren zu können. Die Überwachung der Risiken im Hinblick auf die Wirkung der Maßnahmen wird wiederum von der Risikoüberwachung übernommen. (Löbl, 2008 S. 43)

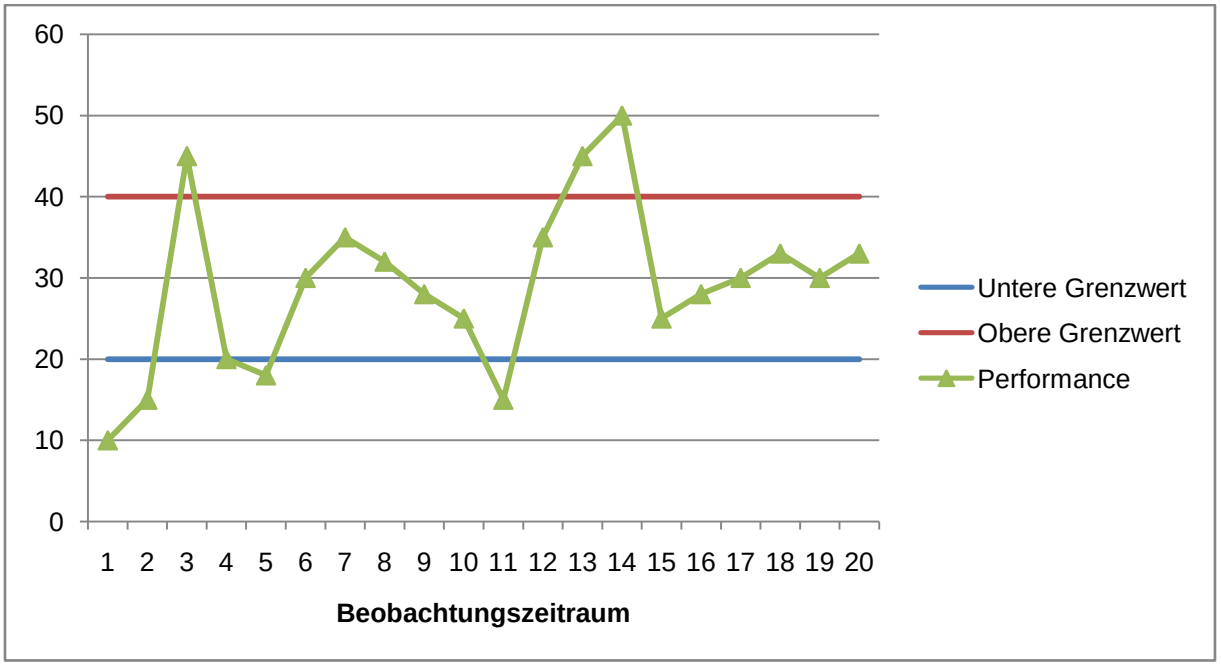


Abbildung 9: Risikoindikator mit oberen und unteren Grenzwerten

5.4.3. Risikoindikatoren

Im vorherigen Unterkapitel wurde die IT-Risikoüberwachung kurz erläutert. Bei der Überwachung der Risiken spielen die Risikoindikatoren eine wichtige Rolle. Ohne diese Indikatoren läuft die Überwachung nicht richtig, da man bei der Überwachung neben Risikotreiber auch messbare Zahlengröße benötigt. Die Risikoindikatoren werden über die Risikoszenarien bei der Identifizierungsphase identifiziert. Um den Umfang der Arbeit nicht zu sprengen, wurden absichtlich die Beschreibung von Risikoszenarien sowie die Identifizierung der Risikoindikatoren ausgelassen.

Man unterscheidet zwei Arten von Risikoindikatoren:

- Messbare Kennzahlen
- Risikotreiber

Messbare Kennzahlen

Dieser Art von Risikoindikatoren sind messbar und kann in Zahlen dargestellt werden. Vorteil von solchen Risikoindikatoren ist die Möglichkeit der statistischen Verarbeitung und Analyse. Beispiele für solche Kennzahlen sind die. Up- und Downtime eines Servers. Wenn man die Qualität des Netzwerks oder die Anbindung überwachen will, überprüft entweder die Ping Zeiten oder SLA Verstöße.

Risikotreiber

Unter Risikotreiber versteht man die Sachverhalte, die einen positiven bzw. negativen Einfluss auf die Eintrittswahrscheinlichkeit sowie die Höhe des Schades haben. Solche Risikoindikatoren sind generell nicht messbar und sind daher für eine statistische Auswertung nicht geeignet. Beispiele für solchen Indikatoren sind z.B. die Motivation oder Knowhow des Mitarbeiters. Eine geringe Motivation ist für das Unternehmen schlecht und der Mitarbeiter macht häufiger Fehler. Ein weiteres Beispiel der Risikotreiber ist die Komplexität des IT-Systems. Man verliert leicht den Überblick bei einer komplexen Systemumgebung und dies führt zu ein erhöhtes Risiko im den Bereich.

6. IT Risikomanagement in Best Practices und Standards

Es gibt keine eigene Norm für das IT-Risikomanagement selbst. Das IT-Risikomanagement bringt jedoch viele Vorteile und ist in vielen internationalen Standards und Best Practices (z.B. ISO 27000-Reihe, IT Grundschutz, Cobit u.a.) integriert oder kurz beschrieben. In diesem Kapitel werden einige wichtige Standards und Best Practices kurz vorgestellt und die Inhalte bezüglich IT Risikomanagement erörtert.

6.1. Cobit

Cobit (Control Objectives for Information and Related Technology) ist ein Modell zur Kontrolle der gesamtem IT und wurde ursprünglich von ISACF (Information Systems Audit and Control Foundation), ein Forschungsinstitut der ISACA (Information Systems Audit and Control Association) entwickelt. Im Jahr 1999 wurde die Aufgabe der Entwicklung an IT-Governance Institut übertragen. Die aktuellste Ausgabe ist die Version 4.0, die im Jänner 2006 erschienen ist.

Das COBIT Framework besteht aus den Kontrollzielen und auch Objekten sowie aus der Struktur für ihre Klassifizierung. Die allgemeine Überlegung ist die, dass es drei Ebenen gibt, wenn es um das Management der IT-Ressourcen geht. Auf der untersten Ebene geht es um die Aktivitäten, die benötigt werden, um ein definiertes Resultat zu erzielen. Diese Aktivitäten werden zu natürlichen Gruppen zusammengefasst, die spezifische Kontrollen zulassen. Diese Aufgabengruppen werden Prozesse genannt. Auf der obersten Ebene werden diese Prozesse zu Domänen konsolidiert, die häufig auch den Organisationsanforderungen der IT Bereiche entsprechen. (Goltsche, 2006 S. 25)

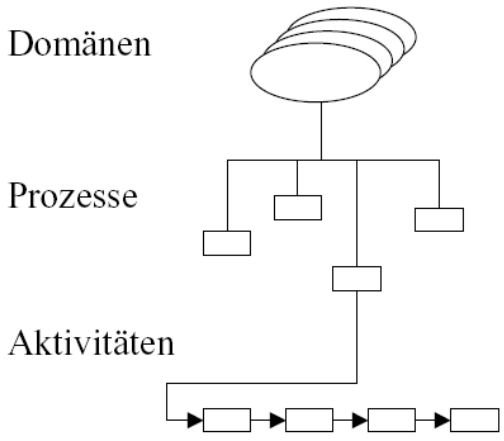


Abbildung 10: Hierarchie von Cobit (Goltsche, 2006 S. 25)

Die obige Abbildung zeigt die Dimension IT Prozesse der Cobit Struktur. Sie wird noch um zwei weitere Dimension ergänzt: IT Ressourcen und Unternehmensanforderungen. Die Abbildung zeigt den Cobit-Würfel, den das gesamte Modell vereinfacht darstellt.

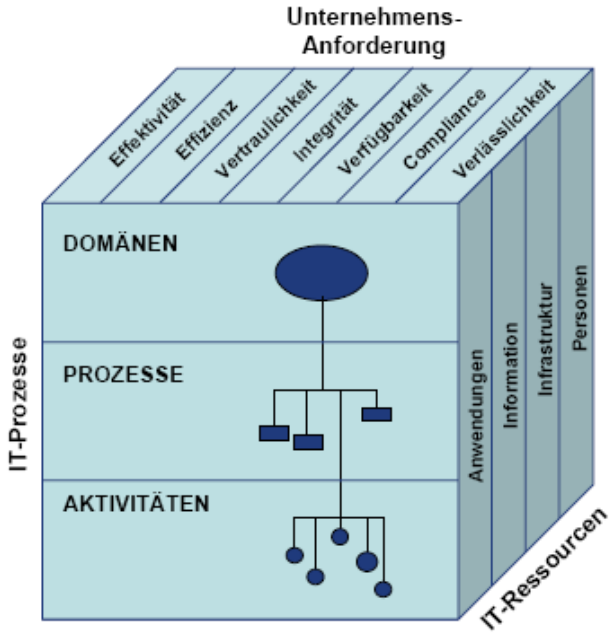


Abbildung 11: Cobit Würfel (IT-Governance Institute, 2006 S. 26)

Im Cobit-Würfel werden die Zusammenhänge zwischen den Dimensionen verdeutlicht. Die IT-Ressourcen werden untergliedert in

- Anwendungen
- Information
- Infrastruktur
- Personen

Die Geschäftsprozesse basieren auf diese IT Ressourcen. Die Ressourcen werden dann durch die IT Prozesse gemanagt, um die Ziele zu erreichen, die auf Unternehmenserfordernisse ausgerichtet sind.

Es gibt insgesamt 34 Cobit-Prozesse, die auf vier Domänen aufgeteilt ist.

- Planung und Organisation
- Beschaffung und Implementierung

- Betrieb und Unterstützung
- Monitoring und Evaluierung

Die Tabelle zeigt einen kurzen Überblick über die gesamten Cobit Prozesse sowie deren Aufteilung in den Domänen.

Planung und Organisation (PO)	
PO1	Definieren eines strategischen IT-Plans
PO2	Definieren der Informationsarchitektur
PO3	Definieren der technischen Ausrichtung
PO4	Definition der IT-Organisation & ihrer Beziehungen
PO5	IT-Investitionsmanagement
PO6	Kommunizieren der Management Ziele und Strategien
PO7	IT-Personalführungsmanagement
PO8	Managen der Qualität
PO9	Risikomanagement
PO10	Projektmanagement
Beschaffung und Implementierung (AI)	
AI1	Identifizierung automatisier Lösungen
AI2	Erwerb und Pflege von Applikationssoftware
AI3	Erwerb und Pflege der technischen Infrastruktur
AI4	Befähigen des Betrieb
AI5	Zurverfügungstellung von IT-Ressourcen
AI6	Change Management
AI7	Installieren und Abnehmen von Systemen und Änderungen
Betrieb und Unterstützung (DS)	
DS1	Service Level Management
DS2	Lieferanten-Management
DS3	Performance und Kapazitätsmanagement
DS4	Continuity Management
DS5	System Security Management
DS6	Kostenmanagement
DS7	Anwenderschulung und Training
DS8	Anwenderunterstützung
DS9	Konfigurationsmanagement
DS10	Problem Management
DS11	Data Management
DS12	Facility Management
DS13	Operationsmanagement
Monitoring und Evaluierung (ME)	
ME1	Überwachen und evaluieren IT Performance
ME2	Überwachen und evaluieren interner Kontrollen
ME3	Sicherstellung der Einhaltung gesetzlicher Vorschriften
ME4	Sorgen für IT-Governance

Tabelle 4: Cobit Prozessübersicht (Goltsche, 2006 S. 28)

Beim Überfliegen der Tabelle fällt sofort der Prozess PO09 – Risikomanagement auf. Laut PO9 soll ein Risikomanagement-Framework erstellt und betrieben werden. Ziel von PO9 ist

die Erkennung, Analyse von Bewertung von Risiken. Ferner soll auch eine Strategie zur Reduktion der Risiken erstellt werden, um das Restrisiko auf ein akzeptiertes Niveau zu reduzieren.

Der Prozess PO09 lässt sich noch detaillierter in sechs Control Objectives unterteilen:

- PO9.1: Abstimmung des Risikomanagements der IT und des Unternehmens
- PO9.2: Festlegung des Risikokontext
- PO9.3: Ereignisidentifikation
- PO9.4: Bewertung von Risiken
- PO9.5: Maßnahmen zur Risikobehandlung
- PO9.6: Erhalt und Monitoring eines Plans zur Risikobehandlung

Anhand der detailierten Unterteilung von PO09 erkennt man die wichtigsten Komponenten eines IT-Risikomanagement-Prozesses. Das Ziel des PO9 Prozesses ist die Ermittlung von Risiken und deren Auswirkungen auf die Geschäftsprozesse. Dieses Ziel wird erreicht, indem man ein Risikomanagement-Framework erstellt und dabei die Kernkomponenten des Risikomanagementprozesses (Identifikation, Bewertung, Steuerung, Überwachung) beschreibt. Das Ziel des Prozesses wird an folgenden Indikatoren gemessen:

- Prozent der kritischen IT-Ziele, die von der Risikobeurteilung abgedeckt sind
- Prozent der identifizierten kritischen IT-Risiken, für die Maßnahmenpläne entwickelt worden sind
- Prozent der Risikomanagement-Maßnahmenpläne, die zur Implementierung genehmigt worden sind (IT-Governance Institute, 2006 S. 67)

Man erkennt, dass das Cobit-Framework kein dezidiertes IT-Risikomanagement-Framework darstellt, unterstützt jedoch die Durchführung des IT-Risikomanagements durch seinen weitgefächerten Ansatz sehr gut. Die Anforderungen an die Informationen und die Ressourceneinteilung können leicht den Ansprüchen des IT-Risikomanagements zugeordnet werden. (Seibold, 2005 S. 187)

6.2. IT Grundschutz-Kataloge und BSI Standards (IT Grundschutz)

Die IT-Grundschutz-Kataloge und die BSI-Standards sind Teile des IT-Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik und werden regelmäßig auf dem Stand

gehalten. Ursprünglich wurde das IT-Grundschutzhandbuch, das im Jahr 2005 auf IT-Grundschutz-Kataloge umbenannt wurde, als Sicherheitsleitlinien für den öffentlichen Bereich entwickelt. Es kann jedoch ohne große Probleme auf den anderen Organisationseinheiten übertragen werden.

Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. (BSI, 2007 S. 14)

Die IT-Grundschutz-Kataloge bestehen aus zwei Teilen: Gefährdungskatalog und Maßnahmenkatalog. Der Umfang des Katalogs ist sehr groß und hat in der neunten Ergänzungsauflage 3718 Seiten. Der umfangreiche Inhalt der Kataloge ist eine Stärke des IT Grundschutzes, wenn man mit den internationalen Standards und Normen vergleicht, die eher übergreifend orientiert sind. Die Kataloge verfolgen das Baukastenprinzip. Ziel dieses Prinzips ist eine bessere Strukturierung und Aufbereitung der Bausteine. Die Bausteine sind wiederum in Schichten zusammengefasst. Diese Schichten sind

- Übergeordnete IT-Sicherheitsaspekte,
- Infrastrukturelle Sicherheit,
- Sicherheit der IT-Systeme,
- Netzsicherheit und
- Sicherheit der Anwendungen.

Neben den IT-Grundschutz Katalogen gibt es die so genannten IT-Grundschutz-Standards, auch BSI Standards genannt. Im BSI Standards sind Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit enthalten. Die Standards der 100er Reihe des BSI umfasst vier Dokumente, wobei ein Dokument (BSI 100-4) derzeit noch in der Überarbeitung ist.

Der erste Standard (BSI 100-1) beschäftigt sich mit den Managementsystemen für Informationssicherheit (ISMS). Er gibt eine kurze Einführung in die Informationssicherheit und definiert die allgemeinen Anforderungen an ein ISMS. BSI 100-1 ist vollständig kompatibel zum ISO 27001 Standard und berücksichtigt weiterhin die Empfehlungen der anderen ISO-Standards der ISO 27000 Reihen.

Der BSI Standard 100-2 baut auf den BSI 110-1 Standard auf und beschreibt die Vorgehensweise im IT-Grundschutz. Diese Vorgehensweise heißt IT-Sicherheitsprozess nach BSI und besteht aus folgenden Aktivtäten:

- Initiierung des Sicherheitsprozesses
- Erstellung nach einer Sicherheitskonzeption nach IT Grundschutz
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Da der Sicherheitsprozess nach BSI nicht das eigentliche Thema der Arbeit ist wird nicht mehr in den Details eingegangen.

Der BSI-Standard 100-3 beschäftigt sich mit der Risikoanalyse, ein Kernthema der Masterarbeit, auf Basis des IT-Grundschutzes. Die folgende Abbildung zeigt die Risikoanalyse im Sicherheitsprozess nach BSI.

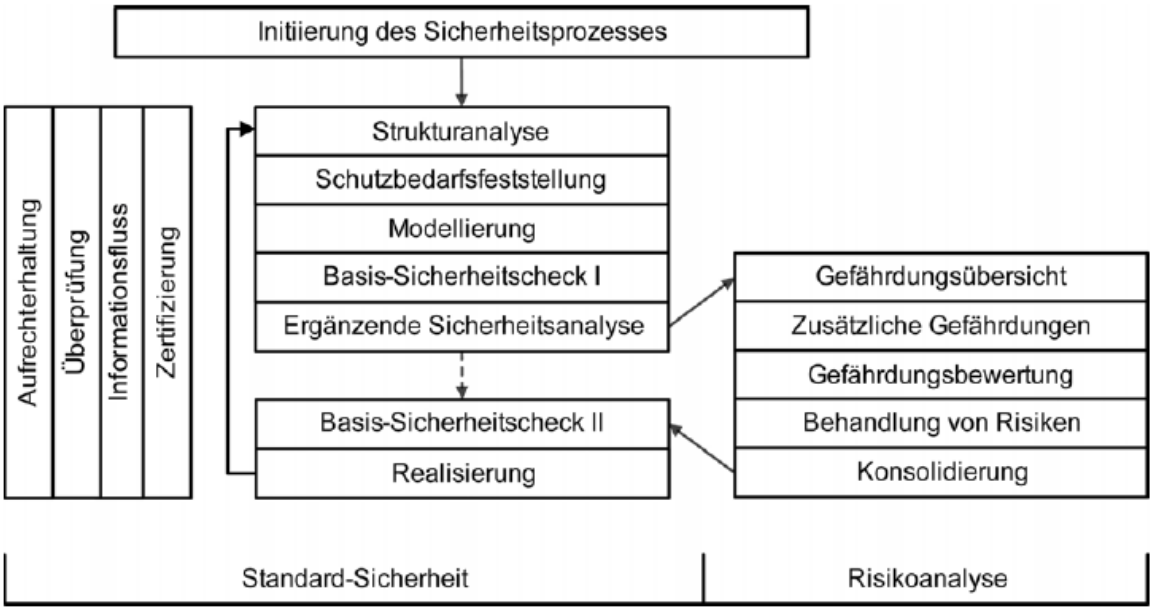


Abbildung 12: Risikoanalyse im IT-Grundschutz (BSI, 2008 S. 5)

Der BS 100-3 Standard beschreibt eine Methodik, wie mit möglichst geringem Aufwand für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf zur Begrenzung von Risiken für die Informationsverarbeitung besteht. (BSI, 2008 S. 4) Voraussetzung für eine Durchführung der Risikoanalyse ist die Umsetzung des BSI Standards 100-2, da die Inputs der Risikoanalyse aus Ergebnissen der IT-Grundschutz-Vorgehensweise stammen.

Der Standard besteht aus folgenden Aktivitäten:

- Erstellung der Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Gefährdungsbewertung
- Behandlung von Risiken
- Konsolidierung des Sicherheitskonzepts
- Rückführung in den Sicherheitsprozess

Man erkennt hier eine gewisse Ähnlichkeit mit dem Risikomanagement-Prozess, der bereits im allgemeinen Theorieteil über das Risikomanagement vorgestellt wurde. In den Aktivitäten „Erstellung der Gefährdungsübersicht“ und „Ermittlung zusätzlicher Gefährdungen“ werden die Gefährdungen ermittelt. Der Output ist die sogenannte Gefährdungsübersicht. In der Aktivität Gefährdungsbewertung wird der Gefährdungsübersicht systematisch abgearbeitet und überprüft, ob das vorhandenen Konzept oder die vorgesehenen Maßnahmen in den IT-Grundschutzkatalogen ausreichend sind.

In den meisten Fällen bleiben nach der Gefährdungsbewertung mehrere Gefährdungen übrig, denen man mit den Maßnahmen des IT-Grundschutzes nicht ausreichend entgegenwirken kann. Aus diesen übriggebliebenen Gefährdungen ergeben sich folglich Risiken für den Betrieb des Informationsverbunds. Man muss daher entscheiden, wie man mit diesen Risiken umgehen soll. Im Theorieteil des Kapitels Risikomanagement wurde bereits die mögliche Vorgehensweise bei diesen Risiken angeführt.

Bei der Risikoanalyse können unter Umständen Gefährdungen identifiziert werden, aus denen Risiken resultieren, die zwar derzeit akzeptabel sind, in Zukunft jedoch voraussichtlich steigen werden. Dies bedeutet, dass sich in der weiteren Entwicklung ein Handlungsbedarf ergeben könnte. In solchen Fällen ist es sinnvoll und üblich, bereits im Vorfeld ergänzende Sicherheitsmaßnahmen zu erarbeiten und vorzubereiten, die in Betrieb genommen werden können, sobald die Risiken inakzeptabel werden. (BSI, 2008 S. 18)

Falls bei der Behandlung von verbleibenden Gefährdungen ergänzende Maßnahmen zu den Standard-Sicherheitsmaßnahmen hinzugefügt wurden, muss das Sicherheitskonzept anschließend konsolidiert werden. (BSI, 2008 S. 21) Konkret bedeutet dies, dass die Sicherheitsmaßnahmen für jedes Zielobjekt anhand von bestimmten Kriterien überprüft werden. Diese Kriterien findet man im Kapitel sieben des BSI Standards 100-3. Nach der Konsolidie-

rung des Sicherheitskonzeptes kann der Sicherheitsprozess nach BSI dann weiter fortgesetzt werden.

Der BSI-Standard 100-4 beschäftigt sich mit dem Thema Notfall-Management. Im BSI 100-4 Standard sind die Vorgangsweisen enthalten, wie man auf ein Schadensereignis reagieren soll und wie man nach einem Schadensereignis die gewöhnlichen Geschäftstätigkeiten so schnell wie möglich wieder aufgenommen werden können. Dieser Standard ist zurzeit in der Überarbeitungsphase und es existiert lediglich ein Entwurfsdokument, das man in der IT-Grundschutz Seite des BSI Homepages herunterladen kann.

Der IT-Grundschutz nimmt in seiner Verbreitung in Deutschland eine Spitzenreiterposition ein. Über 60% der Großunternehmen nutzen diesen Schutz. Aber auch in öffentlichen Organisationen spielt das Handbuch eine wichtige Rolle. In etwa der Hälfte der KMU war der IT-Grundschutz bekannt und nahezu der einzige Standard, der wirklich auch in der praktischen Arbeit verwendet wurde. Dies bedeutet jedoch nicht, dass die Anwenderunternehmen in jedem Fall einen systematischen Grundschutz danach aufbauen. Die Mehrzahl der Unternehmen verwendet IT Grundschutz punktuell, um sich über sichere IT-Lösungen zu informieren. (Teubner, et al., 2005 S. 103)

Wie man aus der Beschreibung erkennt, bezieht sich der IT-Grundschutz ausschließlich auf das IT-Sicherheitsmanagement. Die IT-Grundschutz-Kataloge sind sehr umfangreich und können gut zur Identifizierung und Generierung von Risiken bzw. Maßnahmen verwendet werden. Der BSI Standard 100-3 beschreibt, wie man eine Risikoanalyse auf Basis des IT-Grundschutz anwendet. Dadurch ist es möglich eine Risikoanalyse in das IT Sicherheitsprozess zu integrieren. Wenn man mit internationalen Standards und Best Practices vergleicht, ist die Stärke des IT-Grundschutzes der große Umfang der IT-Grundschutz-Kataloge, in denen viele Gefährdungen und Maßnahmen enthalten sind.

6.3. Österreichisches Informationssicherheitshandbuch

Das österreichische Informationssicherheitshandbuch wurde im Auftrag vom Bundeskanzleramt Österreichs erstellt und aufgrund der ständigen internationalen Entwicklungen angepasst. Das österreichische Informationssicherheitshandbuch wurde vom früheren „IT-Sicherheitshandbuch“ weiterentwickelt und die aktuelle Ausgabe ist die Version 2.3 vom April 2007. Das Buch besteht aus drei Teilen, wobei die ersten beiden Teile als PDF Dokument zur Verfügung stehen.

Neben dem PDF Dokument ist das Informationssicherheitshandbuch seit Jahr 2003 auch in XML Version erhältlich. Durch die XML Struktur ist eine Zielgruppenorientierung möglich. Das allgemeine Informationssicherheitshandbuch kann an die Organisationseinheit (Organisationstyp und Organisationsgröße) angepasst werden. Das Resultat daraus ist das Sicherheitshandbuch der Organisationseinheit. Aus dem Sicherheitshandbuch der Organisationseinheit kann man die zur Verfügung gestellten Checklisten editieren. Aus der Checkliste können dann Ansichten für eine bestimmte Rolle (Management, Umsetzung/Wartung und Anwender) generiert werden.

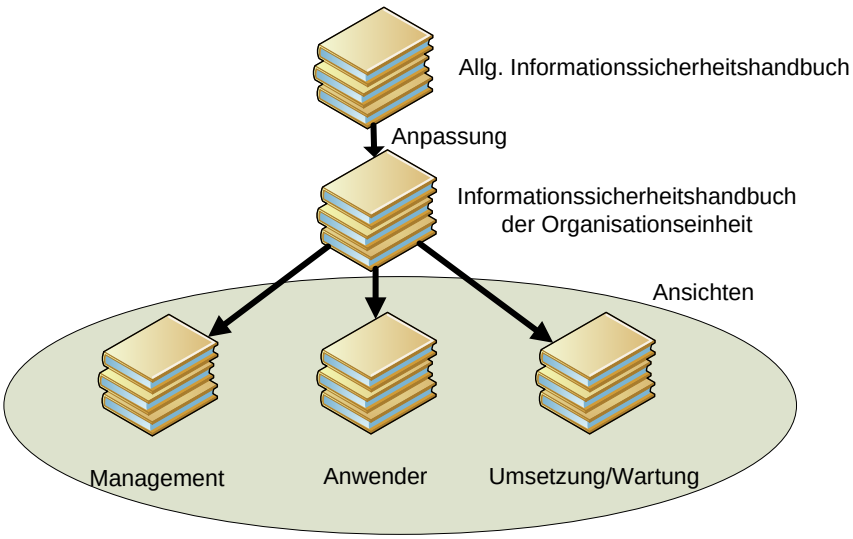


Abbildung 13: Konzept der Personalisierung im Informationssicherheitshandbuch

Der erste Teil "Informationssicherheitsmanagement" beschreibt den grundlegenden Vorgang, Informationssicherheit in einer Behörde, Organisation bzw. einem Unternehmen zu etablieren und bietet eine konkrete Anleitung, den umfassenden und kontinuierlichen Sicherheitsprozess zu entwickeln. (Bundeskanzleramt Österreich, 2007 S. 12)

Der zweite Teil mit dem Titel "Informationssicherheitsmaßnahmen" beschreibt die konkreten Einzelmaßnahmen auf organisatorischer, personeller, infrastruktureller und technischer Ebene, sodass den spezifischen Bedrohungen angemessene Standardsicherheitsmaßnahmen für IT-Systeme und Informationen entgegengesetzt werden können. Dabei wird besonders auf die spezifisch österreichischen Anforderungen, Regelungen und Rahmenbedingungen, aber auch auf die durchgängige Einbeziehung des gesamten Lebenszyklus der jeweiligen Systeme, von der Entwicklung bis zur Beendigung des Betriebs, eingegangen. Ein eigenes Kapitel wurde der "Industriellen Sicherheit" gewidmet, das Unterstützung für die Erstellung einer Sicherheitsunbedenklichkeitsbescheinigung und eine Übersicht aller für industrielle Sicherheit relevanten Vorgabedokumente aus dem nationalen, EU- und NATO-Bereich gibt. (Bundeskanzleramt Österreich, 2007 S. 12)

Teil drei des Informationssicherheitshandbuchs unterstützt die Erstellung von SSRS (System-Specific Security Requirements Statement) und SecOps (Security Operating Procedures). Dabei hilft ein Assistent bei der Erstellung der Vorlage. Der Teil drei ist selbst klassifiziert.

Das österreichische Informationssicherheitshandbuch bezieht sich, wie beim IT-Grundschutz, ausschließlich auf IT-Sicherheit. Im Kapitel vier vom ersten Teil des Handbuchs wird die Analyse der Risiken sowie drei Risikoanalysestrategien beschrieben, um die IT-Sicherheitsrisiken zu identifizieren. Weitere Elemente des Risikomanagement Prozesses werden im Kapitel fünf und sechs behandelt, jedoch auch nur bezogen auf IT-Security. Das österreichische Informationssicherheitshandbuch ist gut für IT-Risikomanagement geeignet. Dennoch ist mehr Detailierungsgrad erwünscht, da in einigen Bereichen des ersten und zweiten Teils nur allgemeines Vorgehen beschrieben wurde.

6.4. ISO/IEC 27001 und ISO/IEC 27002 (ISO 17799)

Die ISO Normen 27001 und 27002 sind Normen aus der ISO 27000-Reihe. Der ISO Standard 27001, Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, ist aus dem zweiten Teil des British Standards Institution BS 7799-2 hervorgegangen.

Der Standard, kurz „ISMS-Standard“, beschreibt in Anlehnung an die Management-Standards ISO 9001:2000 und ISO 14001:2004 ein als Prozess gestaltetes Management-System zur Einrichtung und Aufrechterhalten von Informations-Sicherheit im Unternehmen. Der Prozess und die untergliederten Teilprozesse für das Sicherheits- Management basieren auf dem aus dem Qualitäts-Management bekannten „Plan-Do-Check-Act“-Modell (PDCA). (Königs, 2006 S. 142)

Mit dem Standard wird ein Sicherheits-Management bezweckt, welches den spezifischen Geschäftsrisiken eines Unternehmens Rechnung trägt. In der „Plan“-Phase des PDCA-Zyklus werden demzufolge die Risiken im Einklang mit der Unternehmensstrategie und den Geschäftsanforderungen (rechtlich, regulatorisch oder vertraglich) erhoben und bewertet. Die „Do“-Phase enthält die Anweisungen für die Umsetzung und den effektiven Betrieb der Maßnahmen, einschließlich der dafür notwendigen Management- Aktionen. Die „Check“-Phase dient vor allem der Überwachung der Risiken und der Effizienz der Maßnahmen sowie der

laufenden Kontrolle. Die „Act“-Phase enthält den laufenden Unterhalt und die korrektiven Verbesserung sowie die Kommunikation. (Königs, 2006 S. 142)

Themen, die der ISO/IEC 27001:2005 behandelt sind:

- Begriffe und Definitionen,
- ISMS – Informationssicherheits-Managementsystem,
- Verantwortung des Managements,
- Internes ISMS Audit,
- Managementbewertung des ISMS und
- Verbesserung des ISMS.

Der ISO/IEC 27002 Standard, Informationssicherheit – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management, heißt früher ISO/IEC 17799 und wurde auf ISO/IEC 27002 umbenannt im Juli 2007 und ging aus dem ersten Teil des British Standards BS 7799-1 hervor. Die derzeitige Ausgabe des Standards ist wie folgt strukturiert [Quelle: (Königs, 2006 S. 142)]:

- Kapitel (Insgesamt 15 Kapitel, davon sind 11 Kapitel über Sicherheitsmaßnahmen)
    - Haupt Sicherheitskategorien mit je einem Maßnahmen-Ziel (Insgesamt 39)
        - Maßnahmen (Controls, insgesamt 133)
            - Umsetzungshinweise
            - Andere Informationen

Die Themen des ISO/IEC 27002 Standards sind:

- Risikobewertung und -behandlung,
- Sicherheitsleitlinie,
- Management von organisationseigenen Werte,
- Personalsicherheit,
- Physische und umgebungsbezogene Sicherheit,
- Betriebs- und Kommunikationsmanagement,
- Zugangskontrolle,
- Beschaffung, Entwicklung und Wartung von Informationssystemen,
- Umgang mit Informationssicherheitsvorfällen,
- Sicherstellung des Geschäftsbetriebs (Business Continuity Management) und

- Einhaltung von Vorgaben (Compliance).

Die Standards ISO 27001 und 27002 beziehen sich ausschließlich auf das Thema IT-Security und decken das Thema sehr gut ab. Die detailierten Vorgehensweisen für das IT-Risikomanagement findet man jedoch nirgendwo in den Standards. Lediglich im Kapitel vier des ISO 27002 Standards findet man eine einzige Seite zum Thema Risikoeinschätzung und -behandlung. Das Fehlen der Vorgehensweise für das IT-Risikomanagement soll jedoch nicht als Nachteil betrachtet werden, denn man hat dadurch die Freiheit, selbst eine IT-Risikomanagement-Methode auszuwählen, die für das Unternehmen am besten geeignet ist. Man kann z.B. ISO 27005 verwenden, falls man bei der ISO 27000 Reihen bleiben möchte.

6.5. EBIOS

EBIOS bedeutet Expression des Besoins et Identification des Objectifs de Sécurité (Deutsch: Sicherheitsbedarfsanalyse und Identifizierung von Sicherheitszielen) und ist eine Methode zur Behandlung von IT-Risiken. Es wurde im Jahr 1995 durch DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) entwickelt. Die neuste Version vom EBIOS ist die Version zwei vom Februar 2004.

Die EBIOS-Methode findet eine breite Nutzung im öffentlichen Bereich Frankreichs (alle Ministerien und nachgeordnete Behörden). Neben dem öffentlichen Bereich ist EBIOS auch sehr in Privatsektoren im Frankreich sowie in französischsprachigen Ländern/Regionen wie z.B. Quebec, Tunesien oder Belgien verbreitet.

Alle Dokumente der EBIOS-Methode sind kostenlos über die Webseite der DCSSI erhältlich. Neben den Dokumenten ist die EBIOS-Software ebenfalls kostenlos erhältlich und mit verschiedenen Betriebssystemen (Windows, Linux und Solaris) kompatibel. Sie ist ein Unterstützungswerkzeug für die EBIOS-Methode und erleichtert die Umsetzung der IT-Risikoanalyse. Genaueres über die Software findet man im Evaluierungsteil.

Dir Quellcode der Software ist ebenfalls über die Webseite der DCSSI erhältlich und kann von jeden genutzt und angepasst werden, wenn die Entwicklungen bzw. die Modifizierungen an der Software an DCSSI weitergeleitet werden.

Die EBIOS-Methode besteht aus fünf sich ergänzenden Abschnitten.

- Einführung

- Methodik
- Techniken
- Mittel zur IT-Risikobewertung
- Mittel zur Behandlung von IT-Risiken

Die folgende Abbildung zeigt die globale Methodik der EBIOS dar.

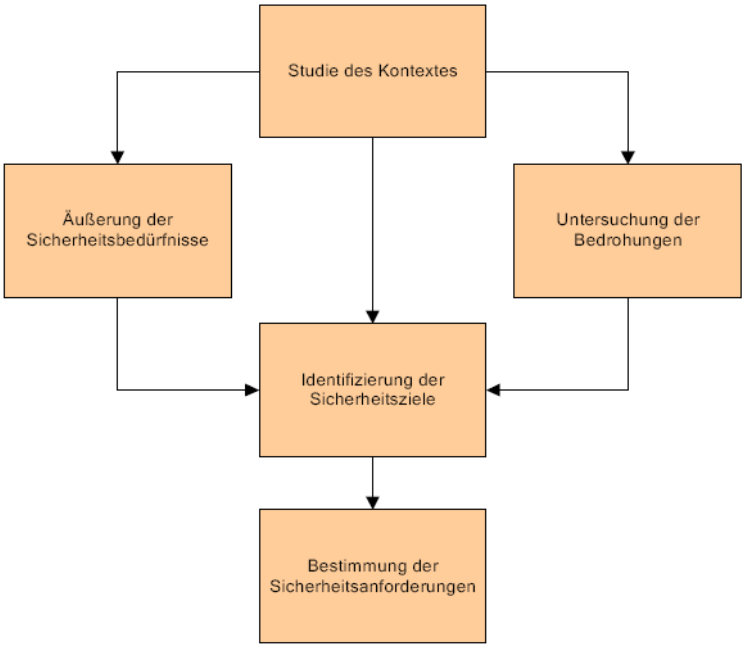


Abbildung 14: Globale EBIOS-Methodik (DCSSI, 2004 S. 6)

Der erste Schritt der EBIOS-Methodik ist die Studie des Kontextes. Wie aus den Namen ableitbar, ist die Aufgabe des ersten Schritts die Studie sowie globale Identifizierung des Zielsystems und seine Position in der Umgebung. Der erste Schritt setzt sich aus insgesamt drei Aktivitäten zusammen:

- Untersuchung der Institution
- Studie des Zielsystems
- die Bestimmung des Ziels der Sicherheitsstudie

Durch den Schritt eins können die für das System absehbaren Konsequenzen, sein Benutzungskontext, die sicherzustellenden Aufgaben oder Dienstleistungen und die eingesetzten Mittel bestimmt werden. Dieser Schritt dient auch dem Zusammentragen aller Informationen, die zur Planung der Studie erforderlich sind. Am Ende dieses Schrittes ist das Nachforschungsfeld der Studie klar abgegrenzt, die Hypothesen, Verpflichtungen und Zwänge sind erfasst und die zu behandelnden Themen sind bekannt. (DCSSI, 2004 S. 7)

Die Analyse des Sicherheitsbedarfs ist der zweite Schritt der EBIOS-Methodik und lässt sich in zwei Aktivitäten aufteilen:

- Realisierung der Bedürfnisblätter
- Zusammenfassung der Sicherheitsbedarfe

Ziel der ersten Aktivität ist die Erstellung von Tabellen, die für die Sicherheitsbedarfsanalyse durch die Nutzer notwendig sind. Mit Hilfe dieser Tabellen können die Nutzer objektiv und kohärent die Sicherheitsbedarfe der Elemente äußern, mit denen sie im Rahmen der Ausübung ihrer Tätigkeit gewöhnlich zu tun haben. (DCSSI, 2004 S. 12) In der zweiten Aktivität des zweiten Schrittes der EBIOS-Methodik wird der nötige Sicherheitsbedarf zusammengefasst. Hier wird jedem Element ein Sicherheitsbedarf pro Sicherheitsgrundwert zugewiesen.

Der dritte Schritt der EBIOS-Methodik ist die Bedrohungsanalyse. Ziel des dritten Schrittes ist die Bestimmung und die Beschreibung der Bedrohungen auf das System. Dieser Schritt besteht aus insgesamt drei Aktivitäten:

- Untersuchung der Ursprünge der Bedrohungen
- Studie der Schwachstelle
- Formalisierung der Bedrohungen

Der vierte Schritt trägt zur Evaluierung und Behandlung der Risiken bei. Er dient der Formalisierung der Risiken, die tatsächlich auf dem System lasten, indem die Bedrohungen (negative Ereignisse) dem Sicherheitsbedarf (Konsequenzen) gegenübergestellt werden. Die Risiken werden durch Sicherheitsziele abgedeckt, die unter Berücksichtigung der Hypothesen, Sicherheitsvorschriften, Vorschriftsreferenzen, des Betriebsmodus und der identifizierten Zwänge definiert wurden. Sie bilden zusammen das Sicherheitslastenheft. (DCSSI, 2004 S. 7) Der vierte Schritt besteht aus insgesamt drei Aktivitäten:

- Gegenüberstellung von Bedrohungen und Bedürfnissen
- Formalisierung der Sicherheitsziele
- Bestimmung der Sicherheitsniveaus

Die Aufgaben der Aktivitäten leiten sich bereits von deren Namen ab. Weitere Details zu den Aktivitäten findet man im Abschnitt zwei vom EBOIS.

Der letzte Schritt der EBIOS-Methodik sind die Bestimmungsanforderungen, die zwei Aktivitäten umfassen: Bestimmung der funktionellen Sicherheitsanforderungen und Bestimmung der Sicherheitsgewährleistungsanforderungen. Ziel dieses Schritts ist es, zu bestimmen, wie man die Sicherheitsziele erreichen kann und wie man den Risiken, die das System bedrohen, entgegentreten kann.

EBIOS ist eine gut geeignete Methode für das IT-Risikomanagement. Sie wird im öffentlichen Sektor in Frankreich und in vielen Unternehmen in der EU eingesetzt. Die EBIOS-Methode ist sehr einfach zu verstehen und anzuwenden. Mit der Hilfe der EBIOS-Software, die kostenlos erhältlich ist, wird die Durchführung einer EBIOS-Studie erheblich beschleunigt bzw. vereinfacht. Neben der EBIOS-Methode wird auch eine Wissensdatenbank angeboten. Diese Datenbank besteht aus zwei Teilen. Im ersten Teil der Datenbank sind Mittel zur Risikobewertung enthalten und im zweiten Teil der Datenbank sind Wege zur Behandlung von IT-Risiken beschrieben.

Die Dokumente von EBIOS sind kostenlos über die Homepage der DCSSI erhältlich. Sie stellen einen sehr großen Vorteil dar, wenn man sie mit andere Methoden oder ISO Normen vergleicht. Der ISO/IEC 27005:2008 Standard kostet laut Shop des österreichischen Normungsinstituts € 112,20 (Stand August 2008) und hat einen Umfang von 55 Seiten. Umgerechnet kostet es genau € 2,04 für eine Seite von ISO/IEC 27005:2008. Bei EBIOS kostet genau € 0,00 pro Seite. Einhundert Euro ist für ein Unternehmen nicht viel, aber warum soll man zahlen, wenn eine andere Methode inklusiv Software kostenlos erhältlich ist?

6.6. ITIL

Die Abkürzung ITIL bedeutet „Information Technology Infrastructure Library“ und ist eine Sammlung von Dokumenten, die die IT-Management-Prozesse, -Methoden und -Konzepten beschreiben. In den letzten Jahren hat sich ITIL in vielen großen und mittelständischen Unternehmen etabliert und kann eigentlich schon als einen de-facto Standard gesehen werden. Man muss heute zwischen zwei Versionen von ITIL unterscheiden:

- ITIL Version 2 (abgelöst durch die Version 3)
- ITIL Version 3 (seit 1. Juli 2007)

Das Thema ITIL ist sehr umfangreich und kann man in einem Unterkapitel nicht umfassend beschrieben werden. Deshalb wird in diesen Unterkapitel lediglich eine kurze Einführung über ITIL sowie den Bezug zum IT-Risikomanagement kurz vorgestellt.

Folgende Abbildung zeigt die Struktur gemäß ITIL Version zwei dar.

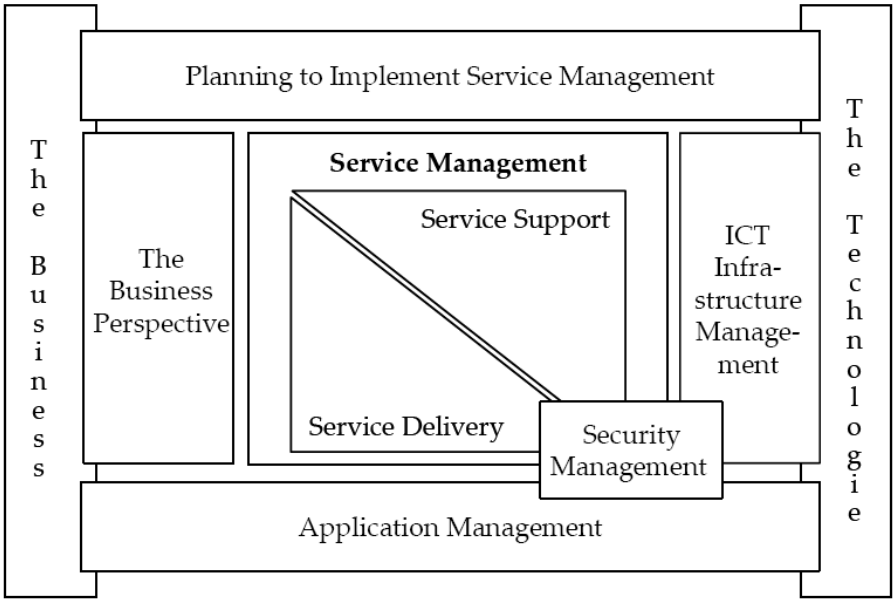


Abbildung 15: ITIL V2 Rahmenstruktur (Buchstein, et al., 2007 S. 8)

Aus der Abbildung erkannt man insgesamt sechs Kernblöcken, die die Kernstruktur des ITIL V2 abbildet. Relevant für die IT-Service Management Prozesse sind „Service Management“, die wiederum in „Service Support“, „Service Delivery“ und „Security Management“ aufgeteilt sind.

ITIL V3 ist deutlich umfangreicher und an einigen Stellen auch präziser geworden. Mit den Erfahrungen der vergangenen zehn Jahre wurden bekannte Lücken und Schwachstellen geschlossen. Die Kerninhalte der sechs ITIL V2 Bände sind in weiten Teilen eingeflossen. So sind jetzt auch bislang meist zu kurz gekommene Themen, beispielsweise aus den Bereichen Application Management oder Infrastructure Management, im Gesamtkonzept enthalten. Das neue ITIL V3 verfolgt die ganzheitliche Sicht auf das Service Management und reflektiert daher stark auf die Integration von Business und IT, auf die jüngsten Entwicklungen in der IT und in der Technik sowie auf die Innovationsfähigkeit der Unternehmen. Auch Bezüge auf geltende Normen und andere Best Practice oder Vorgehensmodelle, wie z.B. ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 27002, CMMI, COBIT, PRINCE2, PMBOK, Six Sigma, SOX, oder SOA, sind an diversen Stellen zu finden. (Olbrich, 2008 S. 144)

Die folgende Abbildung das das ITIL V3 Prozessmodell:

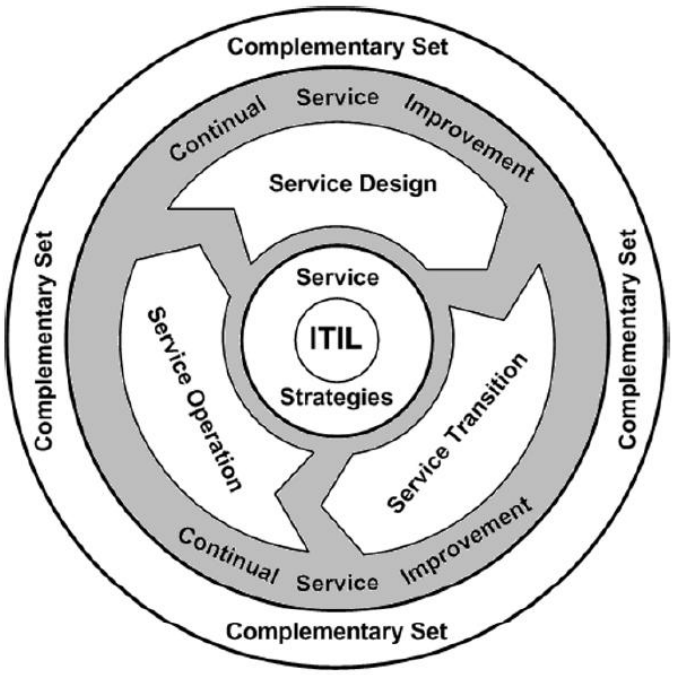


Abbildung 16: ITIL V3 Prozessmodell (Olbrich, 2008 S. 145)

Im Zentrum des ITIL V3 Frameworks ist das Kerngebiet Service Strategies, das maßgeblich auf alle Prozesse einwirkt. Die Kerngebiete Service Transition, Service Operation und Service Design umranden das Kerngebiet Service Strategies. Alle oben beschriebenen Kerngebiete werden von Continual Service Improvement (CSI) umrandet. Die Aufgabe vom CSI ist die Darstellung der Effizienz und Effektivität aller Prozesse anhand von messbaren Kriterien und die Ausschöpfung der Verbesserungspotentiale. Schließlich werden alle Gebiete vom Complementary Set umfasst. Das Complementary Set enthält praxisbezogenen Vorlagen, Empfehlungen und Beispielen zu jeden Kerngebieten von ITIL V3. Weitere Kerngebiete vom ITIL V3 werden hier aufgrund des Umfangs hier nicht mehr behandelt. Falls jemand genaueres über ITIL V3 wissen möchte, ist das Kapitel „ITIL V3 – Die dritte Generation“ vom Buch „ITIL Kompakt und verständlich“ sehr empfehlenswert.

Die IT-Risiken werden sowohl im ITIL V2 als auch ITIL V3 in unterschiedlichen Prozessen betrachtet. Es gibt jedoch keinen spezifischen Prozess für das IT-Risikomanagement. Wenn man ein wenig nachdenkt, ist ITIL auch kein „Standard“, der primär auf die Informationssicherheit oder Risikomanagement abzielt. Jedoch können Teile von Prozessen wie etwa Security Management (ITIL V3: Information Security Management) als Basis in ein IT-Risikomanagement eingegliedert werden.

6.7. NIST 800-30

Der Begriff „NIST" bedeutet das amerikanische National Institute of Standards and Technology und ist eine Bundesbehörde der Vereinigen Staaten von Amerika. Der frühere Name dieser Behörde war „The National Bureau of Standards“ (1901-1988).

Im NIST 800-Serie werden Standards für die Sicherheit von Informationssystemen definiert. Der Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30) erläutert den grundlegenden Ablauf von IT-Security Management anhand des IT-System-Lebenszyklus und verweist hinsichtlich der Detailausprägungen auf andere NIST Standards wie beispielsweise NIST 800-27 Engineering Principles for IT-Security oder den NIST 800-14 Generally Accepted Principles and Practices for Securing Information Technology. (Seibold, 2005 S. 191)

Da NIST 800-30 Standard viele Ähnlichkeiten mit den vorher beschriebenen Standards hat wird hier auf eine ausführliche Beschreibung des Standards verzichtet. Die Schwerpunkte des NIST 800-30 Standards sind Risk Assessment und Risk Mitigation. Man muss jedoch erwähnen, dass der NIST 800-30 zwar das IT-Risikomanagement im Bereich Security unterstützt, jedoch kein umfassendes IT-Risikomanagement darstellt.

Zum Schluss dieses Abschnitts soll noch erwähnt werden, dass der Risikomanagement Standard nach NIST zurzeit neu gestaltet wird. Der hier kurz beschriebene NIST 800-30 Standard wird überarbeitet und beschäftigt sich in der Zukunft ausschließlich mit dem Thema Risk Assessment. Er stellt nur ein Teilprozess des neuen Risikomanagement Framework dar. Ein Entwurf der neu überarbeiteten NIST 800-30 Special Publication „Guide for Conducting Risk Assessments“ soll demnächst erscheinen.

Das neue Risikomanagement Framework wird in der NIST Special Publication 800-39 „Managing Risk from Information Systems – An Organizational Perspective“ beschrieben. Es ist zurzeit noch in der Entwurfsphase und es gibt lediglich einen zweiten öffentlichen Entwurf, den man von der Webseite von NIST Computer Security Resource Center herunterladen kann. Die folgende Abbildung zeigt das neue Risikomanagement Framework im zweiten öffentlichen Entwurf von NIST 800-39.

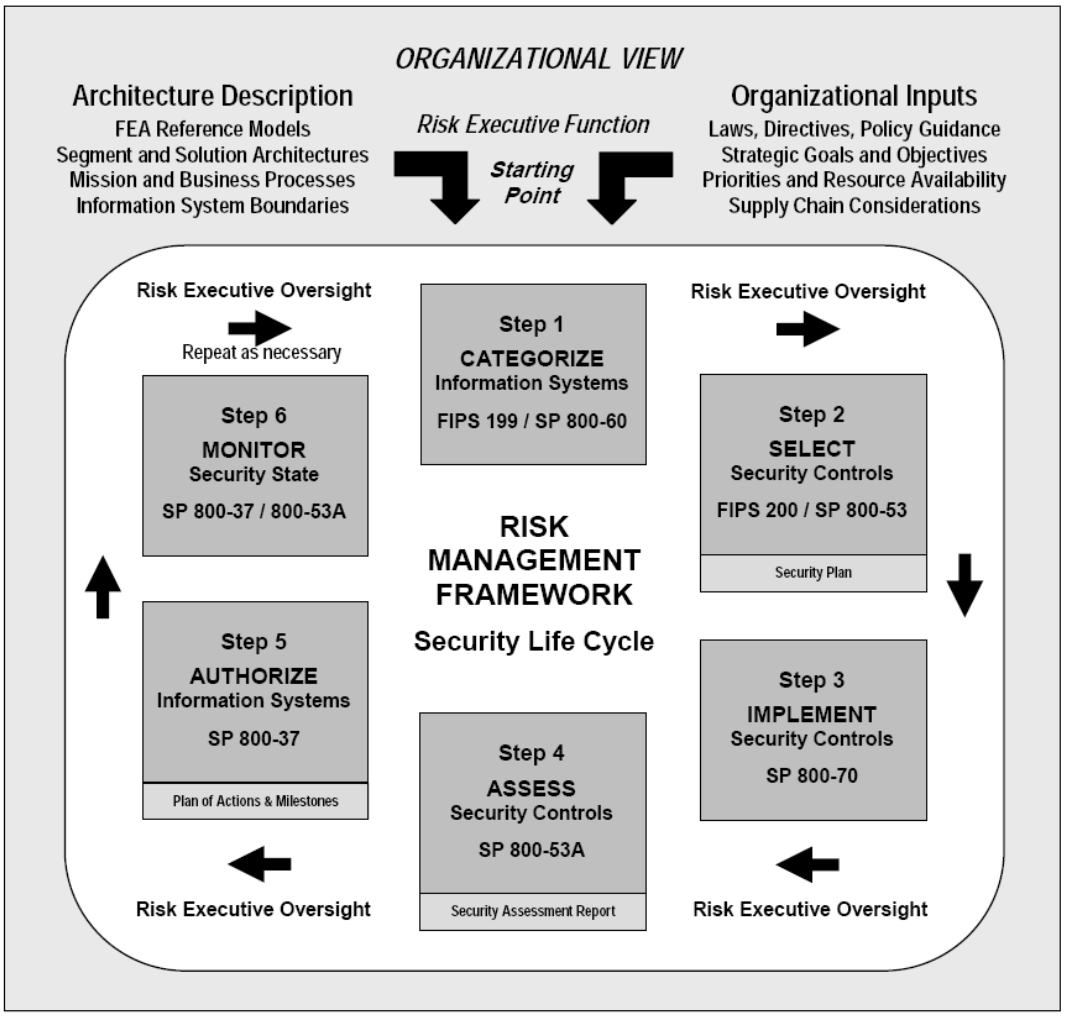


Abbildung 17: NIST 800-39 Risk Management Framework (National Institute of Standards and Technology, 2008 S. 28)

Wie beim derzeitigen NIST 800-30 Standard verweist NIST 800-39 hinsichtlich der Detailausprägungen auf andere NIST Standards. Laut Entwurfsdokument unterstützen insgesamt elf NIST und FIPS Special Publications beim Aufbau des Risikomanagement Frameworks nach NIST 800-39. Da NIST 800-39 zurzeit noch im Entwurfsstadium ist, wird auf eine weitere ausführlichere Beschreibung verzichtet.

7. Arten von IT-Risikomanagement-Software

Es existieren im Markt hunderte von IT-Risikomanagement-Tools. Man kann jedoch nicht alle Tools gleichsetzen, da sie sehr unterschiedlich sind. Außerdem gibt es noch RM-Lösungen, die selbst entwickelt wurden bzw. auf Standardsoftware basiert sind. Man kann generell vier Arten von RM-Software unterscheiden:

- Eine selbstentwickelte RM-Lösung
- RM Software, die auf Standardsoftware basiert
- Standardisierte Spezialprogramme für Risikomanagement
- RMIS – Risk Management Information Systems

Es gibt Unternehmen, bei denen ein Einsatz von IT-Risikomanagement-Software von anderen Unternehmen aus bestimmten Gründen (z.B. Unternehmenspolitische Entscheidungen) nicht befürwortet wird. In diesem Fall wird oft eine eigene Risikomanagement Lösung entwickelt. Nachteil einer solchen Lösung ist natürlich der hohe Aufwand, da eine selbstentwickelte IT-Risikomanagement-Lösung den ganzen Softwareentwicklungsprozess durchlaufen muss. Der Vorteil einer selbstentwickelten Risikomanagement-Lösung ist die vollständige Integration im bestehenden System des Unternehmens. Der Datenaustausch zwischen den anderen Systeme des Unternehmens läuft daher im diesem Fall problemlos.

Mit Hilfe einer Standardsoftware, die in meisten Unternehmen vorhanden ist, kann man auch Risikomanagement durchführen. Ein Beispiel dafür ist das Betreiben von Risikomanagement mit der Hilfe von Office Paketen. Simulationsprogramme, wie beispielsweise Crystal Ball oder @Risk, können als „Add-Ins“ zu Tabellenkalkulationsprogrammen (Microsoft Excel) genutzt werden und ermöglichen eine quantitative Beschreibung von Risiken mittels geeigneter Verteilungsfunktionen (z.B. Normalverteilung) sowie die Aggregation von Risiken (Zusammenfassung von Risiken zu einer Gesamtrisikoposition). (Gleißner, et al., 2005 S. 159) Mit Hilfe der Datenbanksoftware wie Microsoft Access oder MySQL Server können die Risiken zusammengefasst und ausgewertet werden. Mit Textverarbeitungssoftware wie z.B. Microsoft Word oder OpenOffice Writer können die Dokumente für das IT-Risikomanagement erstellt werden. Solche Programme sind zwar relativ günstig oder sogar kostenlos (z.B. Open Office und MySQL Server sind kostenlos erhältlich), jedoch ist der Funktionsumfang relativ begrenzt und eine Kommunikation zwischen verschiedenen Systemen des Unternehmens ist beschränkt oder muss selbst adaptiert werden.

Standardisierte Programme, die speziell für IT-Risikomanagement gedacht sind, sind ebenfalls recht günstig erhältlich. Solche Programme sind meistens Einzelplatzlösungen und bereits auf den Bedarf von IT-Risikomanagement ausgerichtet. Solche Programme sind jedoch auch schwierig in der vorhandenen IT-Landschaft des Unternehmens zu integrieren und sollen nicht im großen Unternehmen eingesetzt werden.

Große Unternehmen mit mehreren hunderten oder tausenden Mitarbeitern sollen im Gegensatz zu vorher erwähnten Softwarelösungen RMIS (Risk Management Information Systems) einsetzen. Solche Systeme sind sehr unternehmensindividuell gestaltbar und können vollständig in das Unternehmen integriert werden.

Derartige Softwaresysteme können ein umfassendes Leistungsspektrum für das Risikomanagement anbieten, und bieten dabei die Möglichkeit möglichst die traditionellen Controlling- und Unternehmensplanungsverfahren zu einer „chancen- und risikoorientierten Planung“ („Stochastische Planung“) weiterzuentwickeln, in der für sämtliche Planungspositionen die risikobedingte Bandbreite (Umfang möglicher Planabweichungen) berechnet werden kann (Gleißner, et al., 2005 S. 160)

8. Evaluierung von IT-Risikomanagement-Software

Im letzten Kapitel wurden die Arten von IT-Risikomanagement Software vorgestellt. In diesen Kapitel soll die Kernfrage dieser Masterarbeit beantwortet werden: Im ersten Teil dieses Kapitels wird ein Kriterienkatalog für die Evaluierung beschrieben. Im zweiten Teil dieses Kapitels werden die zu evaluierenden Tools anhand einiger ausgewählten Evaluierungskriterien miteinander verglichen.

8.1. Evaluierungskriterien

Die Evaluierung der Softwarelösungen ist nicht so leicht zu gestalten, da es keinen eigenen Standard für IT-Risikomanagement gibt. Der Funktionsumfang der zu evaluierenden Tools ist auch sehr verschieden. Es gibt Tools, die nicht nur das IT-Risikomanagement beherrschen, sondern auch andere Funktionen wie Compliance Management oder IT Audits. Es gibt auch Tools, die nur einen bestimmten Standard oder Best Practices unterstützen wie z.B. GSTOOL, das auf IT-Grundschutz basiert.

Bei der Festlegung der Evaluierungskriterien soll daher sichergestellt werden, dass der Schwerpunkt der Softwareevaluierung der Unterstützung der IT-Risikomanagement-Methode dient. Die Vor- oder Nachteile von Standards oder Best Practices haben hier keine Bedeutung. Außerdem soll versucht werden, die Software nach Qualitätskriterien von ISO 9126 zu beurteilen, vorausgesetzt, dass die Bewertung der Qualitätskriterien im Rahmen der Arbeit aufgrund der beschränkten Ressourcen möglich ist.

Generell kann man aber trotzdem die Evaluierung der Risikomanagement-Software in folgende Schwerpunkte/Schritte unterteilen:

- Modellierung anhand eines Business Cases
- Softwarearchitektur
- Import/Export bzw. Austausch von Daten
- Risikomanagement Techniken
- Risk Reporting
- Usability und Layout
- Weitere unterstützende Funktionen, falls vorhanden

Die obigen Punkte stellen jedoch nicht die gesamte Evaluierung dar. Es kann durchaus sein, dass bei einem bestimmten Tool weitere Schwerpunkte aufgrund des unterschiedlichen Funktionsumfangs dazukommen.

Modellierung anhand eines Business Cases

Für die Evaluierung der RM Tools wurde ein Business Case erstellt, der im Anhang der Arbeit zu finden ist. Der Business Case enthält grundlegende Informationen über die IT Infrastruktur eines fiktiven mittelständisches Unternehmens und Interviews von IT Verantwortlichen im Unternehmen. Mit der Hilfe des Business Cases soll es möglich sein, das IT-Risikomanagement mit Hilfe des RM-Tools zu betreiben.

Bei der Modellierung geht man von der folgenden Situation aus:

> *Sie sind der neu ernannte Verantwortliche für das IT-Risikomanagement im Unternehmen. Bisher wurde das IT-Risikomanagement im Unternehmen ein wenig vernachlässigt. Nach einem sehr ernsten Zwischenfall hat man entschieden, in diesem Bereich professioneller umzugehen. Es wurde eine RM-Software vom IT-Manager eingekauft und Sie sollen nun das Programm einrichten und die Daten eingeben.*

Bei der Modellierung gewinnt man den ersten Eindruck über das RM-Programm. Man soll jedoch wissen, dass der Business Case keine vollständige Information über die IT-Landschaft bzw. die IT-Prozesse enthält. Weiters gibt es kein vordefiniertes Ergebnis für die Modellierung. Der Tester soll nach eigenem Ermessen vorgehen, falls ein bestimmter Bereich nicht modelliert werden kann.

Softwarearchitektur

In diesem Bereich wird die Architektur der Risikomanagement-Lösung bewertet. Dabei muss man beachten, dass der Business Case eine typische mittelständige Firma beschreibt. Somit ist nicht jede Architektur geeignet. Am Beginn soll man den groben Aufbau der Software beschreiben. Danach soll man Überlegungen anstellen, wie gut die Architektur der Software für den Einsatz geeignet ist. Eine simple Desktop Anwendung ist nicht unbedingt für eine Firma mit über 500 Mitarbeiten geeignet. Dabei soll man die Firma, beschrieben im Business Case, orientieren und bewerten.

Ein weiteres wichtiges Evaluierungskriterium ist der Aufwand für die Einführung von IT-Risikomanagementsystemen. Es hat kein Sinn, ein supertolles Produkt zu kaufen, wenn man die vorhandenen Geschäftsprozesse radikal verändern bzw. großen Aufwand für Integration der vorhandenen Prozesse des Unternehmens betreiben muss. Neben der Integration in die Geschäftsprozesse soll man auch den Aufwand auf technischer Ebene evaluieren. Dabei soll man sich die Frage stellen, ob die technische Infrastruktur wie z.B. das Netzwerk für die Einführung von IT-Risikomanagement Systeme verändert werden muss. Hier spielen dabei die Kosten für die Veränderung eine große Rolle. Die Kosten der Einführung müssen für das Unternehmen erträglich sein. Es ist nicht nützlich, wenn man neben dem Kauf der Software noch viel Geld in die technische Infrastruktur investieren muss, so dass die Vorteile gegenüber den anderen IT-Risikomanagement Lösungen wieder bedeutungslos werden.

Nachdem man die allgemeine Softwarearchitektur behandelt hat, soll man dann mehr in die Architekturdetails gehen. Dieser Teil ist natürlich abhängig von der Softwarearchitektur, so dass man hier keine konkreten Evaluierungskriterien vorgeben kann. Es sollen aber auf jeden Fall die Aspekte wie Zugriffsmöglichkeiten oder die Sicherheit evaluiert werden.

Ein Beispiel: Die Software hat eine verteilte Client-Server Struktur. Es soll evaluiert werden, wie der Zugriff auf das System erfolgt. Folgende Fragen können von Relevanz sein:

- Muss man ein Programm auf jedem Client PC installieren oder reicht ein Browser wie z.B. Internet Explorer?
- Wie läuft die Anmeldung in das System ab und wie wird die Software geschützt?
- Läuft die Kommunikation über einen gesicherten Tunnel ab, die man vor Anmeldung aufbauen muss oder werden andere Standardtechnologien wie z.B. TLS (Transport Layer Security) für die Übertragung verwendet?

Import/Export und Austausch von Daten

Ein wichtiges Kriterium für die Evaluierung ist der Import bzw. Export von verschiedenen Daten. Viele Unternehmensdaten existieren bereits in irgendeinem elektronischen Format. Unter Unternehmensdaten kann man verschiedenes wie Geschäftsprozesse, Stellenbeschreitung, Bedrohungskataloge, Daten von Vulnerability Assessment usw. verstehen. Ein Import von existierenden Daten kann die Modellierung vereinfachen und man muss nicht alle Daten erneuert in die Risikomanagement Lösung eingeben.

Beim Import gibt es jedoch eine sehr große Hürde. Die Daten können in verschiedensten Formaten (CSV, XML usw.) gespeichert sein. Das System muss daher mit unterschiedlichen Datenformaten klar kommen. Damit die Software mit „exotischen“ Formaten zu Recht kommt, soll es eine Möglichkeit geben, eine eigene Mapping zu definieren. Falls es eine Möglichkeit gibt, Mapping zu definieren, soll man noch diese noch ausführlicher beschreiben.

Die Exportfunktion von Daten aus dem IT Risikomanagement System kann auch von großer Relevanz sein. Ein Unternehmen besteht meistens aus mehreren Systemen, die miteinander kommunizieren. Es ist daher erforderlich, dass man Daten aus Risikomanagementsystem exportieren kann, um anschließend in ein anderes System zu importieren oder für andere Zwecke verwenden zu können. Wie beim Datenimport soll es für die Exportfunktion auch eine Möglichkeit geben, um ein eigenes Mapping zu erstellen, um exotische Datenformate zu unterstützen.

Neben dem Datenexport soll man auch evaluieren, ob der Software eine oder mehrere Schnittstellen zur Verfügung stehen, damit sie direkt von anderen Systemen des Unternehmens angesprochen werden. Wenn es eine solche Schnittstelle gibt, soll die Exportfunktion weniger gewichtet werden.

Risikomanagement Techniken

Die Bewertung von Risikomanagement Techniken hat eine große Bedeutung in der Evaluierung, falls die RM-Software mehrere Standards unterstützt. Zuerst soll festgestellt werden, welche Managementtechniken die Software unterstützt. Es ist besser, wenn das Programm mehrere Techniken beherrscht. Natürlich verwendet man nur eine Managementtechnik für Risikomanagement. Es ist natürlich vorteilhafter, wenn mehrere Optionen zur Auswahl stehen.

Nachdem man die unterstützenden Techniken festgestellt hat erfolgt die Evaluierung anhand des Business Cases. Anhand der Modellierung mit Business Cases wird festgestellt, wie gut das Risikomanagement System die Managementtechniken unterstützt. Die Probleme bei der Modellierung sollen vermerkt sein und in die Bewertung einfließen. Nach der Bewertung der Managementtechniken sollen Vorschläge zur Verbesserung geben, falls das Programm noch Potential zur Verbesserung hat.

Risk Reporting

Ein wichtiges Kriterium ist das Erstellen von Berichten. Die erstellten Berichte dienen meistens als Entscheidungsgrundlage für das Management. Die Geschäftsführung braucht sie in verschiedensten Ausführung bzw. Formen. Daher soll die Evaluierung von Reporting auf folgende Kernpunkte eingehen:

- Arten von Berichte, abhängig von der RM-Managementtechnik
- Möglichkeit für die Generierung von benutzerdefinierte Berichte
- Layout für die generieten Berichte
- Unterstützende Dokumentenformat (Office, PDF usw.)
- Verwaltung von generierten Berichten.

Weitere unterstützende Funktionen

Hier sollen die übrigen Funktionen, die den Risikomanagementprozess unterstützten, evaluiert werden. Ein Beispiel für eine unterstützende Funktion ist das Bereitstellen von Templates für bestimmten Standards oder Best Practices (z.B. ISO 17799), damit man den Ablauf der Modellierung beschleunigen kann.

Ebenfalls wird hier die Verwaltung des Risikomanagement Systems bewertet. Die Administrierbarkeit des Systems steht hier im Vordergrund. Dabei soll man auf die Aspekte wie Benutzerverwaltung, Benutzerrechteverwaltung, Datenzugriffsverwaltung und unter anderem Datensicherung genauer eingehen.

Da die Funktionalitäten der Risikomanagement-Programme verschieden sind, kann es vorkommen, dass je nach Funktionskatalog des Programmes weitere Evaluierungskriterien als Funktionen hinzugefügt wird.

Usability und Layout

Ein hoch entwickeltes Produkt ist nutzlos, wenn es nicht gebrauchstauglich ist. Der Schwerpunkt der Evaluierung in diesem Bereich liegt daher eindeutig bei der Usability (dt. Gebrauchstauglichkeit) des Produkts. Gemäß DIN EN ISO 9241 Teil 11 ist Usability definiert als:

> *„Usability ist das Ausmaß, in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen".*

DIN EN ISO 9241 ist ein internationaler Standard, der Richtlinien der Interaktion zwischen Mensch und Computer beschreibt. Die Definition im Teil 11 ist zwar nicht auf die Gebrauchstauglichkeit eines Softwareproduktes bezogen, jedoch kann man sie auch auf den Bereich der Software-Usability übertragen.

Schlussbemerkung Evaluierungskriterien

Wie man aus den Kriterienkatalog erkennt, sind die Kriterien in zwei Bereiche aufgeteilt: Softwarequalität nach ISO 9126 und die Unterstützung der IT-Risikomanagement-Methode. Nicht alle Softwarequalitätsmerkmale von ISO 9126 können bewertet werden, da die notwendigen Ressourcen bzw. Unterlagen fehlen. Bei einer Bewertung des Merkmals „Reife“ sind beispielsweise die Unterlagen aus der Softwareentwicklung erforderlich, um die Qualität zu bewerten. Solche Unterlagen stehen für die Evaluierung jedoch nicht zur Verfügung. Es ist daher ausreichend, eine kurze Zusammenfassung nach der Modellierung anhand des Business Cases über die Softwarequalität der Risikomanagement-Software zu erstellen

8.2. Evaluierungsergebnis

Es wurde insgesamt drei IT-Risikomanagement-Software im Rahmen dieser Arbeit evaluiert. Die folgende Auflistung zeigt in dieser Arbeit evaluierten Softwares.

- GSTOOL
  http://www.bsi.bund.de
- EBIOS
  http://www.ssi.gouv.fr
- Rimanis
  http://www.hulocon.de

Bevor man mit dem Vergleich beginnt, soll noch erwähnt werden, dass die Suche nach IT-Risikomanagement-Software Programmen relativ leicht ist. Sehr viele IT-Risikomanagement-Software Programme wurden nach einer kurzen Suche im Internet gefunden. Das größte Problem ist jedoch das Anfordern eines Testzugangs. Es wurden sehr viele Anfragen über einen Testzugang per E-Mail versandt. Das Ergebnis der Anfragen ist jedoch sehr enttäuschend. Laut Auswertung werden zirka 70% der Anfragen nicht beantwortet. In den beantworteten E-Mails ist meistens eine Absage enthalten. Nur die Firma HULOCON GmbH hat

nach der Anfrage eine Testversion ohne wenn und aber zur Verfügung gestellt. Die Testversion von GSTOOL und die EBIOS-Software sind im Web ohne Anfragen frei erhältlich.

Wie bereits am Anfang des Kapitels erwähnt, werden hier die unterschiedlichen Software Programme anhand einiger wichtigen Kriterien aus dem Evaluierungskatalog miteinander verglichen. Sinn dieses Vergleichs ist es, den Lesern das Durchlesen der Evaluierung zu erleichtern, da die IT-Risikomanagement-Tools nach gewissen Kriterien verglichen werden. Neben diesem Vergleich findet man alle Details der Evaluierungen in den Kapiteln neun, zehn und elf.

Installation

GSTOOL Die Installation von GSTOOL wird vom einen Setup-Programm unterstützt. Die Installation einer Datenbank-Engine ist verpflichtend, auch wenn man einen zentralen Datenbankserver wie z.B. MS-SQL verwenden will. Die lokale Version der IT-Grundschutz-Kataloge wird nicht mit installiert, auch wenn man eine vollständige Installation ausgewählt hat.

EBIOS Für die Installation braucht man nur die komprimierte ZIP-Datei in den gewünschten Ordner zu extrahieren und anschließend die Datei `ebios.exe` zu starten, um die Software zu starten.

Rimanis Man muss zuerst vor der Installation von Rimanis-Software die Rimanis-Datenbank installieren, da man bei der Installation der Software den Speicherort der Datenbank benötigt. Das Installationsprogramm akzeptiert die Eingabe einer UNC Ressource nicht und gibt eine Fehlermeldung zurück. Man muss daher die Netzwerkressource als Netzlaufwerk einbinden, wenn die Datenbank nicht auf dem lokalen Rechner installiert wurde.

Softwarearchitektur

GSTOOL Das GSTOOL ist eine Einzelplatzanwendung und muss lokal installiert werden. Auf jeden Rechner werden das GSTOOL-Programm und eine Datenbank installiert. Es besteht jedoch die Möglichkeit über das Netzwerk auf andere Datenbank zuzugreifen, um so ein gemeinsames Arbeit an einer Datenbank zu ermöglichen.

EBIOS Die EBIOS-Software ist eine reine Einzelplatzanwendung. Das gemeinsame Arbeiten an einer Datenbasis ist nicht möglich.

Rimanis Die Rimanis-Software muss auf jeden Computer installiert werden, auf den man mit der Software arbeiten will. Ein gemeinsames Arbeiten an einer Datenbank über ein Netzwerk ist möglich.

Benutzeradministration

GSTOOL Die Software verfolgt bei der Benutzeradministration das Anwender-Rollen-Konzept. Im Anwender-Bereich werden die benutzerspezifischen Daten gespeichert und im Rollen-Bereich die Rechte. Diese Daten sind in der Datenbank gespeichert und können problemlos übertragen werden.

EBIOS In der EBIOS-Software unterscheidet man zwei Arten von Benutzer: Administrator und Auditor. Der Administrator hat den vollen Zugriff auf die Software und der Auditor hat lediglich Zugriff auf den Audit Teil. Die Benutzerdaten werden in der Datei `passwd.xml` gespeichert. Durch das Entfernen dieser Datei kann der Passwortschutz des Programmes umgangen werden.

Rimanis Die Rimanis-Software unterscheidet zwei Arten von Benutzer: Administrator und Risiko-Zuständige. Administratoren haben den Vollzugriff auf das Programm. Die Risiko-Zuständigen können nur auf ihre Datensätze zugreifen und haben nur beschränkte Rechte in der Stammdatenverwaltung.

Import und Export

GSTOOL Das Programm bietet Funktionen für Import und Export von Daten an. Sie ermöglichen die Übertragung der Daten vom einen Client auf einen anderen. Zusätzlich bietet die Software die Möglichkeit zum Verschlüsseln bzw. Entschlüsseln der exportierten Daten. Die Verschlüsselung basiert auf den Algorithmus der Chiasmus Software.

EBIOS Die Software bietet keine Funktionen für Import und Export von Daten. Die Daten sind jedoch im XML Format im Verzeichnis `Data` gespeichert und können ohne Probleme kopiert werden.

Rimanis In der Rimanis-Software gibt es keine Möglichkeit, die bereits existierenden Daten zu importieren. Die Exportfunktion von Rimanis ist auch nicht sonderlich fortgeschritten. Man kann lediglich Name, Risiko-Erwartungswert und maximale Vermögensminderung eines Einzelrisikos exportieren. Beim Export kann man zwischen vier Exportformate entscheiden: Microsoft Excel Datei, HTML Datei, Textdatei und XML.

Unterstützung der Risikomanagement-Methode

GSTOOL Die unterstützte Risikomanagement-Methode von GSTOOL erfolgt anhand der IT-Grundschutz-Kataloge und der BSI-Standards. Mit GSTOOL ist es möglich, den IT-Grundschutz von BSI konsequent umzusetzen. Weiters kann man die Wissensbasis nach eigenen Vorstellungen adaptieren

EBIOS Die EBIOS-Software verwendet die EBIOS-Methodik und setzt sie dabei sehr gut um. Die Elemente in der Wissensdatenbank kann man selbst editieren. Der Benutzer wird informiert, falls es nach einer Bearbeitung der Wissensdatenbank Inkohärenzen gibt.

Rimanis Die Rimanis-Software ist eine Eigenentwicklung von HULOCON GmbH und basiert nicht auf irgendwelche Standards oder Best Practices. Im Kapitel elf findet man eine ausführliche Beschreibung, wie das Programm die vier Phasen des Risikomanagement-Prozesses unterstützt.

RM-Berichtswesen

GSTOOL Im Programm ist bereits eine Vielzahl von Berichte vordefiniert und man kann diese Berichte mit einigen Mausklicks schnell generieren. Das Programm unterstützt bei der Berichtserstellung nur das HTML Format. Das Layout eines Berichts wie etwa das Logo kann über die Programmoptionen beeinflusst werden.

EBIOS Insgesamt sind neu vordefinierte Berichte in der EBIOS-Software enthalten. Es ist möglich, das Layout eines Berichts zu verändern, in dem man die Dokumentenvorlage editiert.

Rimanis In Rimanis ist es möglich, zehn Arten von RM-Berichte zu erstellen. Man kann

keinen eigenen Bericht definieren bzw. erstellen. Man muss also mit den zehn oben aufgelisteten Berichtsarten auskommen. Neben der Generierung von Berichte ist es auch möglich, Balkendiagramme für Risiko-Erwartungswerte und max. Vermögensminderung zu erstellen.

Usability und Layout

GSTOOL Die Benutzeroberfläche von GSTOOL ist sehr durchdacht und besteht aus fünf Komponenten: Menüleiste, Toolbar, Navigator, Bearbeitungsfläche und Statusleiste. Mit dem Navigator können alle Bereiche des Programmes schnell erreicht werden.

EBIOS Die EBIOS-Software wurde in Java entwickelt und verwendet folglich nicht die Windows Bibliotheken für die Benutzeroberfläche. Die EBIOS-Software schaut nicht wie eine für das Betriebssystem entwickelte Anwendung aus und dadurch finden sich einige Anwender sicher nicht so leicht zurecht.

Rimanis Die Benutzeroberfläche von Rimanis ist sehr gut aufgebaut und durchdacht. Sie ist als eine SDI Anwendung konzipiert. Das bedeutet, dass die Software nur ein Dokument anzeigen bzw. bearbeiten kann. Viele Bereiche des Programms können mittels eines Navigators schnell erreicht werden.

9. Details zur GSTOOL Evaluierung

Installation

Die Installationsdatei der Testversion kann man von der Homepage der BSI herunterladen. Die Größe der Datei beträgt ca. 130 Megabyte. Nach dem Download der Installationsdatei muss man sie selbst entpacken, die Verzeichnisstruktur anschauen und anschließend die Executable „setup.exe“ ausführen. Es ist nicht verständlich, warum man nicht gleich eine ausführbare Setupdatei erstellt und bei der Ausführung die Daten selbst entpackt. Der Aufwand für die Generierung solcher Dateien ist doch relativ gering, da man höchstens nur paar Zeilen im Setup-Skript hinzufügen muss.

Für die Evaluierung wird das GSTOOL in einer virtualisierten Umgebung mit 512 MB RAM, Microsoft Windows und AMD Athlon 64 3400+ Prozessor verwendet. Nach der Ausführung der Datei „Setup.exe“ fängt das Programm nun an, den Installer zu konfigurieren. Ein paar Sekunden später landet man dann bei einem Willkommensdialog, der von der folgenden Abbildung dargestellt wird.

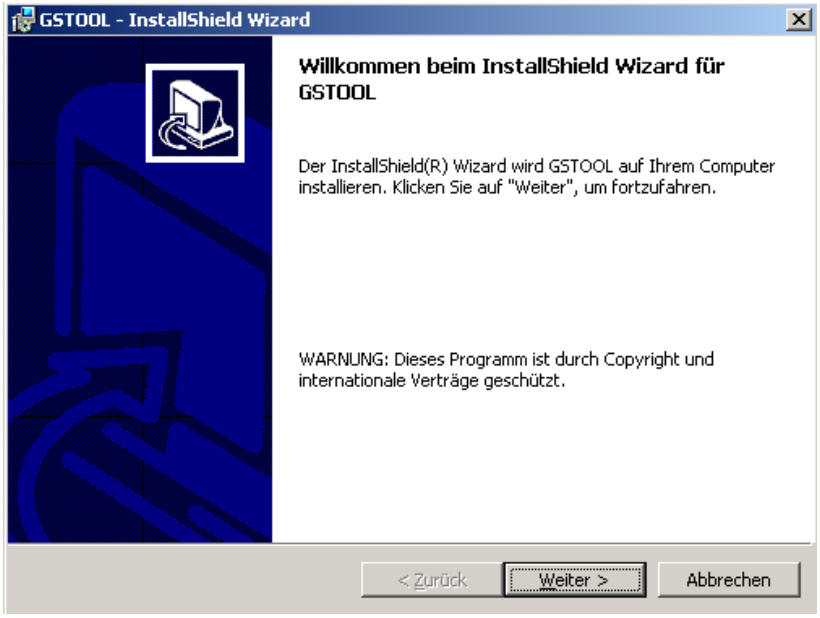


Abbildung 18: GSTOOL Installation - Willkommen

Es folgen danach die üblichen Schritte wie z.B. das Akzeptieren der Lizenzbedingungen. Anschließend kann man dann den Umfang der Installation auswählen. Dabei unterscheidet man zwischen einer vollständigen und einer benutzerdefinierten Installation. Die folgende Abbildung zeigt die Optionen der benutzerdefinierten Installation.

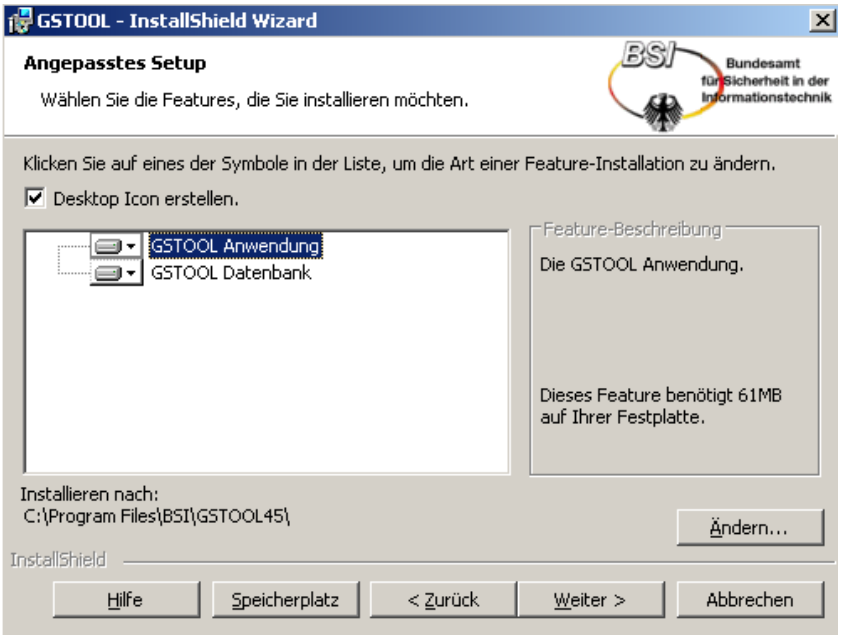


Abbildung 19: GSTOOL Installation – Benutzerdefinierter Auswahl

Bei der Evaluierung wird die vollständige Installation ausgewählt, da das GSTOOL als Einzelplatzanwendung getestet wird. Nach der Auswahl der Installationsart bekommt man dann folgende Meldung:

Abbildung 20: GSTOOL Installation - Datenbank

In der Abbildung wurde dem Anwender mitgeteilt, dass ein Datenbankserver (Microsoft Desktop Engine 2000) installiert wird. Im Anschluss muss das Datenbankpasswort bekannt gegeben werden. Die Installation des Datenbankservers ist Pflicht und man kann sie nicht

verhindern, auch wenn man eine eigene Datenbank betreiben möchte, da der Funktionsumfang von MDSE 2000 eingeschränkt ist. Die Datenbanken der MDSE 2000 können maximal nur 2 GB groß sein und sollen nicht von mehr als fünf Anwendern gleichzeitig bearbeitet werden.

Nach der Meldung über die Datenbankserver-Installation ist die Vorbereitung des Installationsvorgangs fertig und man kann mit dem Kopieren der Dateien beginnen. Das Kopieren dauert in der virtuellen Umgebung zirka drei Minuten. Danach ist das Programm einsatzbereit und kann verwendet werden.

Die Installation des GSTOOL benötigt zirka 180MB Speicherplatz. Ein Deinstallationsprogramm ist ebenfalls vorhanden und kann über die Systemsteuerung aktiviert werden. Die Deinstallation dauert ziemlich schnell. In der Testumgebung hat die Deinstallation weniger als eine Minute gedauert. Jedoch werden nicht alle Daten entfernt. Die bei der Installation erstellte Datenbank, die ca. 90 MB groß ist, wird nicht entfernt. Ein manuelles Löschen ist daher erforderlich.

Erste Eindrücke zur Benutzeroberfläche

Die Die Installation der Benutzeroberfläche von GSTOOL kann über ein Icon im Desktop gestartet werden. Folgende Abbildung zeigt die Benutzeroberfläche direkt nach der Installation.

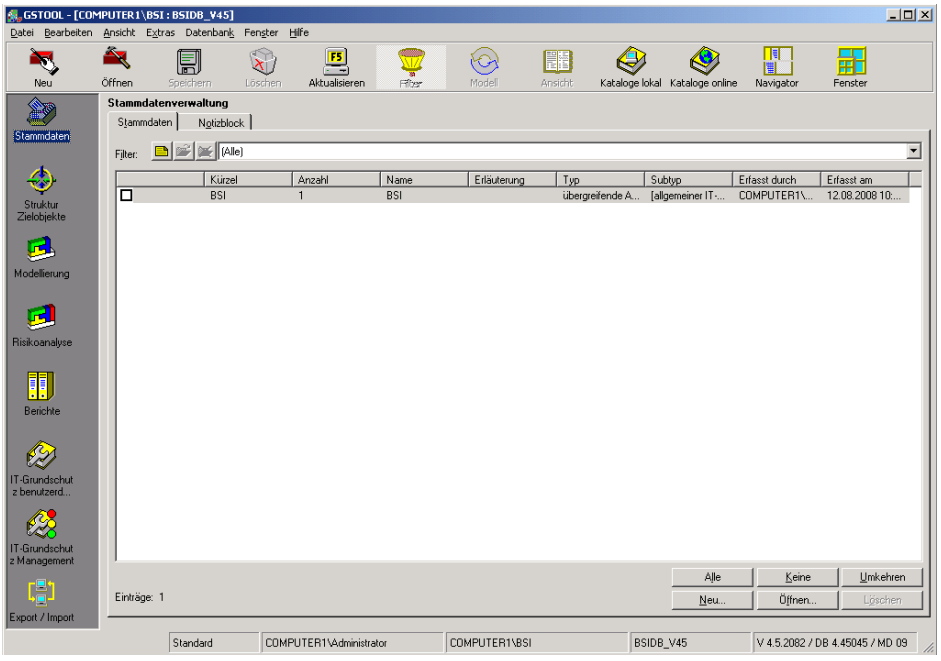


Abbildung 21: GSTOOL Oberfläche

Der erste Eindruck der Benutzeroberfläche ist durchaus positiv zu bewerten. Man kann die Oberfläche in insgesamt fünf Komponenten aufteilen: Menüleiste, Toolbar, Navigator, Bearbeitungsfläche und Statusleiste. Grundsätzlich gibt es bei den ersten Eindrücken der Benutzeroberfläche nichts zu bemängeln.

Administration

Das GSTOOL muss auf jeden Arbeitsrechner installiert werden, wenn man darauf arbeiten möchte. Ein Web-Zugriff oder ähnliches bietet das Programm nicht. Bei jeder Installation wird eine lokale Datenbank mit installiert. Es ist jedoch möglich, dass die Clients auf einer gemeinsamen Datenbank zugreifen und miteinander arbeiten. Die folgende Abbildung zeigt das Prinzip der Mehrbenutzerfähigkeit der Datenbank.

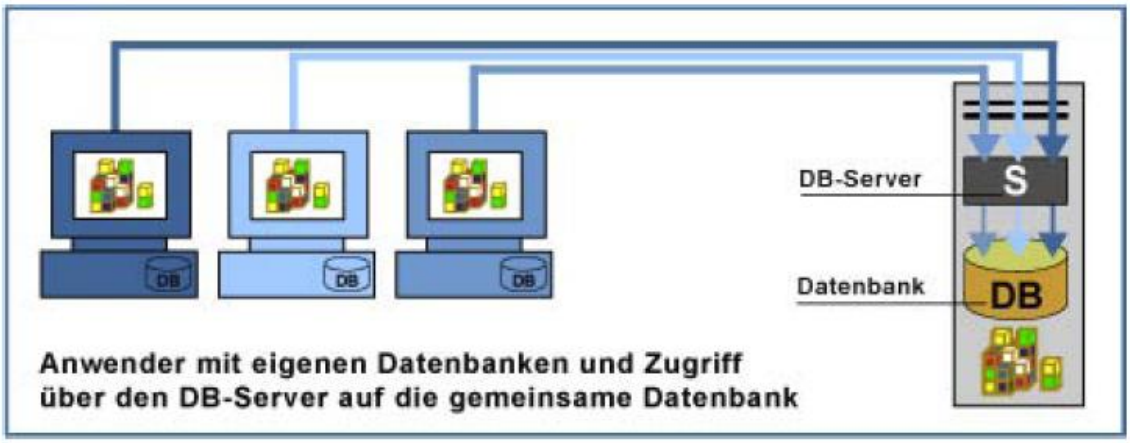


Abbildung 22: GSTOOL – Mehrbenutzerfähigkeit der Datenbank (BSI, 2008 S. 88)

Wenn man an einer gemeinsamen Datenbank arbeitet, ist die Verwaltung von Anwendern sowie deren Zugriffsrechte von Bedeutung. Um ein gemeinsames Mitarbeiten an einer Datenbank zu ermöglichen, verfolgt das GSTOOL das Konzept Anwender und Rollen. Um einen Anwender anzulegen, ruft man zunächst die Anwenderübersicht über die Option „Anwender“ im Menü „Extras“ auf.

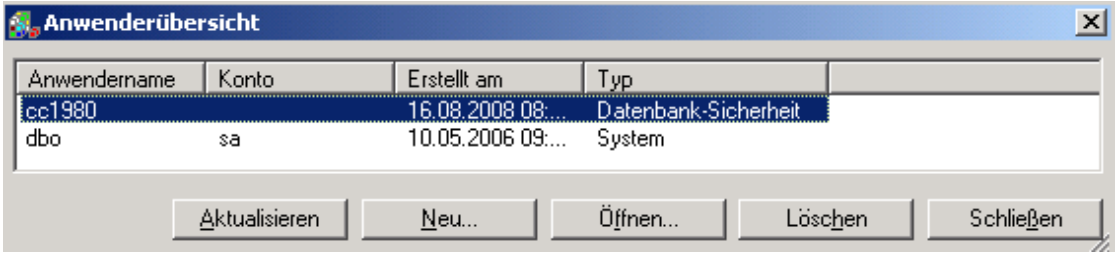


Abbildung 23: GSTOOL – Anwenderverwaltung

Für das Anlegen eines neuen Anwenders drückt man einfach den Button „Neu“ und die Maske für neuen Anwender wird aufgerufen.

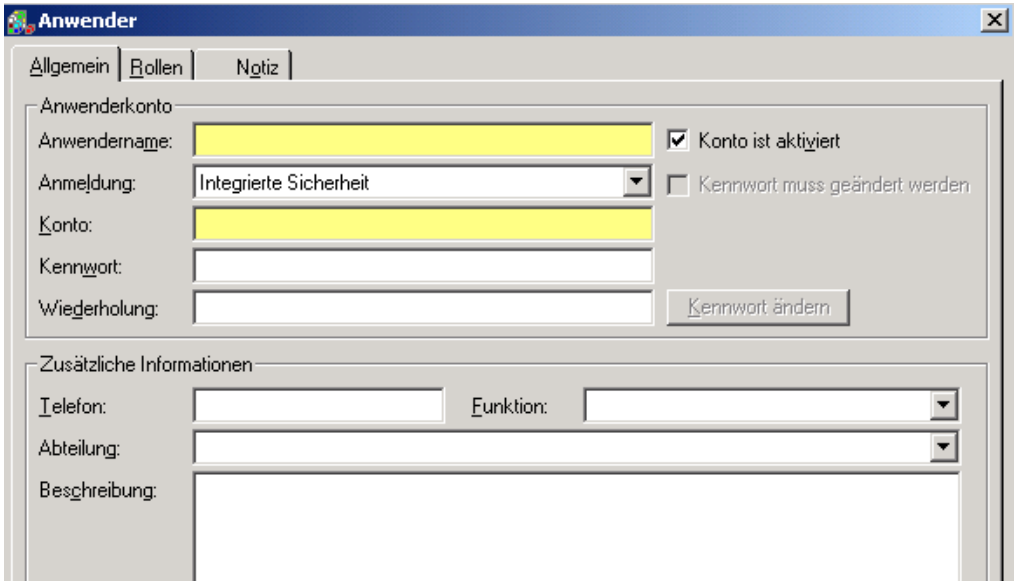


Abbildung 24: GSTOOL – Maske für neuen Anwender

Bei der Erstellung des Anwenders muss man einen Anwendername sowie Art der Anmeldung bekanntgeben. Man unterscheidet hier dabei eine Anmeldung mit integrierter oder mit Datenbank-Sicherheit. Wenn man zu einem Anwender eine Bemerkung anbringen möchte, kann man sie in Registerkarte „Notiz“ hinzufügen. Nachdem man alle erforderlichen Daten eingetragen hat, drückt man einfach den „OK“ Button und der Anwender wird angelegt.

Beim Anlegen eines neuen Anwenders werden einige Rollen vordefiniert und andere müssen im Nachhinein speziell zugewiesen werden. Rollen Das GSTOOL unterscheidet hierbei drei Arten von Rollen [vgl. (BSI, 2008 S. 77)]:

- System-Rollen: Diese Rollen sind vorgegeben und können nicht verändert werden. Es gibt insgesamt drei System-Rollen im GSTOOL Version 4.5: „Freigabe“, „System“ und „Import 4.1“.
- Rechte-Rollen: Mit Hilfe von Anwender Rollen kann man Rollen wie z.B. „Projektleiter“ oder „Anwendungsbetreuer“ definieren. Der Umfang der zugeordneten Berechtigungen kann frei gewählt werden. Alle Inhaber solcher Rolle haben immer dieselben Rechte.
- Anwender-Rollen: Diese Rolle wird automatisch erzeugt, wenn man einen neuen Anwender einträgt, der Zielobjekte anlegen darf. Diese Rolle kann man nicht manuell

bearbeiten. Diese Anwender haben Schreib- und Leserechte für alle von ihnen angelegten Objekte. Diese Rechte gelten exklusiv, es sei denn, dass anderen Anwendern explizit Rechte an den eigegebenen Objekten zugewiesen wurden.

Laut obige Auflistung wird ersichtlich, dass man eigentlich nur Rechte-Rollen selbst erstellen und definieren kann. Um die bereits angelegten Rollen im System anzusehen, braucht man nur die Rollenverwaltung über die Option „Rollen“ im Menu „Extras“ aufrufen.

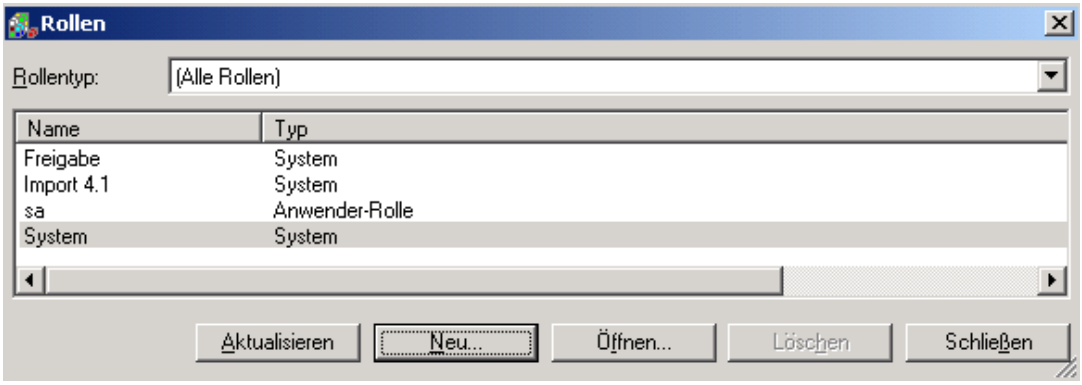


Abbildung 25: GSTOOL – Rollenverwaltung

Wenn man den Button „Neu“ drückt, wird die Maske für das Anlegen neuer Rechte-Rolle aufgerufen. Die folgende Abbildung zeigt die Maste für das Anlegen neuer Rollen-Rechte. Dieselbe Maske kann man ebenfalls unter der Registerkarte „Rollen“ in der Anwender-Maske aufrufen.

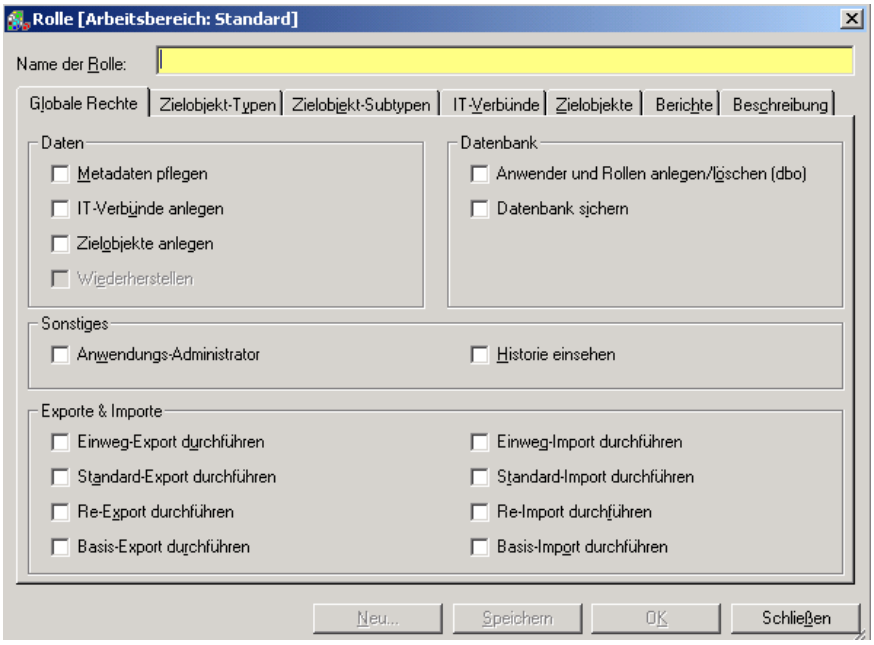


Abbildung 26: GSTOOL – Rollenverwaltung

Nachdem man der Rolle einen Namen zugewiesen hat, kann man dann die Rechte definieren. Es gibt sehr viele Arten von Rechten, die sehr übersichtlich mittels Registerkarten geordnet sind. Aufgrund der unzähligen Arten an Rechten wird hier nicht mehr auf die Details dieser Rechte eingegangen, da sonst der Umfang der Arbeit zu groß wird. Falls man am Ende noch eine Bemerkung hat, kann man sie in der letzten Registerkarte eintragen. Die Möglichkeit, eine eigene Beschreibung zu Rollen hinzufügen zu können, wird als positiv bewertet. Nachdem man die Rechte definiert hat, drückt man einfach den „OK“-Button, um die neue Rechte-Rolle in der Datenbank zu speichern.

Wie bereits erwähnt, kann man nur Rechte-Rollen selbst hinzufügen. Die übrigen Rollen können über die Rollenverwaltung eingesehen werden, jedoch ist eine Veränderung nicht möglich. Nachdem man eine Rolle erstellt hat, kann man sie einem Anwender zuweisen. Um den Anwender eine Rolle zuzuweisen, ruft man einfach die Anwender-Maske über die Anwenderverwaltung auf. Anschließend wählt man die Rollen, die man zuweisen möchte, in der Registerkarte „Rollen“ aus.

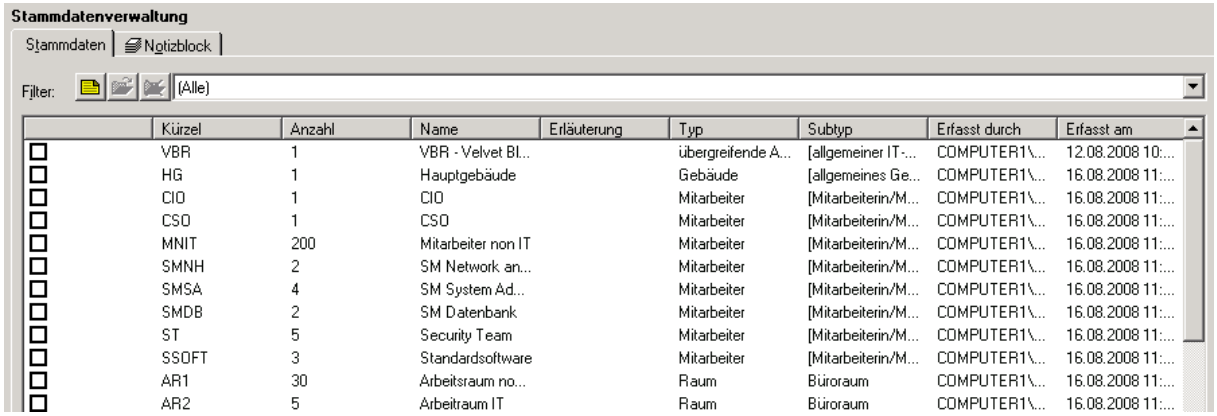
Die Anwender-Rollen Konzept des GSTOOL ist sehr gut durchgedacht. Dadurch sind eine saubere Rechteverteilung und ein problemloses gemeinsames Arbeiten an einer Datenbank möglich. Bei einer großen Arbeitsumgebung soll man vor Einsatz von GSTOOL das Rollenkonzept ausarbeiten. Für die Evaluierung von GSTOOL wird lediglich ein Anwender mit allen möglichen Rechten angelegt.

Modellierung

Im diesem Abschnitt werden die gewonnen Kenntnisse über das Programm beschrieben. Der IT-Grundschutz wurde bereits im Kapitel Standards und Best-Practices vorgestellt, daher wird hier nicht mehr auf die Vorgehensweise eingegangen. Für die Modellierung wird der Business Case als Ausgangspunkt hergenommen. Informationen, die zwar für die Modellierung erforderlich, jedoch nicht im Business Case, enthalten sind, werden durch geschätzte Werte ersetzt.

Der erste Schritt der Modellierung ist das Festlegen des IT-Verbunds sowie die IT-Strukturanalyse. Bei der Installation wurde bereits ein Verbund mit dem Namen „BSI“ angelegt. Man braucht sie nur umbenennen. Nach der Umbenennung des IT-Verbunds wechselt man über die Navigator in die Ansicht „Struktur Zielobjekt“, um den IT-Struktur zu modellieren sowie die erforderlichen Informationen einzutragen. Das Hinzufügen des Zielobjekts ist

relativ einfach und das Programm gibt einen Hinweis, falls nicht alle erforderlichen Felder eingetragen sind. Das Eintragen der Zielobjekte wird bei großen Unternehmen ziemlich mühsam sein. Da solche Daten meistens schon irgendwo existieren, ist eine Importfunktion mit eigenem Mapping empfehlenswert. Nach der Erfassung aller Zielobjekte kann man sie in der Stammdatenverwaltung ansehen.



Kürzel	Anzahl	Name	Erläuterung	Typ	Subtyp	Erfasst durch	Erfasst am
VBR	1	VBR - Velvet Bl...		übergreifende A...	[allgemeiner IT-...	COMPUTER1\...	12.08.2008 10:...
HG	1	Hauptgebäude		Gebäude	[allgemeines Ge...	COMPUTER1\...	16.08.2008 11:...
CIO	1	CIO		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
CSO	1	CSO		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
MNIT	200	Mitarbeiter non IT		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
SMNH	2	SM Network an...		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
SMSA	4	SM System Ad...		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
SMDB	2	SM Datenbank		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
ST	5	Security Team		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
SSOFT	3	Standardsoftware		Mitarbeiter	[Mitarbeiterin/M...	COMPUTER1\...	16.08.2008 11:...
AR1	30	Arbeitsraum no...		Raum	Büroraum	COMPUTER1\...	16.08.2008 11:...
AR2	5	Arbeitraum IT		Raum	Büroraum	COMPUTER1\...	16.08.2008 11:...

Abbildung 27: GSTOOL – Erfasste Objekte in der Stammdatenverwaltung

Falls man zu viele Zielobjekte erfasst hat und löschen will, kann man das in der Stammdatenverwaltung ganz leicht erledigen. Man wählt zu löschende Objekte aus und drückt danach einfach den Button „Löschen“.

Nach der Erfassung der Zielobjekte folgt nun deren Strukturierung. Man verknüpft dabei das Zielobjekt und bildet dadurch eine hierarchische Struktur. Im GSTOOL unterscheidet man zwei Arten von Verknüpfungen: direkte und indirekte.

Ein Objekt ist direkt mit einem IT-Verbund verknüpft, wenn es in der Liste der Zielobjekt-Typen direkt unterhalb des IT-Verbunds enthalten ist. Nur dann wird das betreffende Zielobjekt bei der Modellierung berücksichtigt. (BSI, 2008 S. 21)

Ein Objekt ist lediglich indirekt mit einem IT-Verbund verknüpft, wenn es im Baum unterhalb der direkt verknüpften Zielobjekte eingeordnet ist. Diese Verknüpfungen helfen bei der späteren Schutzbedarfsfeststellung, den Schutzbedarf voneinander abhängiger Zielobjekte angemessen einzuschätzen. (BSI, 2008 S. 22)

Die folgende Abbildung vom Webkurs GSTOOL stellt das Prinzip der direkten und indirekten Verknüpfungen noch einmal graphisch dar.

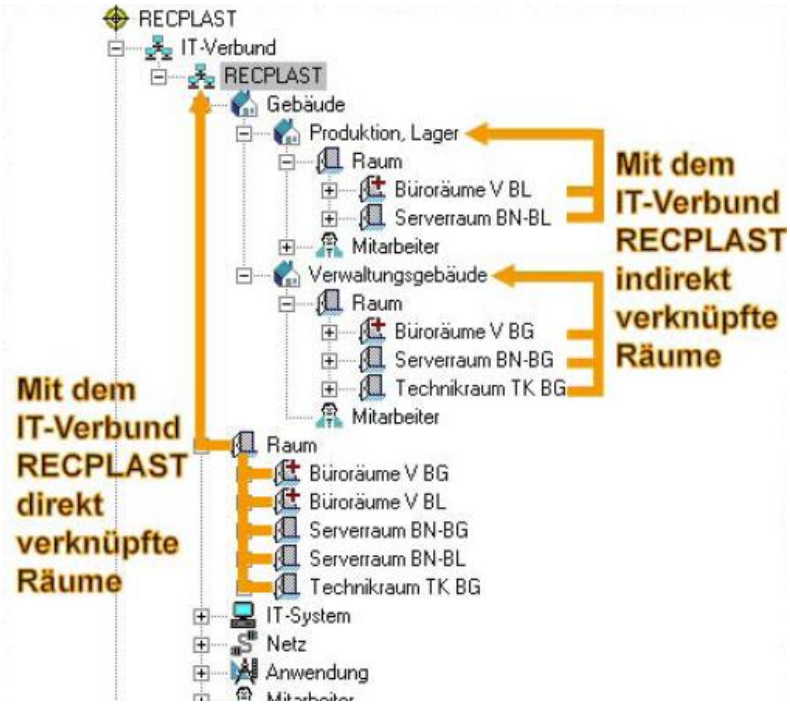


Abbildung 28: GSTOOL – Direkte und indirekte Verknüpfung (BSI, 2008 S. 22)

Es gibt insgesamt zwei Möglichkeiten, Verknüpfungen zu erstellen. Die einfachste Möglichkeit ist über Drag & Drop. Zuerst wählt man das Objekt, das man verknüpfen möchte, aus. Anschließend zieht man das Objekt zum Zielobjekt und wählt die Option „Verknüpfung anlegen“. Die ganze Operation dauert lediglich nur ein paar Sekunden.

Der nächste Schritt ist die Feststellung des Schutzbedarfs. Dabei wird bei den Zielobjekten der Schutzbedarf in Bezug auf die Grundwerte „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ ermittelt und eingetragen. Voreingestellt sind drei Schutzbedarfdefinitionen: „niedrig bis mittel“, „hoch“ und „sehr hoch“. Diese Einstellung kann man in der Ansicht „Grundschutzhandbuch benutzerdefiniert“ verändern. Die Feststellung des Schutzbedarfs soll immer nach der Strukturierung der Zielobjekte erfolgen, da der Schutzbedarf vererbt wird.

Nachdem man den Schutzbedarf eingetragen hat, kann man dann zur Ansicht Modellierung wechseln. Dieser Arbeitsbereich ist für die Schritte Modellierung, Basis-Sicherheitscheck und Realisierungsplanung zuständig. In diesem Bereich kann man Bausteine der IT-Grundschutz-Kataloge entfernen und verknüpfen sowie Bausteine wie etwa den. Umsetzungsgrad oder die Kosten der Maßnahmen bearbeiten.

Seit Version 4.5 gibt es die Ansicht Risikoanalyse. Dieser Arbeitsbereich ist am BSI Standard 100-3 orientiert und wurde bereits kurz im Kapitel Standards und Best Practices besprochen. In dieser Ansicht werden nur Zielobjekte angezeigt, bei denen eine ergänzende Sicherheitsanalyse erforderlich ist. In der Evaluierung sind keine Schwierigkeiten in dieser Phase aufgetreten.

Reports

Über den Navigator kann man zur Ansicht „Berichte“ wechseln, wo die Berichte generiert werden. Folgende Abbildung zeigt den Arbeitsbereich Berichte dar.

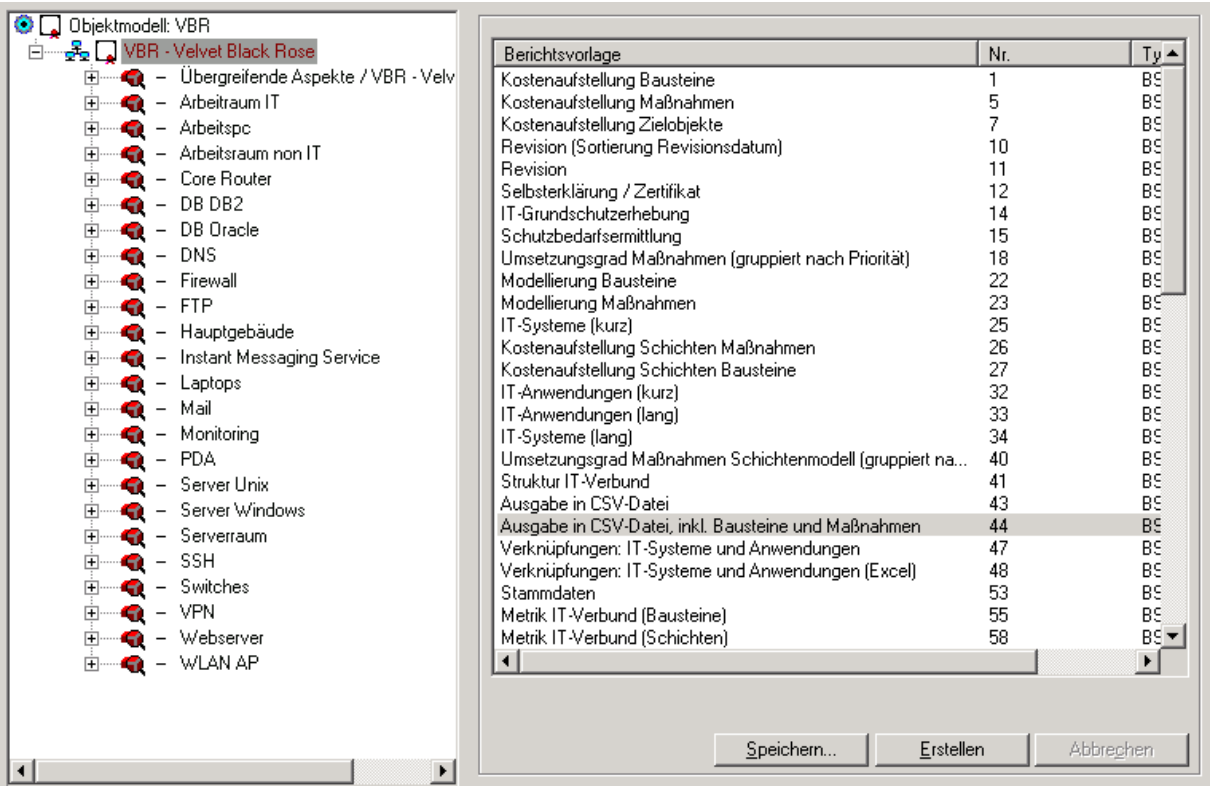
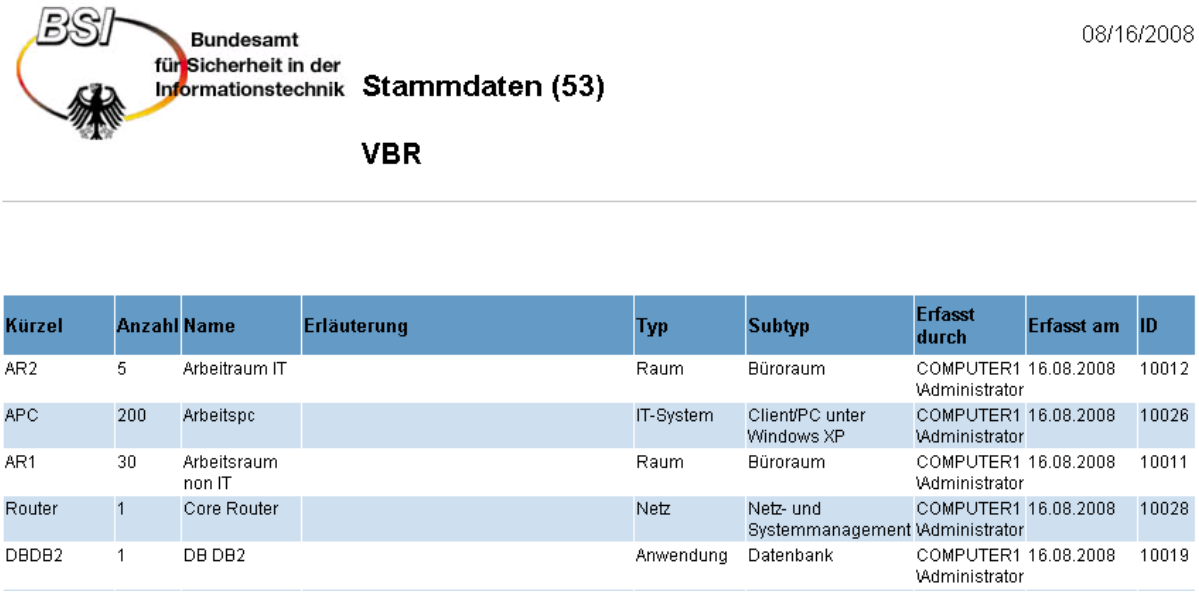


Abbildung 29: GSTOOL – Arbeitsbereich Berichte

Viele Arten von Berichte kann man im GSTOOL erstellen. Das Erstellen eines Berichts ist auch ziemlich einfach. Man wählt einfach Art und Umfang des Berichts aus und drückt den Button „Erstellen“.

Je nach der Art des Berichts braucht GSTOOL nur wenige Sekunden für die Generierung des Berichts. Dabei generiert das GSTOOL ein HTML Dokument und stellt es anschließend mit dem Standardbrowser des Betriebssystems dar. Laut GSTOOL Beschreibung werden

alle Arten von gängigen Browsern unterstützt, jedoch ist es optimiert für Internet Explorer. Folgende Abbildung zeigt einen von GSTOOL generierten Bericht.



Bundesamt für Sicherheit in der Informationstechnik

08/16/2008

Stammdaten (53)

VBR

Kürzel	Anzahl	Name	Erläuterung	Typ	Subtyp	Erfasst durch	Erfasst am	ID
AR2	5	Arbeitraum IT		Raum	Büroraum	COMPUTER1 \Administrator	16.08.2008	10012
APC	200	Arbeitspc		IT-System	Client/PC unter Windows XP	COMPUTER1 \Administrator	16.08.2008	10026
AR1	30	Arbeitsraum non IT		Raum	Büroraum	COMPUTER1 \Administrator	16.08.2008	10011
Router	1	Core Router		Netz	Netz- und Systemmanagement	COMPUTER1 \Administrator	16.08.2008	10028
DBDB2	1	DB DB2		Anwendung	Datenbank	COMPUTER1 \Administrator	16.08.2008	10019

Abbildung 30: GSTOOL – Ein Bericht

Die Generierung in HTML ist zwar schon in Ordnung, aber die Generierung des Berichts im PDF Format ist nach persönlicher Meinung sehr wünschenswert und die Integration solcher Funktionen sollte auch nicht schwierig sein. Das Layout des Berichts kann man ebenfalls beeinflussen. Die nötige Einstellungen findet man in der Option „Optionen“ im Menü „Extras“.

Import/Export und Datenaustausch

Das GSTOOL bietet Funktionen für den Import bzw. Export von Daten. Ziel dieser Funktion ist die Übertragung der Daten vom einen Client auf den anderen zu ermöglichen. Zwar ist GSTOOL netzwerkfähig und ermöglicht eine gemeine Nutzung der Datenbank, dennoch ist es in manchen Situationen notwendig, die Daten manuell zu übertragen. Außerdem kann man auch diese Funktionen für eine manuelle Backup/Wiederherstellung „missbrauchen“.

Es gibt insgesamt fünf Arten von Import/Export-Funktionen (BSI, 2008 S. 95):

- *Zielobjekt-Export und Zielobjekt-Import*, mit denen Zielobjekte in Tabellenform exportiert und in eine andere Datenbank eingelesen werden können,
- *Standard-Export und Standard-Import*, mit denen nicht nur Zielobjekte, sondern auch Informationen zu Bausteinen und Maßnahmen zur Bearbeitung in einer anderen Datenbank ex- bzw. importiert werden können,

- *Re-Export und Re-Import*, mit denen die zuvor mit Standard-Ex- und -Import übertragenen und evtl. weiterbearbeiteten Daten in die Quelldatenbank zurück übertragen werden können,
- *Einweg-Export und Einweg-Import*, mit denen eine Datenbank vollständig oder teilweise in eine andere übertragen werden kann,
- *Basis-Export und Basis-Import*, mit denen Bausteine, Gefährdungen und Maßnahmen in eine andere Datenbank übernommen werden können.

Neben der Import/Export Funktionalität bietet das GSTOOL auch das Verschlüsseln der Daten an. Das Verschlüsselungsfenster kann unter der Option „Verschlüsselung“ im Menü „Extras“ aufgerufen werden.

Abbildung 31: GSTOOL – Verschlüsselung

Die Verschlüsselung basiert auf den Algorithmus der Chiasmus Software. Chiasmus ist eine Verschlüsselungssoftware für Windows und wurde ebenfalls von BSI entwickelt. Durch eine Verschlüsselung der Daten kann man ein ungewünschtes Mitlesen der Daten effektiv bekämpfen.

Stärke und Schwäche

Eine Stärke von GSTOOL ist der Preis der Lizenzen. Eine Einzelplatzlizenz kostet lediglich € 895,52 (Stand August 2008) und kann als recht günstig angesehen werden. Falls man bereits eine Lizenz hat, sind die Kosten für ein Upgrade ebenfalls sehr günstig. Die Höhe der Preise für das Upgrade hängt davon ab, wie alt die eingesetzte Version ist. Ein Upgrade von Version 4.0/4.1 auf Version 4.5 kostet lediglich € 35.25 (Stand August 2008).

Man kann das Tool kostenlos herunterladen und 30 Tage lang testen, ohne Lizenz einzugeben. Nach der 30-tägigen Testlaufzeit muss man ein gültiger Lizenzschlüssel angegeben werden, sonst ist eine Speicherung der neuen Daten nicht mehr möglich und man kann

nur die vorhandenen Daten betrachten. Jedoch kann man diese Einschränkungen sehr leicht umgehen. Man dreht einfach das Datum zurück und schon ist eine Speicherung wieder möglich. Theoretisch kann man GSTOOL auf einer virtuellen Umgebung installieren und das Datum immer wieder zurückdrehen. Dann kann man GSTOOL theoretisch unendlich lange benutzen. Der mangelnde Schutz der Software stellt eigentlich eine Schwäche dar, nicht jedoch unbedingt für den Anwender der Software.

Mittels GSTOOL ist es möglich, den IT-Grundschutz vom BSI konsequent umzusetzen. Sehr lobenswert ist auch die Benutzeroberfläche von GSTOOL. Man findet sich im Programm schnell zurecht. Mit Hilfe vom Navigator und der Symbolleiste kann man alle Funktionen des Programms schnell und recht problemlos ausführen.

Ebenfalls lobenswert ist der Webkurs zum GSTOOL. Den Webkurs kann man entweder online lesen oder als PDF herunterladen. Das PDF Dokument hat 108 Seiten und ist in zwei Teilen gegliedert: Anwendung und Administration. Der Anwendungsteil beschreibt die Verwendung des GSTOOLs sehr gründlich und enthält auch Übungsfragen sowie deren Lösungen. Im Administrationsteil werden die Aufgaben zum Verwalten des Programmes ebenfalls sehr gut beschrieben. Der Webkurs bleibt jedoch von der Kritik nicht verschont. Der Webkurs ist zum Zeitpunkt der Evaluierung noch nicht auf die neuste Version angepasst worden. Im Webkurs steht z.B. keine Beschreibung oder Einführung über die Risikoanalyse Funktionalität.

Neben den oben angeführten Stärken hat GSTOOL nach persönlicher Ansicht auch einige Schwächen. Der erste Nachteil, der bei der Evaluierung auffallend war, ist die absolute Unverständlichkeit mancher Fehlermeldungen. Die folgende Abbildung zeigt eine Fehlermeldung beim Testen von GSTOOL:

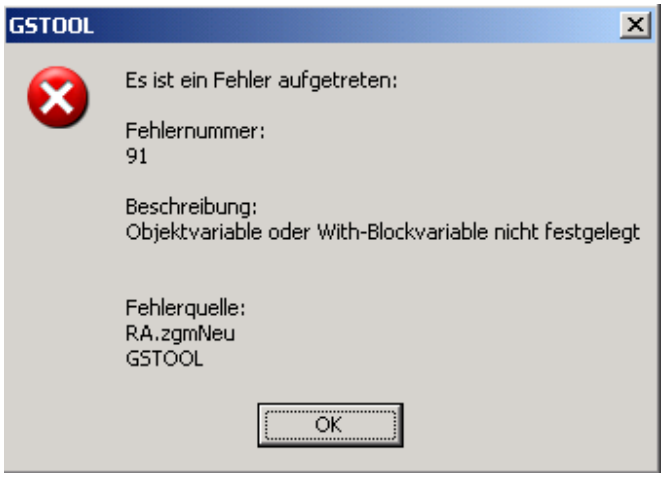


Abbildung 32: GSTOOL – Eine unverständliche Fehlermeldung

Es ist natürlich gut, dass man versucht, alle Fehler abzufangen. Aber als Anwender hat man leider keine Ahnung, was die obige Meldung zu bedeuten hat. Außerdem muss erwähnt werden, dass diese Fehlermeldung nach dem Drücken vom „OK“ Button sofort wieder auftaucht und das Programm nur mehr über den Windows Task-Manager beendet werden kann.

Ein weiterer Kritikpunkt ist die eigenartige Installation von GSTOOL. Wie bereits oben erwähnt, muss man bei jeder Installation einen Datenbankserver installieren, auch wenn man einen zentralen Datenbankserver verwenden möchte. Außerdem wird bei der Installation nicht alles mit installiert. Die lokale Version der IT-Grundschutz-Kataloge ist nicht installiert worden. Die folgende Abbildung zeigt den Beweis der Behauptung. Ein Video kann man nicht leider in einer Masterarbeit einbinden.

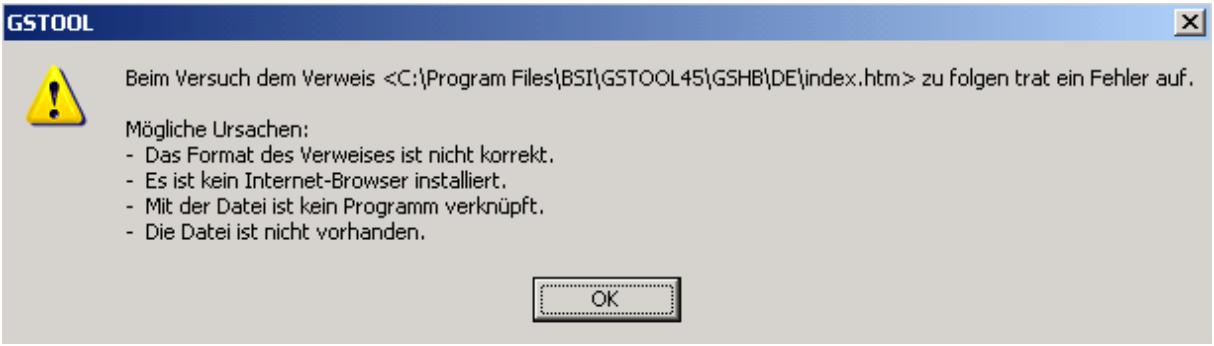


Abbildung 33: GSTOOL – eine Fehlermeldung

Um diesen Fehler zu beheben, braucht man nur die HTML Version der IT-Grundschutz-Kataloge herunterladen und im entsprechenden Verzeichnis entzippen oder die Datei „gstool-html.exe“ im GSTOOL-Installationsverzeichnis ausführen. Beim Installationsvorgang wurde nirgendwo ein Hinweis über die fehlende Mit-Installation der lokalen Version der IT-Grundschutz-Kataloge angeführt. Da man das Problem schnell beheben kann, ist die Bedeutung des Problems eher als gering einzustufen.

Eine weitere Kritik ist die mangelnde Unterstützung verschiedener Datenbankprodukte. Standardmäßig wird die Microsoft Desktop Engine (MSDE 2000) installiert. Diese Version hat jedoch Einschränkungen. Wenn man höhere Anforderungen an die Datenbank benötigt, muss man selbst einen MS SQL Server kaufen. Laut Webkurs Seite 87 bietet GSTOOL nur eine Schnittstelle zum Microsoft SQL Server 2000. Kostenlose Datenbaken wie z.B. Oracle 10g Express Edition oder PostgreSQL werden nicht unterstützt. Die Erweiterung der DB-Schnittstellen ist daher empfehlenswert.

Die letzte Kritik, die noch angeführt wird, ist die aufwändige Erfassung von Daten. Es dauert sehr lang, einen sehr großen IT-Verbund zu erfassen. Bei großen Unternehmen existieren die meisten Daten bereits in irgendeiner Form. Eine Import- Funktion der Daten mit der Möglichkeit, ein eigenes Mapping zu erstellen, ist in diesem Fall sehr begrüßenswert.

Zusammenfassung

Mit der Hilfe vom GSTOOL kann der IT-Grundschutz konsequent umgesetzt werden. Der Aufbau der Benutzeroberfläche und die Bedienung sind sehr gelungen. Viele kleine Features unterstützen den Anwender bei der Modellierung und man findet sich sehr leicht im Programm zurecht.

Zu bemängeln gibt es eigentlich nicht viel. Die Installation ist ein wenig eigenartig und manche Teile des Programmes scheinen noch unausgereift zu sein. Man erhält Fehlermeldungen, die man als Anwender nicht versteht und gerät in eine Situation, in der man das Programm nur durch den Windows Task-Manager beenden kann. Eine Importfunktion mit Möglichkeit, ein eigenes Mapping zu erstellen, ist begrüßenswert, auch wenn solche Importfunktionen nicht üblich sind.

Zum Schluss soll erwähnt werden, dass GSTOOL ausschließlich IT-Grundschutz unterstützt, was auch verständlich ist, da das Tool von BSI entwickelt wurde. Wer eine andere IT-Risikomanagement-Methode bevorzugt bzw. verwenden will, soll lieber ein anderes Tool aussuchen.

10. Details zur EBIOS-Software Evaluierung

Die EBIOS-Software ist ein Werkzeug für die Realisierung der EBIOS Methode, ähnlich wie das GSTOOL. Der wichtigste Grund für die Evaluierung der EBIOS-Software ist die freie Verfügbarkeit. Sie wird direkt von DCSSI vertrieben und ist kostenlos erhältlich. Es ist sicher interessant, kostenlose Software mit anderen teuren Risikomanagement Tools zu vergleichen, auch wenn die verwendete Risikomanagement-Methode nicht gleich sind.

Installation

Die Installationsdatei der EBIOS-Software ist über die Webseite der französischen Regierung für die Sicherheit von Informationssystemen beziehbar. Neben der Installationsdatei ist auch der Quellcode dort erhältlich, da die EBIOS Software Open-Source ist. Um die Software Laufen zu bringen, muss man lediglich die Installationsdatei im den gewünschten Verzeichnis entpacken und anschließend die Datei „ebios.exe“ ausführen.

Die Installation der EBIOS-Software ist relativ einfach, obwohl es nur eine Anleitung in französischer Sprache gibt. Notfalls kann man die Anleitung mit einem Online-Übersetzer wie z.B. Google Translation übersetzen.

Erste Eindrücke

Bevor man die Software zum ersten Mal startet wird die Verzeichnisstruktur der EBIOS Software untersucht. Dabei wurde herausgefunden, dass die EBIOS Software auf Basis von Java entwickelt wurde. Mit der Installation wird eine Java Laufzeitumgebung mit Version 1.3.1_02 mitgeliefert und befindet sich im Verzeichnis `/arch/bin`.

Neben dem `arch` Verzeichnis sind noch folgende Verzeichnisse vorhanden: `data`, `images` und `lib`. Im `data` Verzeichnis werden die Konfiguration, Logs und EBIOS Knowledge Base gespeichert. Im Verzeichnis `lib` befinden sich die Java Klassen, die in JAR Dateien verpackt sind. Im `images` Verzeichnis sind Bilder enthalten, die die EBIOS-Software verwendet.

Wenn man die Software zum ersten Mal startet, verwendet das Programm die französische Sprachdatei. Folgende Abbildung zeigt das Hauptfenster der EBIOS Software in deutscher Sprache.

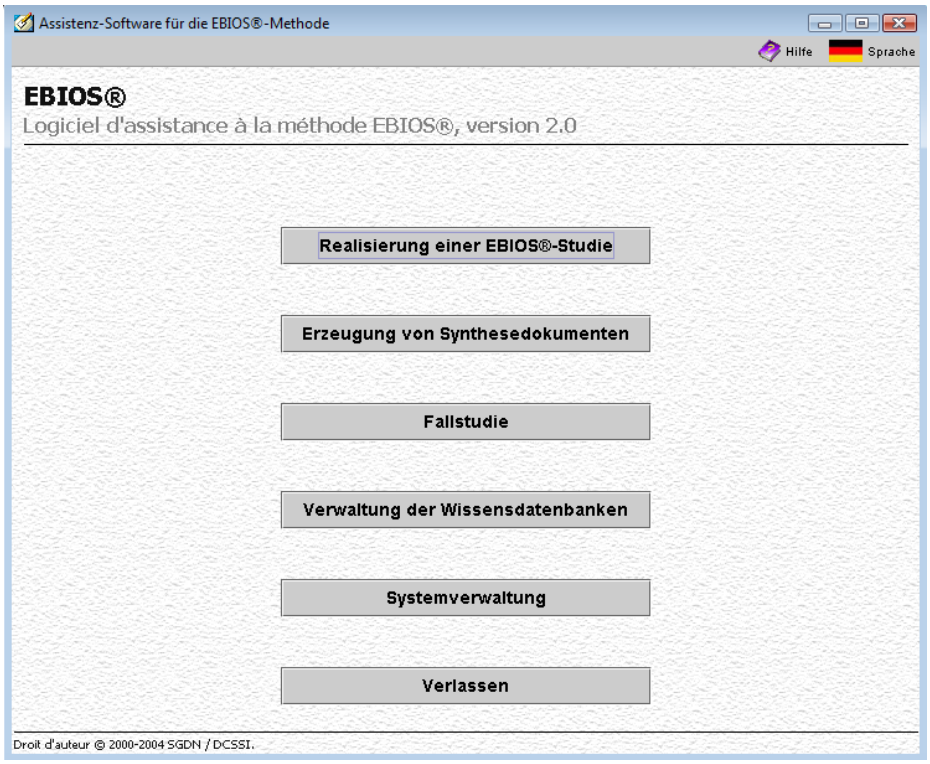


Abbildung 34: EBIOS Software - Hauptmenü

Die Sprache kann man ganz leicht ändern. Wenn man auf die Flagge Symbol rechts oben klickt, zeigt das Programm die verfügbare Sprachen.

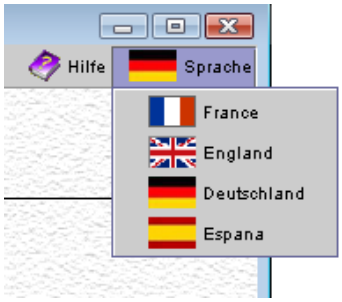


Abbildung 35: EBIOS Software – Verfügbare Sprachen

Da die EBIOS-Software in Java entwickelt wurde, wird ohne Codeanalyse angenommen, dass die Swing Library verwendet wurde. Das bedeutet, dass man die Nachteile von Java Swing ohne Diskussion auch an die EBIOS-Software übertragen kann. Die EBIOS-Software schaut nicht wie eine für das Betriebssystem entwickelte Anwendung aus und dadurch finden sich einige Anwender sicher nicht so leicht zurecht. Man kann dieses Problem. durch eine Auswahl von Pluggable Look-and-Feels teilweise oder zur Gänze lösen.

Da die aktuellste Version von EBIOS Software bereits über drei Jahre alt ist, soll man sich die Frage stellen, ob das Programm überhaupt unter dem neusten Betriebssystem von

Microsoft, Windows Vista, läuft. Testhalber wurde das Programm unter Windows Vista ausgeführt. Die EBIOS-Software läuft prinzipiell unter Windows Vista, jedoch verträgt sich das Programm nicht mit bestimmten visuellen Elementen von Windows Vista. Bei der Ausführung der Software wird das Farbschema automatisch auf Windows Vista Basis umgestellt und Aero wird deaktiviert. Man muss mit dieser Einschränkung leben, wenn man EBIOS-Software unter Windows Vista verwenden will.

Administration

Man kann unter EBIOS-Software folgende Bereiche administrieren:

- Benutzer,
- Dokumente und
- EBIOS Wissensdatenbank

Falls noch kein Benutzer angelegt wurde, kann man alle Bereiche der EBIOS-Software ohne Einschränkung verwenden. In der EBIOS-Software unterscheidet man zwei Arten von Benutzer: Administrator und Auditor. Der Administrator hat vollen Zugriff auf das Programm und der Auditor hat lediglich Zugriff auf den Audit-Teil sowie die Erstellung der Dokumente. Bevor man ein Auditor-Benutzer anlegen kann, muss mindestens ein Administrator-Benutzer existieren, sonst kann man keinen Auditor-Benutzer anlegen. Folgende Abbildung zeigt das Fenster zum Anlegen eines Benutzers:

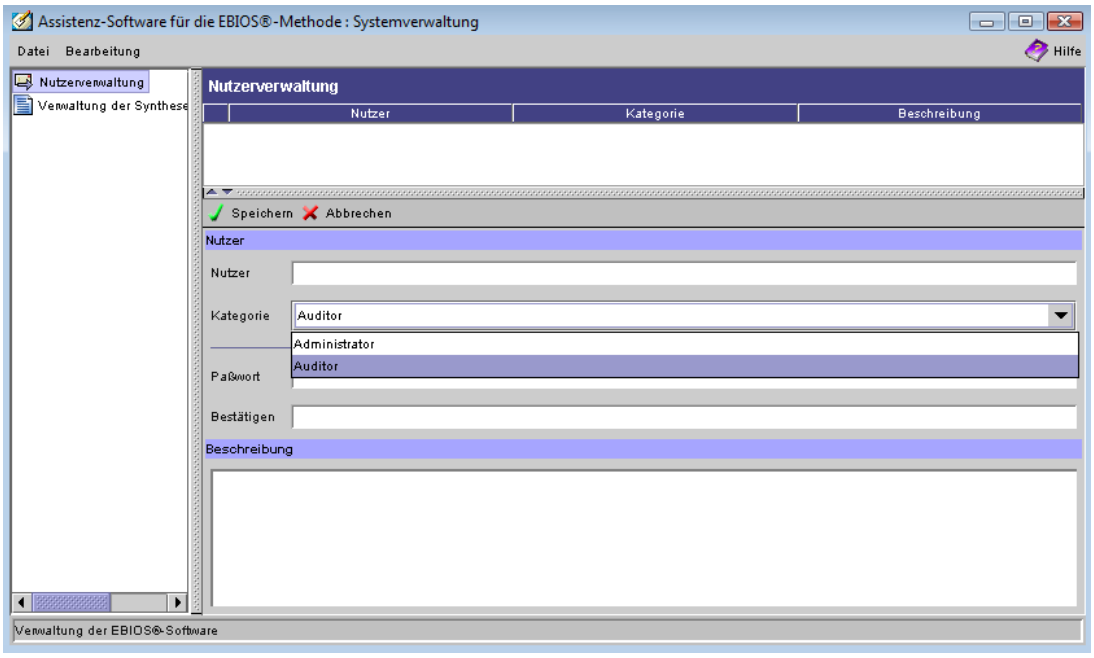


Abbildung 36: EBIOS-Software – Benutzerverwaltung

Neben der Benutzerverwaltung kann man auch im Bereich „Systemverwaltung“ der EBIOS-Software die Synthesedokumente verwalten. Man kann dort neue Synthesedokumente hinzufügen bzw. löschen. Näheres zum Thema Synthesedokumente wird im Abschnitt Reporting genauer beschrieben.

Die letzte Administrationsmöglichkeit ist die Verwaltung der Wissensdatenbanken. Standardmäßig liefert die Software die Wissensdatenbank in vier Sprachen mit. Um die Wissensdatenbank zu bearbeiten, geht man in den Bereich „Verwaltung der Wissensdatenbank“ und öffnet anschließend die Wissensdatenbank-Datei in der gewünschte Sprachen. Nachdem man die Datenbank geöffnet hat, kann man dann beliebige Elemente wie z.B. Glossar, Fragebogen oder Abkürzungen hinzufügen/ändern/löschen. Die mit der Software gelieferter Wissensdatenbank stammt vom Jahr 2004. Eine neure Version der Datenbank gibt es anscheinend nicht. Es gibt jedoch die Möglichkeit in der Software, eine eigene Wissensdatenbank aufzubauen. Falls beim Aufbau oder bei der Bearbeitung der Datenbank Inkohärenzen gibt, wird dies ebenfalls von der Software angezeigt.

Modellierung

Vor Beginn der Modellierung soll folgendes noch einmal klargestellt werden, dass Der Schwerpunkt der Evaluierung die Software und nicht die EBIOS-Methode ist. Das bedeutet, dass die Schwächen der Software aufgrund der Methode hier nicht berücksichtigt werden. Es werden lediglich die Eindrücke des funktionalen Umfangs festgehalten.

Im Kapitel „Standards und Best Practices“ wurde die EBIOS-Methode vorgestellt. Die Vorgehensweise der EBIOS-Methode wird daher nicht nochmal beschrieben. Generell kann man die Vorgehensweise bei der Erstellung einer EBIOS-Studie mit der EBIOS-Software wie folgt beschreiben:

1. Man fängt mit dem ersten Schritt der EBIOS Methodik an.
2. Man beginnt mit der ersten Aktivität des EBIOS Schrittes.
3. Man arbeitet die Aktivität ab und beendet sie mit dem „Akzeptieren“ Button.
4. Falls noch weitere Aktivitäten im EBIOS Schritt gibt, wird Schritt 2 wiederholt.
5. Falls es keine Aktivitäten mehr gibt, validiere den Schritt.
6. Man arbeite am nächsten Schritt der EBIOS Methodik weiter und wiederhole dabei den Schritten zwei bis fünf.

7. Die EBIOS-Studie ist beendet, wenn der letzte Schritt der EBIOS Methodik abgearbeitet wurde.

Folgende Abbildung zeigt den Arbeitsbereich der Software.

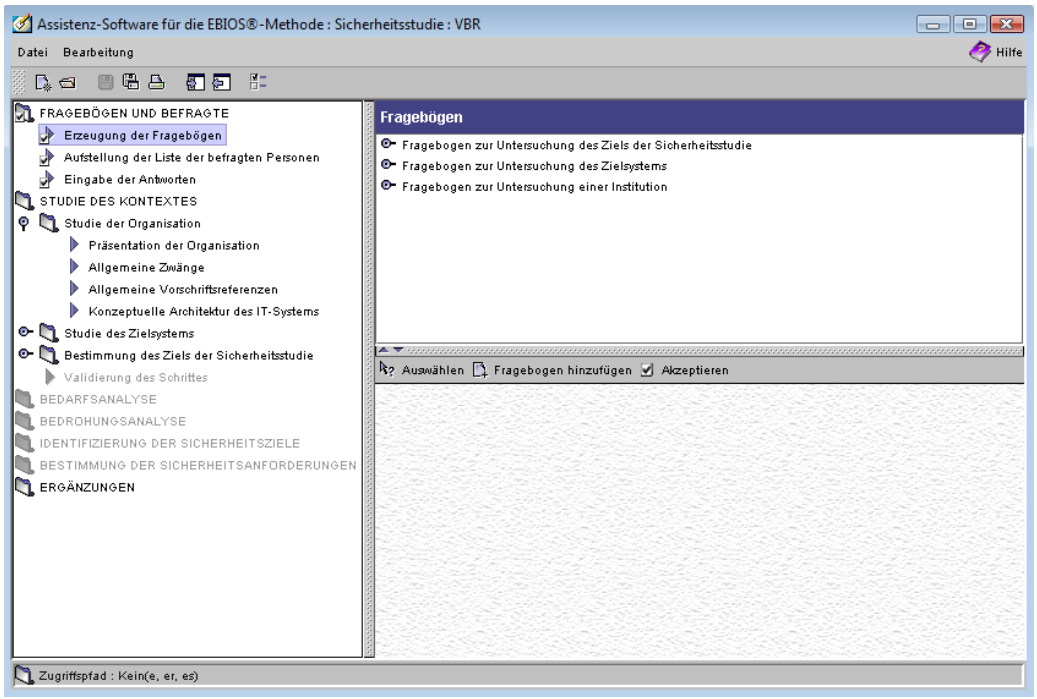


Abbildung 37: EBIOS-Software – Arbeitsbereich

Da die Benutzeroberfläche der Software auf Java basiert ist, empfindet man bei der Anwendung ein ungutes Gefühl. Am meisten stört es, dass die Software nicht auf die Eingabe des Maus Scroll-Rads reagiert. Man muss immer die Scroll-Leiste der Software verwenden und es ist einfach zu unbequem.

Schon bei der Erstellung bzw. Beantwortung der Fragebögen ist man mit der Einschränkung der Software konfrontiert. Die EBIOS-Software ist als eine Einzelplatzanwendung einzustufen. Es gibt daher keine vernünftige Möglichkeit, gemeinsam an einer Datenbasis zu arbeiten. Glücklicherweise ist der Business Case bereits in der elektronischen Form vorhanden und man muss dabei nur Copy & Paste anwenden. Bei einer großen Befragung auf Papierbasis ist die Eingabe der Antworten wohl eine echte Zumutung.

Auf die restlichen Schritte bei der Modellierung anhand des Business Cases wird nicht näher eingegangen, um eine Kritik an der Methodik zu verhindern. Nicht jede RM-Methode ist perfekt und sie hat ihre Vor- und Nachteile. Generell läuft die Modellierung in wie bereits oben erwähnte Schritte ab und es treten keine Schwierigkeiten auf. Viele Elemente kann man bei

der Modellierung der Studie direkt von der Wissensbasis übernehmen und dadurch verringert sich der Aufwand bei der Modellierung.

Wie bei der Evaluierung soll natürlich noch einmal erwähnt werden, dass der Business Case keine vollständigen Informationen über das Unternehmen gibt. Die fehlenden Daten wie z.B. die Bedürfnisblätter werden von der Wissensdatenbank übernommen. Einige Werte werden nach persönlicher Einschätzung erstellt, dies beeinflusst natürlich den Ausgang der Modellierung. Am Ende der Modellierung kann man grundsätzlich sagen, dass es keine großen Probleme aufgetreten ist. Die größte Arbeit bei der Erstellung der EBIOS Studie ist die Einarbeitung in die EBIOS-Methodik.

Erstellung von Dokumente

In der EBIOS-Software ist es möglich, Dokumente zu erstellen. Um ein Dokument zu erstellen, geht man einfach im Bereich „Erstellung der Synthesedokumenten“. Folgende Abbildung zeigt die Software im Dokumentenerstellungsmodus:

Abbildung 38: EBIOS-Software – Erstellung von Synthesedokumenten

Die Erstellung eines Synthesedokuments besteht aus drei Schritten:

1. Auswahl der Sicherheitsstudie
2. Wahl des Dokumentenblocks
3. Generierung des Synthesedokuments

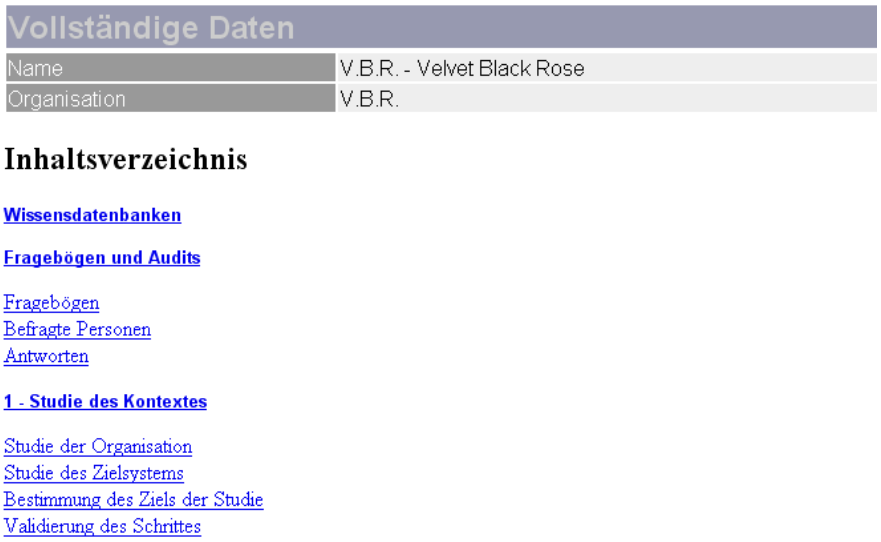
Die Reihenfolge der Ausführung kann beim Schritt eins und zwei vertauscht werden. Der dritte Schritt kann logischerweise erst ausgeführt werden, wenn die ersten beiden Schritte durchgeführt sind. Solange die erste beide Schritte noch offen sind, ist die Option „Generierung des Synthesedokuments“ grau markiert und nicht zugänglich.

Folgende Dokumente kann man mit der EBIOS Software erstellen (ohne nähere Beschreibung über die Art bzw. Funktion des Dokuments):

- FEROS
- SSRS
- Schutzprofile
- FEROS Synthese
- Sicherheits-Strategiemitteilung
- Sicherheitsvorgabe für ein Produkt
- Sicherheitsvorgabe für ein System
- Vollständige Studie
- PSSI

Es ist auch möglich, ein eigenes Synthesedokument zu erstellen. Um ein eigenes Dokument zu verwenden, muss man jedoch über Kenntnisse über XML verfügen, da die Dokumentenvorlage in XML definiert ist. Ferner ist zu bemerken, dass nirgendwo angeführt ist, wie man in Deutsch eine eigene Synthesedokument-Vorlage erstellt.

Nachdem man die Studie und die Art des Synthesedokuments ausgewählt hat, muss man nur noch den Pfad zur Dokumentengenierung angeben und anschließend auf dem Button „Generieren“ drücken. Folgende Abbildung zeigt ein Beispieldokument:


Vollständige Daten

Name	V.B.R. - Velvet Black Rose
Organisation	V.B.R.

Inhaltsverzeichnis

Wissensdatenbanken

Fragebögen und Audits

Fragebögen
Befragte Personen
Antworten

1 - Studie des Kontextes

Studie der Organisation
Studie des Zielsystems
Bestimmung des Ziels der Studie
Validierung des Schrittes

Abbildung 39: EBIOS-Software – Ein Synthesedokument

Die EBIOS Software unterstützt nur ein einziges Dokumentenformat: HTML. Wenn man die Dokumente auf PDF haben möchte, muss man die Konvertierung selbst machen. Die Unterstützung von anderen Dokumentenformaten ist wünschenswert, jedoch ist diese Einschränkung nicht sehr schwerwiegend.

Eine weitere Kritik im Bereich Dokumentenerstellung ist das nichtautomatische Öffnen des Synthesedokuments durch ein Browser nach der Generierung. Zurzeit muss man nach Generierung das Dokument selbst mit dem Browser öffnen. Wenn schon nur HTML unterstützt, sollte man sich schon ein wenig Mühe geben, um die Benutzerfreundlichkeit zu steigern.

Zum Abschluss dieses Abschnitts soll noch angemerkt werden, dass das Wort „Synthesedokument“ etwas unpassend gewählt ist. Es ist zwar eine persönliche Meinung, aber das Wort Synthese passt semantisch hier nicht in den Kontext, da ein Dokument aus einer Zusammensetzung von verschiedensten Daten besteht.

Programmsicherheit

Wie bereits erwähnt, basiert die EBIOS-Software auf die Programmiersprache Java. Die Konfiguration ist im XML-Datenformat gespeichert und sie befindet sich im Verzeichnis `data` unter dem EBIOS Installationsverzeichnis. In diesem Abschnitt werden die Aspekte bezüglich die Sicherheit genauer unter die Lupe genommen.

Im Abschnitt Administration wurde erwähnt, dass man in der EBIOS-Software verschiedenen Benutzer erstellen kann. Nach der Recherche werden die Benutzerdaten in der Datei `passwd.xml` gespeichert. Der folgende Codeabschnitt zeigt den Inhalt der Datei.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Users>
	<User ID="User.1219878995173" login="cc1980" type="administrator" pass
		word="wT7YHm2v%24FG5GCs.GdYGa2HT0IPmSi0" description="" />
	<User ID="User.1220124880132" login="audit" type="administrator" pass
		word="uNfTK9ig%24cdOYfYSV7Zqphw2brDbzH%2F" description="" />
</Users>
```

Testhalber wurde die Datei `passwd.xml` gelöscht und anschließend die EBIOS-Software neu gestartet. Das Programm bemerkt, dass die Datei `passwd.xml` fehlt und schreibt dabei folgende Einträge in das Error-Log:

```
14:15:15 GMT 2008     : [java.io.File] -> File for loading not found : <data/passwd.xml>
14:15:15 GMT 2008     : [scssi.ebios.user.UserManager] -> USER.Error.FileNotFound
```

Danach erzeugt das Programm einfach eine neue `passwd.xml` Datei. Da alle Benutzerdaten verloren gegangen sind, kann man dann wieder ohne weitere Zugangshürden auf allen

Teilen des Programmes zugreifen. Der Passwortschutz des Programmes kann man also sehr leicht umgehen.

Die Passwörter werden zwar in Hashwerten gespeichert, jedoch schützt die Speicherung der Passwörter in Hashwerte auch nicht vor der Umgehung der Benutzerrechte, da man die Datei `passwd.xml` problemlos editieren kann. Theoretisch kann man z.B. woanders eine EBIOS-Software Instanz starten und die Hashwerte ermitteln. Anschließend ersetzt man einfach den alten Hashwert durch einen neuen Hashwert, weil man dann das Passwort in Plaintext kennt. Damit ist der Passwortschutz umgangen. Wenn man danach die alte `passwd.xml` Datei wiederherstellt, wird der Benutzer wohl kaum etwas bemerken.

Es gibt viele Möglichkeiten, dieses Problem zu lösen. Ein Beispiel hierfür ist das Setzen der Rechte auf der Dateisystem-Ebene. Nachdem man die Anwender erstellt hat, setzt man die Datei `passwd.xml` einfach auf Nur-Lesen und verhindert damit effektiv das Überschreiben der Passwortdatei. Diese Lösung hat natürlich einen Nachteil: Man muss jedes Mal die Rechte umändern, falls man einen neuen Anwender anlegen möchte.

Sonstige Funktionen

Falls man nicht mit der EBIOS-Methodik vertraut ist bzw. noch nie mit der EBIOS-Software gearbeitet hat, ist der Bereich „Fallstudie“ die erste Anlaufstelle. Folgende Abbildung zeigt den Bereich „Fallstudie“:

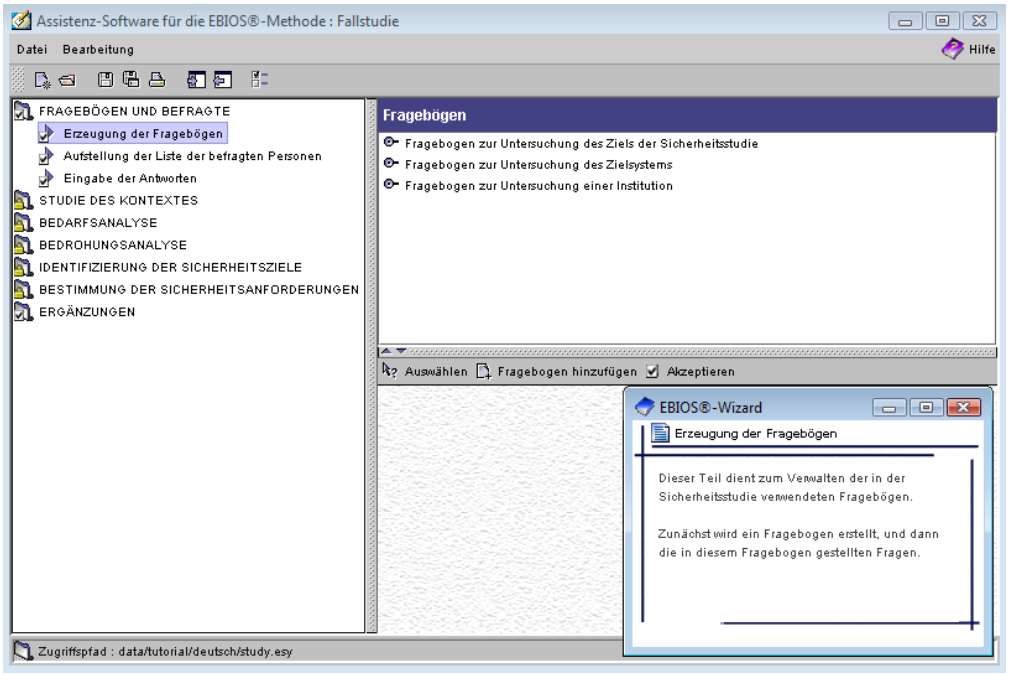


Abbildung 40: EBIOS-Software – Fallstudie mit Wizard

Man erkennt anhand der Abbildung nachdem man den Button „Fallstudie“ gedrückt hat, dass ein Arbeitsbereich für die Erstellung der EBIOS-Studie gestartet wird. Außerdem wird gleich die Fallstudie, die sich im Verzeichnis `/data/tutorial` befindet, geladen. Zusätzlich wird noch ein Wizard gestartet. Im Wizard stehen die relevanten Informationen über die markierte Aktivität. Anhand des Wizard kann man dann die Software bzw. die EBIOS-Methodik genauer kennenlernen.

Stärke und Schwäche

Die EBIOS-Software ist Open-Source, d.h. man kann sie herunterladen und für eigene Zwecke anpassen. Man muss jedoch anmerken, dass die neuste Version der Software bereits drei Jahre alt ist und es bereits die ersten Inkompatibilitäten mit Windows Vista gibt.

Die wichtigste Schwäche des Programms ist die bereits oben beschriebene Schwäche im Bezug auf die Softwaresicherheit. Das Programm soll zumindest einen Alarm geben, wenn die Passwortdatei verschwunden ist und nicht einfach den Fehler in das Error-Log zu schreiben und anschließend mit der Standardeinstellung starten.

Die graphische Oberfläche auf Basis von Java wird von manchen Personen sicher als unangenehm empfunden. Die Software ist nach der Kategorisierung von Risikomanagement Software im Kapitel sieben eine Einzelplatzanwendung und ein gemeinsames Arbeiten an einer Studie ist nicht möglich. Die Antworten der Fragebogen muss der Auditor selbst eintragen und es kann bei einer Papierbefragung mit sehr vielen Leuten sehr lang dauern.

Zusammenfassung

Die EBIOS Software ist für die konsequente Umsetzung der EBIOS Methode eine gute Lösung. Das Programm ist kostenlos und die Quellcodes sind frei zugänglich. Doch die letzte Version der Software ist bereits drei Jahre her und es erweckt den Eindruck, dass die Software nicht mehr weiterentwickelt wird. Aufgrund des Alters der neusten Version der Software ist sie bereits nicht mehr mit einigen visuellen Komponenten der Windows Vista kompatibel. Dennoch ist sie ein gutes Werkzeug, falls man die EBIOS Methode anwendet. Es wäre schön, wenn demnächst eine neure Version von EBIOS Software mit der aktuellsten Version der JRE herausgegeben wird.

11. Details zur Rimanis Evaluierung

Rimanis ist ein Risikomanagement-Informationssystem der Firma Hulocon mit Sitz am Frankfurt am Main in Deutschland. Diese Software kann man als ein Werkzeug für das Risikomanagement im operationellen Bereich einstufen. Jedoch kann man sie eigentlich auch ohne große Probleme im Bereich IT-Risikomanagement einsetzen. Eine Evaluierung der Software ist zahl sich daher auf jeden Fall aus.

An diese Stelle möchte ich mich noch bei Herrn Prof. Dr. Michael Huth für die unkomplizierte und schnelle Bereitstellung des Zugangs bedanken. Nicht sehr viele Firmen sind bereit einen Testzugang von ihrer Risikomanagement-Software bereitzustellen oder antworten überhaupt nicht auf die Evaluierungsanfrage.

Installation

Die Installation von Rimanis ist recht einfach, da ein Installer diese Aufgabe übernimmt. Die Größe der Installationsdaten (ZIP Datei) beträgt lediglich 36 Megabyte. In der Datei sind die Daten enthalten, die auch in der Rimanis-Installations-CD zu finden ist. Wenn man die Datei `rimanis.exe` startet, bekommt man folgende Willkommensmeldung zu sehen:

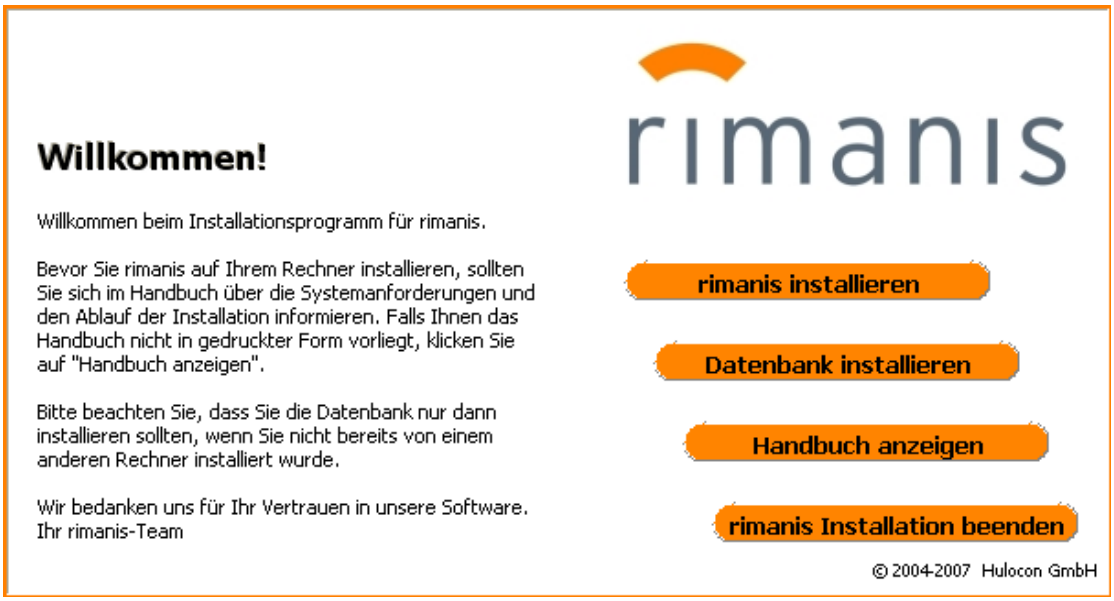


Abbildung 41: Rimanis – Willkommensfenster (HULOCON GmbH, 2007 S. 7)

Um die Software betriebsfähig zu machen, müssen folgende Installationsschritte durchgeführt bzw. eingehalten werden:

1. Installation der Datenbank
2. Installation der Rimanis-Software

Bevor man die Rimanis-Software installiert, muss die Rimanis-Datenbank bereits installiert sein, weil man bei der Installation der Software den Pfad zur Datenbank angeben muss. Die Installation der Rimanis-Datenbank ist recht einfach. Die Installation der Datenbank läuft wie folgt ab: Man akzeptiert die Lizenzbedingung, gibt die Benutzerdaten an und wählt das Verzeichnis der Installation aus. Danach braucht man nur noch einfach auf den Button „Weiter“ drücken. Da die Screenshots über die Installation der Datenbank sehr ähnlich der Installation der Rimanis Software sind, werden hier keine Screenshots beigefügt.

Bei der Installation der Datenbank werden lediglich vier Dateien in das vorgegebene Installationsverzeichnis kopiert:

- `currencies.dat`,
- `DBAccess.dat`,
- `Lizenzvereinbarung.pdf` und
- `rimanis.mdb`.

Die Datei `currencies.dat` enthält einige Abkürzungen der Landeswährungen. Die Funktion der Datei `DBAccess.dat` ist leider unbekannt, da die Länge der Datei null Byte ist. Man kann jedoch anhand vom Namen vermuten, dass diese Datei irgendwas mit dem Datenbankzugriff zu tun hat. In der Datei `Lizenzvereinbarung.pdf` sind die Lizenzvereinbarungen enthalten. Die Datei `rimanis.mdb` ist die eigentliche Datenbankdatei.

Nach der Installation der Rimanis Datenbank folgt nun die Installation der Rimanis Software. Wichtig bei der Installation ist, dass der Pfad der Datenbankdatei bekannt ist, sonst ist eine Installation nicht möglich. Die Installation der Software erfolgt auf ähnlichem Weg wie die Installation der Datenbanksoftware und wird hier nicht genauer beschrieben. Nachdem man alle erforderlichen Daten eingegeben hat, kann man zwischen vollständige und angepasste Installation auswählen. Die folgende Abbildung zeigt die verfügbaren Optionen bei einer angepassten Installation der Rimanis Software:

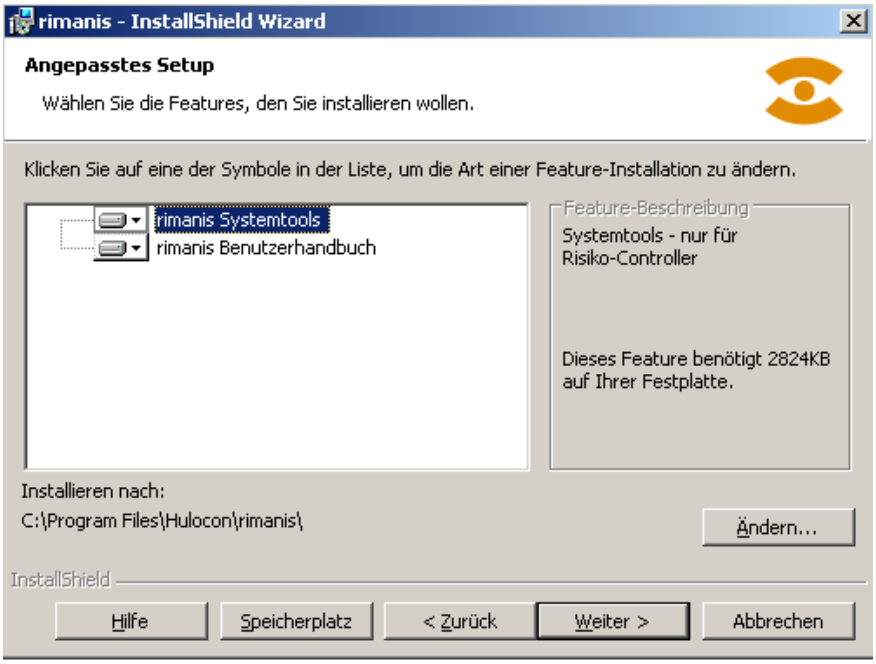


Abbildung 42: Rimanis – Angepasstes Setup

Nachdem man die Installationsoption ausgewählt hat, beginnt nun das Installationsprogramm, die Dateien zu kopieren. Nach kurzer Zeit ist die Installation fertig und die Software ist bereit für die erstmalige Anwendung. Laut Windows Explorer benötigt man für die Installation der Datenbank sowie die Software lediglich 10 Megabyte Speicherplatz. Daher kann man daraus schließen, dass Rimanis sehr kompakt ist und auch unter alten Systemen gut läuft. Ein Blick in das Benutzerhandlich bestätigt die Hypothese. Das Programm benötigt nur sehr wenige Ressourcen. Die Systemanforderungen für Rimanis sind:

- Windows ab Version 98
- Prozessor mit mindestens 133 MHz.
- Mindestens 32 MB Arbeitsspeicher
- Ca. 110 MB Festplattenspeicher

Einrichtung und die erste Eindrücke

Wenn man die Rimanis Software zum ersten Mal startet, wird man sofort mit einer Aufforderung zur Eingabe von Benutzer sowie das dazugehörige Passwort konfrontiert. Wer das Benutzerhandlich bis jetzt bis zum Kapitel Installation durchgelesen hat, wird sich jetzt ganz schön wundern, da man bei der Installation der Datenbank keine Passwörter eingegeben hat. Wenn man das Benutzerbuch jedoch weiterliest, steht im Kapitel „Rimanis zum ersten Mal starten“ genau mit welchem Benutzername man sich beim ersten Mal einloggen soll.

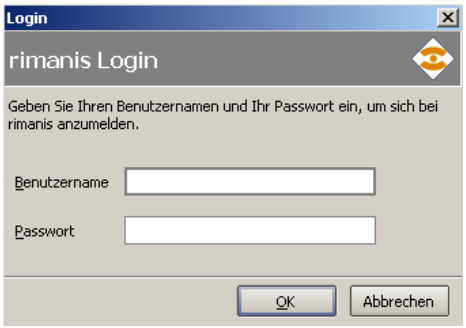


Abbildung 43: Rimanis – Login Dialog

Nachdem man den Benutzername eingegeben hat, startet das Programm automatisch einen Assistent für das erstmalige Einrichten des Programmes. Bei der Einrichtung fordert der Assistent auf, die relevanten Informationen über das Unternehmen wie z.B. Name oder Anschrift einzugeben. Nachdem man die Information zum Unternehmen eingegeben hat, muss man noch den Risiko-Erwartungswert sowie die maximale Vermögensminderung eingeben, da diese Werte eine effektive Risikosteuerung gewährleistet.

Wenn man bei der Einrichtung des Programmes nicht alle Daten zur Verfügung stehen, soll man zuerst einen geschätzten Wert eingeben. Die Daten können, falls erforderlich, später noch im Administrationsteil verändert werden. Nachdem man alle Daten eingegeben hat, wird noch die erste Managementperiode angelegt. Danach ist das Programm eingerichtet und kann sofort verwendet werden. Die folgende Abbildung zeigt das Hauptfenster des Rimanis-Programms:

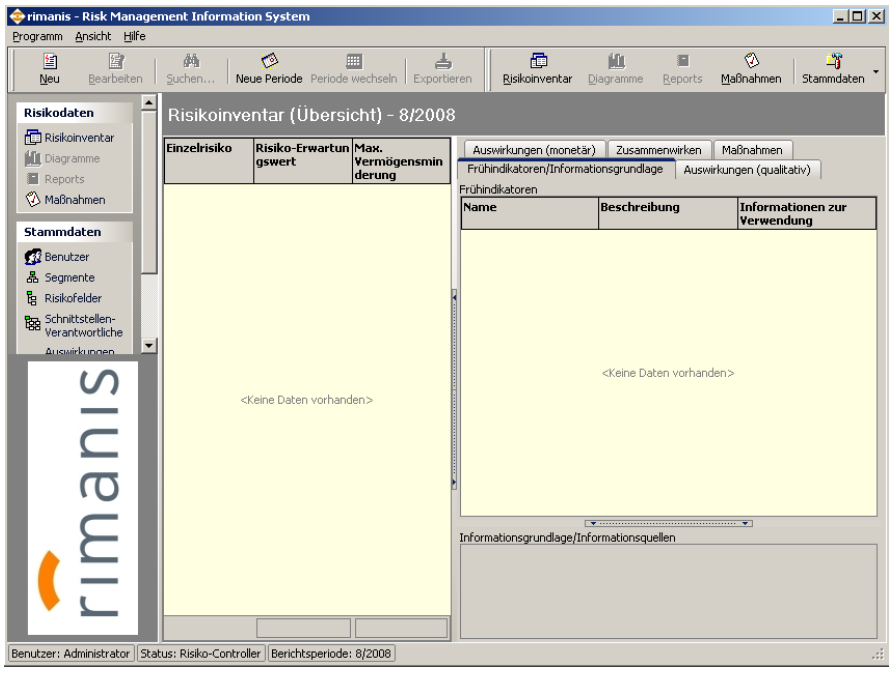


Abbildung 44: Rimanis – Hauptfenster

Die Rimanis-Software ist als eine SDI-Anwendung konzipiert. Das bedeutet, dass die Software nur ein Dokument anzeigen bzw. bearbeiten kann. Das Hauptfenster der Rimanis Software ist wie folgt aufgebaut:

- Ein zentraler Arbeitsbereich, wo die Diagramme, Reports und Risiken im verschiedenen Forman angezeigt werden.
- Die Rimanis-Leiste an der linke Seite des Hauptfensters, die einen schnellen Zugriff auf alle Elemente von Risikodaten und Stammdaten der Rimanis-Software ermöglicht.
- Eine Menüleiste.
- Eine Symbolleiste, die, viele Aufgaben wie z.B. Drucken oder Export der Daten schnell ermöglicht..
- eine Statusleiste, die verschiedene Informationen wie z.B. die Berichtsperiode anzeigt.

Der erste Eindruck zum Hauptfester des Rimanis-Programmes ist durchaus positiv zu bewerten. Das Design der Benutzeroberfläche ist gründlich durchdacht worden und man kann verschiedene Elemente des Programmes sehr schnell erreichen.

Verwaltung der Stammdaten

Nach der Einrichtung durch den Assistenten beim erstmaligen Start benötigt die Rimanis-Software noch andere Informationen, damit man ein Risikomanagement anfangen kann. Bevor man beginnt die Risiken zu erfassen, müssen die Stammdaten des Unternehmens wie z.B. Benutzer, Organisationsaufbau usw. in die Software eingespeist werden. Im Stammdatenbereich der Software kann man folgende Elemente verwalten:

- Benutzer
- Segmente
- Risikofelder
- Schnittstellenverantwortliche
- Auswirkungen auf das System
- Frühindikatoren
- Stammdaten des Unternehmens

Bevor man ins Details der Stammdatenverwaltung geht, muss noch gesagt werden, dass die Testversion von Rimanis zwar voll innerhalb der fünfzehn tägigen Testzeit lauffähig ist, jedoch einer wesentlichen Einschränkung unterliegt: der Anzahl der Datensätze. Die Anzahl an Datensätzen, die man in der Testversion eintragen kann, ist beschränkt. In den meisten Be-

reichen der Stammdatenverwaltung kann man maximal fünf Datensätze anlegen. Daher ist eine vollständige Modellierung des Business Cases in Rimanis nicht möglich. Dennoch kann man einen guten Eindruck über die Software gewinnen.

In der Benutzerverwaltung von Rimanis soll man nur Personen eintragen, die mit dem IT-Risikomanagement des Unternehmens zu tun haben. Die Rimanis Software unterscheidet dabei zwei Arten von Benutzer: Risiko-Controller und Risiko-Zuständige. Der Risiko-Zuständige Benutzer hat lediglich Zugriff auf seine eigenen Daten. Der Risiko-Controller Benutzer hat den vollen Zugriff auf die Stammdaten und kann die Operationen Erstellen, Löschen und Verändern von Elementen beliebig ausführen.

Standardmäßig ist der Benutzer „Administrator“ eingerichtet. Dieser Benutzer hat kein Passwort, es ist daher empfohlen, ein Passwort für diesen Benutzer zu setzen. Um einen Benutzer anzulegen, wechselt man einfach mit Hilfe der Rimanis-Leiste in die Benutzerübersicht. Alternativ kann man auch die Tastenkombination STRG+F2 verwenden, um noch schnell in die Benutzerübersicht umzuschalten. Die folgende Abbildung zeigt einen Dialog an, wie ein Benutzer in Rimanis angelegt werden kann:

Abbildung 45: Rimanis – Benutzer anlegen

Wie aus der Abbildung ersichtlich, muss man beim Erstellen eines Benutzers nicht viel tun. Die Benutzerarten sind, wie bereits oben erwähnt, fix definiert und können nicht mehr erweitert werden. Ein erweitertes Rechte Management wie z.B. das Rollenmanagement in GSTOOL ist wünschenswert, jedoch ist es nicht zwingend aufgrund der Art der Risikomanagement-Software erforderlich.

In der Verwaltung von Segmenten kann man die Struktur des Unternehmens erfassen. Es werden üblicherweise die funktionalen Einheiten des Unternehmens gespeichert. In der Eva-

luierung wird in diesem Fall der funktionale Aufbau der IT im Business Case eingetragen. Aufgrund der Beschränkung der maximal erstellbaren Datensätzen ist die komplette Erfassung des funktionalen Aufbaus im Business Case nicht möglich. Nur ein Benutzer mit der Funktion „Risiko-Controller“ kann Segmente anlegen, bearbeiten oder löschen. Ein Benutzer mit „Risiko-Zuständige“ Funktion kann lediglich die vorhandenen Segmente in der Datenbank anzeigen lassen.

Neben den Segmenten kann man auch die Risikofelder verwalten. Die Verwaltung der Risikofelder dient als eine andere Möglichkeit zur Strukturierung des Unternehmens. Laut Rimanis Handbuch werden Risikofelder häufig angewandt, um die objektbezogene Einheiten (Sparten) eines Unternehmens abzubilden. Bei der Evaluierung wird hier der IT-Service-Aufbau im Business Case verwendet. Wie bei der Verwaltung der Segmente, ist auch bei der Verwaltung der Risikofelder die maximale Anzahl von Datensätze beschränkt und eine komplette Abbildung des Business Cases nicht möglich. Der „Risiko-Controller“ Benutzer hat in der Risikofelder-Verwaltung den vollen Zugriff. Ein Benutzer mit der Funktion „Risiko-Zuständige“ kann nur die Risikofelder bearbeiten, die er als Verantwortliche zugewiesen bekommen hat.

Die Verwaltung der Schnittstellen-Verantwortlichkeiten hat in der Evaluierung anhand des Business Cases eher wenig Bedeutung. Bei bestimmten Organisationsformen wie der Matrixorganisation ist es jedoch erforderlich, für die Schnittstellen Verantwortlichkeiten zwischen Segment und Risikofelder zu definieren. Wie bei anderen Administrationsbereichen hat der Risiko-Controller den vollen Zugriff. Benutzer mit der Funktion „Risiko-Zuständige“ können sich nur die Schnittstellen-Verantwortlichkeiten anzeigen lassen.

Bevor man mit der Eingabe von Risikodaten beginnt, soll man noch die möglichen Auswirkungen im Falle eines Risikoeintritts in der Stammdatenverwaltung eintragen. Die Auswirkungen können vom allen Benutzer angelegt werden. Die Bearbeitung und die Lösung der Auswirkungen sind nur durch Risiko-Controller möglich.

Aufgrund der begrenzten Anzahl der erstellbaren Datensätze werden bei der Evaluierung nur sehr allgemeine Auswirkungen des Unternehmens wie z.B. Imageverlust oder finanziellen Schaden eingetragen. Um eine Auswirkung anzulegen, wechselt man einfach mittels Rimanis-Leiste in der Verwaltung der Auswirkungen. Noch schneller geht der Wechsel über die Tastenkombination STRG+F6.

In der Stammdatenverwaltung ist es ebenfalls möglich, Frühindikatoren anzulegen. Im Theorieteil wurden bereits die Risikoindikatoren vorgestellt, daher wird hier das Thema Indikatoren im Risikomanagement nicht weiter behandelt. Der Wechsel in die Frühindikatoren-Verwaltung erfolgt über die Rimanis-Leiste oder über die Tastenkombination STRG+F7. Aufgrund der Einschränkungen der Testversion werden bei der Evaluierung nur allgemeine Indikatoren wie z.B. Systemlast oder SLA Verstöße eingetragen.

Die Rimanis-Software macht im Teil der Stammdatenverwaltung einen sehr guten Eindruck. Mittels Rimanis-Leiste oder einer Tastenkombination kann man sehr schnell zwischen verschiedenen Verwaltungsübersichten wechseln. Die Dialoge für das Anlegen, Bearbeiten und Löschen der Stammdaten sind gut durchgedacht und man kommt hier schnell zurecht. Das Fehlen eines erweiterten Managements der Benutzerrechte ist jedoch kritisch zu sehen. Die starre Aufteilung von Benutzer in Risiko-Controller und Risiko-Zuständige ist wahrscheinlich für große Firmen nicht ausreichend.

Eingabe von Risikodaten

Nachdem man die Stammdaten eingegeben hat, kann man mit dem Eintragen der der Risiken in die Rimanis-Software beginnen. Die folgende Abbildung zeigt wohl den wichtigsten Arbeitsbereich in der Rimanis - das Risikoinventar:

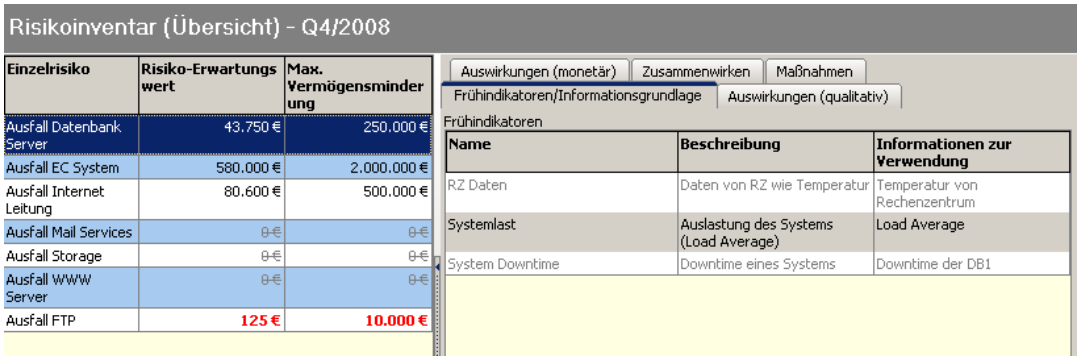


Abbildung 46: Rimanis – Das Risikoinventar

Das Risikoinventar im zentralen Arbeitsbereich der Rimanis ist in zwei Bereiche aufgeteilt. Auf der linken Seite werden die Einzelrisiken in tabellarischer Form dargestellt. Im rechten Bereich des Risikoinventars werden die Details eines ausgewählten Einzelrisikos auf mehreren Registerblätter dargestellt. Es gibt viele Einstellmöglichkeiten bei der Darstellung von Einzelrisiken im Risikoinventar. Man kann z.B. das Risikoinventar so einstellen, dass die Einzelrisiken nach Risikofelder gruppiert dargestellt werden. Nähere Informationen zur Ein-

stellung bzw. das Anpassen des Risikoinventars findet man im Benutzerhandbuch und wird hier nicht mehr weiter behandelt.

Das Anlegen eines Einzelrisikos ist sehr einfach, da man von einem Assistenten unterstützt wird. Um ein Einzelrisiko anzulegen, klickt man einfach auf das Symbol „Neu“ in der Symbolleiste. Alternativ kann man auch die Tastenkombination STRG+EINF verwenden. Der Assistent für das Anlegen eines Einzelrisikos enthält insgesamt fünf Schritten:

Schritt 1 Name und Beschreibung: Bei diesem Schritt soll man einen eindeutigen Namen für das Einzelrisiko angeben. Außerdem soll man noch eine Beschreibung für das Einzelrisiko eintragen, damit man später nicht raten muss, falls der Name des Risikos „ungünstig“ ausgewählt wurde.

Schritt 2 Verantwortlichkeiten: Hier werden die Verantwortlichkeiten eines Einzelrisikos definiert. Die Verantwortlichkeiten sind bereits in der Verwaltung von Segmenten und Risikofeldern definiert. Hier ordnet man einfach das neue Einzelrisiko einem Segment bzw. Risikofeld zu. Die Verantwortlichkeiten werden nach der Zuordnung automatisch im Assistenten angezeigt.

Schritt 3 Frühindikatoren: Die Indikatoren wurden bereits in der Stammdatenverwaltung definiert. Bei diesem Schritt kann man alle Frühindikatoren, die für das neue Einzelrisiko relevant ist, eintragen. Bei der Zuordnung von Frühindikatoren kann man noch zusätzlichen Informationen zur Verwendung des Frühindikators eingeben.

Schritt 4 Informationsgrundlagen: In diesem Schritt kann man weitere Informationsgrundlagen für das Einzelrisiko eintragen.

Schritt 5 Auswirkung auf das Zielsystem: Im fünften Schritt werden die relevanten Auswirkungen des Einzelrisikos erfasst. Die Auswirkungen müssen natürlich bereits in der Stammdatenverwaltung eingetragen sein. Es muss mindestens eine Auswirkungsart als relevant markiert werden, sonst ist das Fortsetzen nicht möglich.

Schritt 6 Weitere Auswirkungen auf das Zielsystem: Hier kann man noch die zusätzlichen Auswirkungen auf das System eintragen und es können weitere Auswirkungen beschrieben werden, die in der Stammdatenverwaltung, aus welchen

Grund auch immer, nicht erfasst sind.

Schritt 7 Monetäre Auswirkungen: In diesem Schritt werden die monetäre Auswirkungen des Einzelrisikos modelliert, falls man sie abschätzen kann. Wenn man die monetäre Auswirkungen schätzen kann, soll man die Vermögensverminderung sowie die Wahrscheinlichkeit für folgende drei Szenarien eingeben: hohe Vermögensminderung, mittlere Vermögensminderung und geringe bzw. gar keine Vermögensminderung.

Schritt 8 Toleranzwerte: In diesem Schritt werden die Toleranzwerte für den Risiko-Erwartungswert und für die maximale Vermögensverminderung angegeben. Bei einer Überschreitung der Toleranzwerte wird eine Warnung an den Verantwortlichen geschickt.

Schritt 9 Zusammenwirkung mit anderen Einzelrisiken: Es gibt Einzelrisiken, die mit anderen Einzelrisiken zusammenwirken. Der letzte Schritt beim Erstellen eines Einzelrisikos ist die Definition des Zusammenwirkens des Einzelrisikos mit anderen Einzelrisiken.

Nachdem Schritt neun ausgeführt wurde, wird das Einzelrisiko in die Datenbank gespeichert. Nach der Speicherung verlangt die Rimanis anschließend die Eingabe, ob man gleich die Maßnahmen zur Risikosteuerung anlegen möchte. Es ist nicht erforderlich die Steuerungsmaßnahmen gleich nach der Erstellung des Einzelrisikos anzulegen.

Falls man falsche Daten bei der Anlegung eines Einzelrisikos eingegeben hat, kann man sie ohne Probleme nachträglich löschen bzw. bearbeiten. Die folgende Abbildung zeigt den Arbeitsbereich für das Bearbeiten der Einzelrisiken:

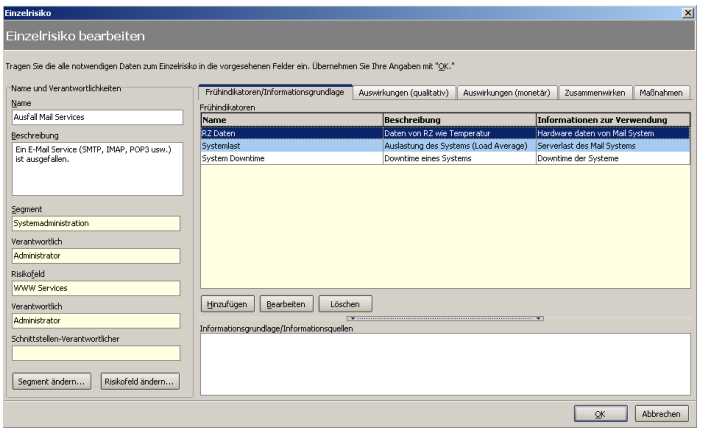


Abbildung 47: Rimanis – Einzelrisiko bearbeiten

Der Bearbeitungsdialog ist sehr verständlich aufgebaut. Im linken Bereich des Dialogs kann man den Namen sowie die Verantwortlichen des Einzelrisikos bearbeiten. Im rechten Bereich des Dialogs findet man fünf Registerblätter (Frühindikatoren/Informationsgrundlage, Auswirkungen qualitativ, Auswirkungen monetär, Zusammenwirken und Maßnahmen), wo man weitere Informationen zum Einzelrisiko bearbeiten kann.

Die Registerkarte „Maßnahmen“ ist die einzige Stelle im Programm, wo man die Maßnahme für die Risikosteuerung anlegen kann. Es gibt zwar eine Maßnahmenübersicht, jedoch kann man dort lediglich die Maßnahmen anzeigen sowie bearbeiten. Es gibt Steuerungsmaßnahmen, die man bei mehreren Risiken anwenden kann. In Rimanis sind die Maßnahmen an das Einzelrisiko gebunden. D.h. man muss eine neue Steuerungsmaßnahme mit dem gleichen Inhalt anlegen, wenn man die gleiche Maßnahme mit einem anderen Einzelrisiko verbinden will. Zuerst eine neue Maßnahme anlegen und dann an die Einzelrisiken zuweisen, ist der bessere Weg. Dadurch spart man das mehrmalige Eingeben der gleichen Maßnahme.

Die folgende Abbildung zeigt die Übersicht der Steuerungsmaßnahmen:

Maßnahmen (Übersicht)

Beschreibung	Einzelrisiko	Verantwortlich	Risiko-Controller/Risi	Priorität	Fällig am	Status	Erinnerung
Umschaltung auf 2. Backup Server	Ausfall Datenbank Server	Lina Inverse	Chia-chang Lin	Hoch	31.08.2008	Nicht erforderlich	30.08.2008
Umschaltung auf Backup EC System	Ausfall EC System		Luna Inverse	Hoch		Nicht erforderlich	
Backup Mail Service verwenden	Ausfall Mail Services		Sakura Hime Azuma	Normal		Nicht erforderlich	
Überprüfung und Reboot	Ausfall Storage	C.C.	Yoshika Mijafuji	Hoch		Nicht erforderlich	
Dateisystemüberprüfung	Ausfall Storage		Luna Inverse	Normal		Nicht erforderlich	
Umschaltung auf Backup Leitung	Ausfall Internet Leitung		Sakura Hime Azuma	Hoch		Nicht erforderlich	

Abbildung 48: Rimanis – Übersicht der Steuerungsmaßnahmen

Man kann mittels der Tastenkombination STRG+A ganz schnell in die Übersicht der Steuerungsmaßnahmen wechseln. Alternativ kann man auch die Rimanis-Leiste verwenden. Die Steuerungsmaßnahmen werden tabellarisch dargestellt und sind sehr übersichtlich. Um eine Maßnahme zu bearbeiten oder zu löschen, wählt man einfach in der Tabelle die Maßnahme aus und wählt anschließend das gewünschte Symbol (Löschen bzw. Bearbeiten) in der Symbolleiste der Software.

Risikomanagement Berichte

Die Rimanis Software bietet wie bei anderer Risikomanagement-Software die Möglichkeit, Berichte zu generieren. Es ist möglich folgende Berichte zu erstellen:

- Segment bezogene Risiken
- Risikoinventar nach Segmenten
- Ausgewähltes Einzelrisiko
- Risikoinventar nach Segmenten mit Zeitreihe der monetäre Auswirkungen
- Top 10 Risiko-Erwartungswert
- Risikofeld bezogene Risiken
- Risikoinventar nach Risikofeldern
- Risikoinventar-Handbuch
- Risikoinventar nach Risikofelder mit Zeitreihe der monetäre Auswirkungen
- Top 10 max. Vermögensverminderung

Es ist nicht möglich, einen eigenen Bericht zu definieren und zu erstellen. Man muss also mit den oben aufgelisteten zehn Berichtsarten auskommen. Falls man damit nicht auskommt, muss man das Risikoinventar exportieren und anschließend versuchen, selbst den Bericht zu erstellen. Die folgende Abbildung zeigt einen einfachen Risikomanagement-Bericht:

rimanis Risikomanagement-Report

V.B.R - Velvet Black Rose
Meidlinger Hauptstraße 47, 1120 Wien

Übersicht über risikofeld-bezogene Risiken (Q4/2008)

Risikofeld	Anzahl zugeordneter Einzelrisiken	Anzahl Risiken mit Risiko-Erwartungswert > 0
DB Services	1	1
Netzwerk	1	1
Storage	1	0
WWW Services	4	2
Anzahl	**7**	**4**

Abbildung 49: Rimanis – Ein Risikomanagement Bericht

Neben der Generierung von Berichte ist es auch möglich, Diagramme zu erstellen. Folgende Abbildung zeigt ein Diagramm, das während der Modellierung erstellt wurde:

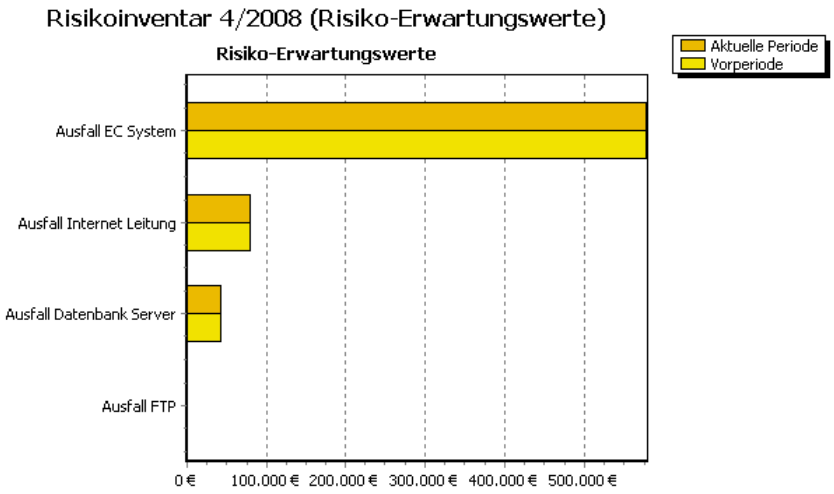


Abbildung 50: Rimanis – Diagramm über die Risiko Erwartungswerte

Die Software unterstützt nur Balkendiagramme, andere Diagrammarten werden nicht unterstützt. Wie bei der Generierung der Berichte, gibt es keine Möglichkeit unter Rimanis, selbst definierte Diagramme zu erstellen. Das Programm erlaubt lediglich für die Risiko-Erwartungswerte und die maximale Vermögensverminderung die Generierung von Balkendiagrammen. Wenn man andere Diagrammarten haben möchte, muss man das Risikoinventar exportieren und selbst erstellen.

Die Berichtsfunktion von Rimanis ist für kleine und mittelständische Unternehmen geeignet. Für große Unternehmen wird die Berichtsfunktion wohl aufgrund der hohen Anforderungen nicht ausreichend sein. Die Möglichkeit, einen eigenen Bericht oder ein eigenes Diagramm zu definieren, ist nicht vorhanden. Aber aufgrund des günstigen Preises pro Lizenz kann man nicht erwarten, dass solche Funktionen vorhanden sind.

Import/Export von Daten

In der Rimanis-Software gibt es keine Möglichkeit, die bereits existierenden Daten zu importieren. Das Fehlen der Importfunktion ist nicht so schwerwiegend, da der Preis der Software auch recht günstig ist. Falls man doch etwas importieren möchte, kann man es mit Microsoft Access versuchen, da die Datenbank von Rimanis eine Access Datenbank ist. Jedoch soll man vorher ein Backup machen, weil nach dem Import Probleme entstehen können.

Die Exportfunktion von Rimanis ist auch nicht sonderlich ausgereift. Man kann lediglich das Risikoinventar exportieren. Beim Export kann man zwischen vier Exportformate entscheiden: Microsoft Excel-Datei, HTML-Datei, Textdatei und XML-Datei.

Eigentlich denkt man, bevor man das Benutzerhandbuch anschaut, beim Export von Risikoinventar, dass alle zugehörigen Daten zu einem Risiko (Name, Verantwortliche, Frühindikatoren usw.) exportiert werden. Wenn man einen Export ausführt und anschließend die Datei anschaut, erlebt man eine Überraschung, wenn man das Benutzerhandbuch noch nicht angeschaut hat. Die folgende Abbildung erklärt warum:

	A	B	C
1	**Einzelrisiko**	**Risiko-Erwartungswert**	**Max. Vermögensminderung**
2	Ausfall Datenbank Server	43750	250000
3	Ausfall EC System	580000	2000000
4	Ausfall Internet Leitung	80600	500000
5	Ausfall Mail Services	0	0

Abbildung 51: Rimanis – Export des Risikoinventars

Wie man anhand der Abbildung erkennt, werden lediglich drei Elemente des Risikoinventars exportiert: der Name des Einzelrisikos, der Risiko-Erwartungswert und die maximale Vermögensminderung. Mit den exportierten Daten kann man also recht wenig anfangen, außer paar Diagrammen zu erstellen.

Rimanis und der Risikomanagement-Prozess

Die Rimanis-Software ist eine Eigenentwicklung von HULOCON GmbH und basiert nicht auf irgendwelche Standards oder Best Practices. Es ist daher sehr interessant, zu untersuchen, mit welchen Funktionen der Rimanis-Software die entsprechenden Komponenten des Risikomanagementprozesses (Risikoidentifikation, Risikobewertung, Risikosteuerung, Risikoüberwachung) unterstützt werden.

Kontextdefinition:	Durch die Verwaltung der Stammdaten, vor allem der Segmente und der Risikofelder, wird der zu betrachtende Kontext für das IT-Risikomanagement definiert.
Risikoidentifikation:	In der Phase Risikoidentifikation hilft die Software bei der Erfassung der Risiken mittels eines Assistenten. Die erfassten Risiken werden im Risikoinventar übersichtlich dargestellt. Außerdem ist eine Gruppierung und Sortierung der Risiken möglich.
Risikobewertung:	Die Rimanis-Software erfasst die Wahrscheinlichkeit eines Risikoeintritts. Die ermittelten Auswirkungen eines Risikoeintritts werden in der Stammdatenverwaltung erfasst.
Risikosteuerung:	Im Risikoinventar können die Steuerungsmaßnahmen eines Einzelrisikos erfasst werden. Alle Steuerungsmaßnahmen werden tabellarisch in der Maßnahmenübersicht angezeigt und können bearbeitet bzw. gelöscht werden.
Risikoüberwachung:	Die Berichtsfunktion unterstützt die Überwachung der Risiken. Mittels Diagrammfunktion kann die Entwicklung der Risiken übersichtlich dargestellt werden. Bei der Überschreibung eines vordefinierten Toleranzwertes wird automatisch die verantwortliche Person eines Einzelrisikos informiert.

Sonstige Bemerkungen

Die Preisgestaltung der Rimanis-Software ist recht interessant. Die erste Lizenz ist die teuerste und kostete laut Preisliste von 1. Januar 2008 € 950,00. Falls man mehr Lizenzen braucht, kostet die zweite bis fünfte Lizenz nur € 250,00 zusätzlich pro Lizenz. Die sechste bis zehnte Lizenz ist noch günstiger, nämlich € 200,00 zusätzlich pro Lizenz. Wie man sieht sind die Preise gestaffelt. Hier ein kleines Berechnungsbeispiel:

Preis für 15 Rimanis Lizenzen		
1. Lizenz	1 x € 950,00	€ 950,00
2. bis 5. Lizenz	4 x € 250,00	€ 1.000,00
6. bis 10. Lizenz	5 x € 200,00	€ 1.000,00
11. bis 15. Lizenz	5 x € 150,00	€ 750,00
Summe		**€ 3.700,00**

Tabelle 5: Rimanis – Kosten für 15 Lizenzen

Neben dem Preis soll noch erwähnt werden, dass mehrere Leute auf eine gemeinsame Datenbank der Rimanis Software arbeiten können. Das ist auch der Grund, warum die Installation in zwei Schritten (Installation der Datenbank, Installation der Software) aufgeteilt wurde. Wenn man eine zentrale Datenbank einrichten will, muss der Installationspfad über das Netzwerk erreichbar sein (z.B. Installation auf einen Dateiserver). Bevor man mit der Installation der Software beginnt, muss man noch im Windows Explorer die Netzwerkressourcen als Netzlaufwerk einbinden, denn das Installationsprogramm akzeptiert direkte Eingabe von UNC Ressource, wo sich die Datenbank befindet, nicht.

Die gemeinsame Nutzung der Datenbank läuft einwandfrei und wurde auf mehreren virtuellen Maschinen getestet. Die Software bleibt jedoch für den Einsatz in großen Unternehmen ungeeignet, obwohl ein gemeinsames Arbeiten auf einer Datenbank möglich ist. Die Microsoft Access Datenbanken haben eine beschränkte Netzwerkfähigkeit und die Leistung ist nicht für große Unternehmen ausreichend. Für kleine und mittlere Unternehmen ist diese Lösung jedoch ideal.

Stärke und Schwäche

Die Stärken und Schwächen der Rimanis Software richten sich nach dem Einsatzgebiet der Software. Die Software ist nicht sonderlich für große Firmen geeignet und hat viele Nachteile

wie z.B. Performance der Datenbank. In mittelständischen oder kleinen Unternehmen ist das Problem nicht so relevant, da nicht viele Benutzer auf die Software zugreifen.

Ein wichtiger Vorteil der Rimanis-Software ist der Preis. Fast jedes Unternehmen kann sich diese Software leisten, da sie relativ günstig ist. Die Lizenzpreise sind gestaffelt, je mehr Lizenzen man kauft, desto günstiger ist der durchschnittliche Preis pro Lizenz. Trotz des günstigen Preises ist eine Evaluierung vor dem Kauf notwendig, um herauszufinden, ob die Software geeignet für die geplante Einsatzumgebung ist.

Ein weiterer Vorteil neben den Preis ist die Kompaktheit des Programmes. Die Systemanforderungen an die Software bzw. die Hardware für die Verwendung des Programmes sind relativ gering. Man kann daher ohne Bedenken Rimanis auf einem alten Computersystem installieren. Jedoch muss man einwenden, dass die geringe Systemvoraussetzungen eigentlich kein richtiger Vorteil ist, denn es ist sehr unwahrscheinlich, dass noch sehr alte PC-Systeme in Verwendung sind, egal wie groß das Unternehmen ist.

Die Benutzeroberfläche der Rimanis-Software ist gut durchgedacht und kann auch als ein Vorteil gewertet werden. Mittels Rimanis-Leiste kann man sehr schnell in andere Übersichten wechseln. Um die Suche nach ein bestimmtes Einzelrisiko zu erleichtern, wurde eine Suchfunktion implementiert. Der Bearbeitungsdialog des Einzelrisikos wird sofort geöffnet, falls bei der Suche das zu suchende Einzelrisiko eindeutig identifiziert wurde.

Zu kritisieren ist die umständliche Installation, falls man auf einer gemeinsamen Datenbank arbeiten möchte. Man muss zuerst die Netzwerkressource, wo die Datenbank sich befindet, als Netzlaufwerk in Windows einbinden, bevor man die Installation der Rimanis-Software durchführt, da das Installationsprogramm die Eingabe einer UNC Ressource nicht akzeptiert und eine Fehlermeldung zurückgibt. Durch die Verwendung von Microsoft Access als Datenbank ist das Einsatzgebiet der Software auch eingeschränkt. Die Netzwerkfähigkeit der Access-Datenbanken ist beschränkt, außerdem muss man vorsichtig mit der Freigabe der Netzwerkressource umgehen, damit man die Datenbank nicht versehentlich bzw. absichtlich löscht. Die Unterstützung eines Datenbankserver-Produktes wie z.B. Microsoft SQL Server oder die Oracle-Datenbank ist notwendig, falls man das Programm in einer großen Umgebung verwenden möchte.

Ein weiterer Kritikpunkt der Software ist der bescheidene Umfang der Exportfunktion. Zwar unterstützt die Software unterschiedliche Exportformate, jedoch nutzt dies wenig, wenn man nur Name, Risiko-Erwartungswert und maximale Vermögensverminderung exportieren kann.

Eine Erweiterung des Exportumfangs ist daher sehr notwendig, auch wenn die Preise für die Software recht günstig sind.

Der letzte Kritikpunkt der Rimanis-Software, der noch hier erwähnt werden soll, ist die zu starke Kopplung der Steuerungsmaßnahmen an den Einzelrisiken. Die Steuerungsmaßnahmen müssen über dem Bearbeitungsdialog der Einzelrisiken erstellt werden. Die neu erstellte Steuerungsmaßnahme gilt nur für ein bestimmtes Einzelrisiko. Eine Steuerungsmaßnahme kann man in manchen Fällen auch für mehrere Einzelrisiken verwenden. In der Rimanis-Software müssen in diesem Fall mehrere gleiche Steuerungsmaßnahmen aufgrund der zu starken Kopplung erstelle werden. Die Lösung des Problems ist hier recht einfach: das Baukastenprinzip. Die Steuerungsmaßnahmen soll zentral über die Maßnahmenübersicht erstellt, bearbeitet und gelöscht werden. Bei der Bewertung eines Einzelrisikos werden dann die in der Datenbank vorhandenen Steuerungsmaßnahmen ausgewählt und verknüpft. Dadurch ist es möglich, die mehrmalige Eingabe von gleichen Risiko-Steuerungsmaßnahmen zu umgehen.

Zusammenfassung

Die Rimanis Software ist ein brauchbares Tool, das Risikomanagement in Klein- und Mittelbetrieben ausreichend unterstützt. Sie basiert auf den allgemeinen Risikomanagement-Prozess und nicht auf irgendwelche Standards oder Best Practices. Dadurch ist das Programm nicht nur im Bereich IT-Risikomanagement einsetzbar, sondern auch im operationellen Risikomanagement.

Insgesamt kann man zusammenfassen, dass die Rimanis-Software nur im kleinen und mittelständischen Unternehmen geeignet ist. Für den Einsatz im großen Firmen gibt es andere Produkte, die besser dafür geeignet sind. Der Hauptkritik bei der Rimanis Software ist das schlechte Design bei den Steuerungsmaßnahmen sowie die bescheidene Exportfunktionen. Wenn man jedoch die Preisaspekte mit in Betracht zieht, muss man die Nachteile hinnehmen, da die Lizenzkosten gering sind.

12. Zusammenfassung und Abschluss

Das IT-Risikomanagement wird bereits in vielen Unternehmen, egal ob groß oder klein, durchgeführt und gewinnt immer mehr an Bedeutung aufgrund der Entwicklung im Bereich der Informationstechnologie. Die meisten Unternehmen sind heutzutage bereits mit dem Internet verbunden und werden von verschiedenen Gefahren/Risiken wie beispielsweise. Spionage oder Hacking bedroht.

Um den Schaden im IT-Bereich zu minimieren, ist es daher notwendig, IT-Risikomanagement durchzuführen. Das IT-Risikomanagement ist ein sich wiederholender Prozess, der niemals endet. Man kann den RM-Prozess generell in vier Komponenten unterteilen: Risikoidentifizierung, Risikobewertung, Risikoüberwachung und Risikosteuerung.

Es gibt keinen allgemeinen Standard für das IT-Risikomanagement. Das ist auch der Grund, warum die Evaluierung von Risikomanagement-Tools sehr schwierig zu gestalten ist. Es existiert eine Vielzahl von Standards und Best Practices, auf die die Risikomanagement-Tools basieren. Daher wurde bei der Evaluierung entschieden, dass der Schwerpunkt der Bewertung die Software selbst ist. Dabei werden die Vor- und Nachteile von bestimmten Standards oder Best Practice Ansätze bewusst nicht in die Evaluierung aufgenommen, um eine endlose Diskussion über den Vor- und Nachteile des Standards oder Best Practice Ansatzes zu vermeiden. Das Unternehmen muss vor bzw. bei der Evaluierung selbst entscheiden, welchen Standard oder Best Practice Ansatz es einsetzen will.

Wenn man die Vor- und Nachteile der Standards und Best Practice Ansätze nicht in der Bewertung einfließen lässt, kann man das GSTOOL als Sieger der Evaluierung bezeichnen. Die Software setzt den IT-Grundschutz sehr konsequent um und die Bedienung ist sehr durchdacht. Weiters gibt es im GSTOOL ein sehr überlegtes Management von Benutzerechten. Zu kritisieren ist hier die eigenartige Installation sowie der Webkurs zum GSTOOL, das bei der Evaluierung nicht auf den neusten Stand ist.

Die Rimanis Software basiert nicht auf irgendeinen Standard oder Best Practice Ansatz, sondern unterstützt den allgemeinen Risikomanagement-Prozess. Das Design der Benutzeroberfläche ist sehr gut gelungen und man findet sich im Programm schnell zurecht. Obwohl das Programmdesign sehr gut gelungen ist, belegt die Rimanis-Software lediglich den zweiten Platz, weil die Software weniger Funktionen anbietet als GSTOOL. Außerdem ist die Exportfunktion nicht besonders toll.

Die EBIOS-Software ist kostenlos erhältlich und setzt die EBIOS-Methodik konsequent um. Trotzdem landet die EBIOS-Software auf den dritten Platz der Evaluierung. Die Bedienung ist sehr gewöhnungsbedürftig und es gibt kein Benutzerhandbuch im Deutsch. Ein gemeinsames Arbeiten an einer Datenbank ist in EBIOS nicht möglich und es gibt bereits die ersten Inkompatibilitäten mit Windows Vista, da die Software seit drei Jahren nicht mehr aktualisiert wurde. Ebenfalls zu kritisieren ist die schlechte Sicherheitseigenschaft des Programmes. Um den Vollzugriff zu erlangen, braucht man lediglich die Passwortdatei löschen.

Abschließend ist es noch zu bemerken, dass der Ausgangspunkt der Evaluierung ein mittelständisches Unternehmen ist. Der Einsatz von Risikomanagement-Software ist generell zu empfehlen, egal ob das Unternehmen groß oder klein ist. Der Einsatz hängt jedoch auch von der Risikomanagement-Organisation des Unternehmens ab. Manchmal reicht es auch aus, die Risiken einfach manuell zu verwalten, wenn das Unternehmen klein ist. Die Beschaffung solcher Software hängt daher sehr stark vom Nutzen ab. Es hat kein Sinn eine IT-Risikomanagement-Software zu kaufen bzw. zu verwenden, wenn das Einsparungspotential nicht vorhanden ist.

Anhang A. Business Case

A.1. Kurzbeschreibung Business Case

Der Business Case enthält Informationen und dient als Input für die Evaluierung der RM-Software. Am Anfang des Dokuments wird die Firma kurz vorgestellt. Danach folgen die Interviews der IT Abteilungen. Am Ende des Dokuments befinden sich noch drei Abbildungen, um einen Überblick über die IT Organisation zu geben.

A.2. Unternehmensprofil

Das Unternehmen V.B.R. ist eine Handelsfirma im Bereich Export/Import von Waren. Sie ist weltweit tätig und die Firmenzentrale befindet sich in Wien. Weitere Standorte in Europa sind Amsterdam und Hamburg. Ihre Tätigkeit besteht hauptsächlich aus dem Import von Lebensmittelspezialitäten aus aller Welt, um sie dann in Europa an verschiedenen Handelskette bzw. Lebensmittelgeschäft zu verkaufen.

In der Firmenzentrale Wien sind mehr als 250 Mitarbeiter in verschiedenen Bereichen tätig. Die IT Abteilung besteht aus ein Team von ca. 40 Personen. Sie betreut neben der IT Infrastruktur der Firmenzentrale auch noch die E-Commerce Anwendungen, die von allen Standorte verwendet werden.

Im Anhang befinden sich drei Zeichnungen, die die IT Organisation in der Firmenzentrale Wien in verschiedenen Aspekten beschreiben.

A.3. Interview mit CIO

Q: Beschreiben sie Ihre Tätigkeiten als CIO im Unternehmen.

Meine Aufgabe als Chief Information Officer ist die Führung, Reorganisation und Coaching der unternehmensinternen IT Abteilung, die aus 40 Personen besteht. Ich bin außerdem verantwortlich für die Leitung, Koordination, Ausführung und Optimierung der aktuellen und zukünftigen Architektur des Unternehmens sowie den zugehörigen Projekten.

Q: Sie haben vor drei Jahren entschieden, vermehrt Open Source Software einzusetzen. Warum haben sie für Open Source Software entschieden?

Die Softwarekosten waren nicht der einzige Grund, vermehrt Open Source Software einzusetzen. Durch Open Source können wir flexibler auf alle Anforderungen reagieren und zugleich unsere Unabhängigkeit bewahren.

Viele Mitarbeiter unserer Abteilung haben schon mehrere gute Erfahrungen mit Open Source Lösungen gemacht. Deshalb gab es keine Bedenken über den Einsatz von Open Source Lösungen. Bevor ein Produkt zum Einsatz kommt, werden natürlich ausführliche Tests durchgeführt. Zusätzlich haben wir uns vor dem Einsatz von Open Source Software mit Support Verträgen abgesichert. Wir haben die Umstellung zuerst in unkritischen Bereichen wie z.B. FTP Server begonnen. Nach einer Evaluierungsphase haben wir dann entschieden, die Umstellung auch im Kernbereich durchzuführen. Die Umstellung auf Open Source Software in Kernbereichen wie der Datenbank oder unseren E-Commerce Anwendungen wurde bereits vor ein Jahr abgeschlossen. Die allgemeine Reaktion auf die Umstellung war sehr gut und unser CFO freut sich natürlich auch.

Q: Warum haben sie einige Software bzw. Betriebssysteme auch nicht auf Open Source Software umgestellt?

Es war eine ausdrückliche Bitte (oder Aufforderung?) an mich, bei den Workstations noch proprietäre Software wie z.B. Microsoft Windows XP einzusetzen. Zugegeben wir sind keine IT Dienstleistungsfirma und nicht alle Mitarbeiter sind IT Profis. Viele ältere bzw. IT unerfahrene Angestellte können nicht so gut mit dem Computer umgehen. Nach der Ansicht des Managements ist es wohl besser, dass die Mitarbeiter nichts von der Umstellung spüren sollen und dadurch wie gewohnt arbeiten können. Dies ist auch fast gelungen. Die Mitarbeiter haben kaum was bei der Umstellung auf Open Source Software gemerkt.

Die Zusammenarbeit zwischen Open Source und proprietäre Software funktioniert in unserem Unternehmen sehr gut und es gibt kaum Schwierigkeiten. Bevor der Support von Windows XP abläuft, müssen wir überlegen, wie es weiter geht im Bereich von Workstations. Ich habe zurzeit noch Bedenken mit dem Umstieg auf Windows Vista, da die Umstellung sehr schwierig ist. Alte Hardware müssen auf den neusten Stand gebracht werden, bzw. ist man mit der Inkompatibilität von älterer Software die bei uns noch gibt, mit Windows Vista, konfrontiert. Die Umstellung auf Open Source Software bzw. Betriebssystemen ist jedoch auch sehr schwierig. Selbst wenn die Beschaffung kostenlos ist, muss man die aufwändige Migration der Daten wie z.B. Word- oder Excel Makros durchführen. Ich werde die Lage noch ein wenig beobachten und unsere Abteilung für Standardsoftware beauftragen, Windows Vista

noch mal genau anzuschauen, wenn Service Pack 1 zur Verfügung steht. Ich erwarte bzw. glaube, dass Microsoft mit den ersten beiden Service Packs die gröbsten Probleme von Windows Vista bereinigt.

Q: Worauf legen Sie als Leiter der IT Abteilung bezüglich Ihrer IT-Infrastruktur den größten Wert?

Wie immer soll eine IT Infrastruktur ausfallsicher, skalierbar, flexibel und natürlich auch kostengünstig sein.

Q: Wie schaut die weitere IT Pläne des Unternehmens aus?

Für unseren Kunden gestalten wir derzeit unsere E-Commerce Lösung um. In naher Zukunft können unsere Kunden direkt auf unser Bestellsystem zugreifen bzw. das Bestellsystem in ihre Systeme integrieren. Damit ist eine vollautomatische Abwicklung der Bestellungen möglich und die Effizienz wird dadurch gesteigert.

Neben der Optimierung des Geschäftsprozess im Kundenbereich werden weitere interne Geschäftsprozesse verbessert. Die Zusammenarbeit zwischen den Mitarbeitern soll erleichtert werden. Dafür haben wir bereits ein Instant Messaging Service eingeführt. Der nächste Schritt ist die Verbesserung von vorhandener Groupware im Intranet, um den Mitarbeiter bei der Zusammenarbeit weiter zu unterstützten.

A.4. Interview CSO

Q: Beschreiben sie ihre Aufgaben als CSO

Einfach ausgedrückt, bin ich der Verantwortliche für den Bereich Sicherheit. Dazu gehört nicht nur die IT Sicherheit, sondern auch die Sicherheit im organisatorischen und physischen Bereich. Ferner bin ich verantwortlich für die Durchführung, Einhaltung, Kontrolle Entwicklung von sicherheitsrelevanten Themen.

Q: Sicherheit ist ein sehr wichtiger Aspekt. Haben sie keine Bedenken bezüglich Sicherheit beim Einsatz von Open Source Software?

Ich habe eigentlich nicht viele Bedenken bezüglich Sicherheit beim Einsatz von Open Source Lösungen. Wir setzen außerdem nur Produkte ein, wenn wir sie für den Einsatz genug stabil halten.

Wir haben im Unternehmen einen CSO sowie eine Abteilung für IT-Security, die das Netzwerk überwacht und bei Problemen eingreift. Die Security Patches werden regelmäßig im System installiert und wir haben uns auch mit Verträgen von Sicherheitsspezialisten abgesichert, falls doch ein sehr schwerwiegendes Sicherheitsproblem entdeckt würde.

Q: Wie ist die IT-Security Abteilung aufgebaut?

Die IT-Security Abteilung ist in zwei Teams aufgeteilt: Netzwerk Security und Application Security. Wie der Name aussagt, ist das Netzwerk Security Team nur im Bereich des Netzwerks tätig. Das Application Security Team beschäftigt sich mit der Sicherheit der eingesetzten Software. Näheres erfahren Sie beim Interview mit dem Leiter des Security Teams.

Q: An welchen Security Incident können Sie besonders daran erinnern?

An einen Fall vor ca. ein Jahr kann ich mich ganz genau erinnern: Unsere EC-Systeme waren von DDoS Attacke eines Botnetzes betroffen. Zwar steht vor den Servern eine Firewall, die bei DDoS jedoch so gut wie nichts hilft. Die Server waren mehr als überlastet und wurden blockiert. Um unser Netzwerk bzw. unsere Systeme zu schützen, bleibt uns leider nichts anderes übrig, als ein paar IP Null zu routen. Wir waren aufgrund dieses Angriffs mehreren Stunden nicht erreichbar und viele Server mussten neu überprüft werden. Die Schäden waren im finanziellen Bereich enorm. Auch das Image des Unternehmens hat darunter stark gelitten.

A.5. Interview mit Network Security Team

Q: Welche Aufgabe hat das Network Security Team?

Das Network Security Team hat die Aufgabe, das Netzwerk zu überwachen. Dabei suchen wir nach Anomalien im Netzwerk der Unternehmenszentrale. Wir greifen aktiv im Netzwerk ein, falls die Anomalie ein Angriff von außen ist. Neben der Überwachung des Netzwerks erstellen wir auch regelmäßig Berichte über die Netzwerksicherheit und leitet sie an den CSO weiter.

Q: Wie wird das Netzwerk überwacht?

Um das Netzwerk zu überwachen, setzen wir Network Intrusion Detection Systeme ein. Dabei kommt Snort, ein sehr populäres Network IDS, zum Einsatz. Der Netzwerk Traffic wird auf der Basis von Regelwerken überwacht.

Q: Wie viele Anomalien entdeckt das Team pro Tag?

Das Intrusion Detection System meldet sehr viele Anomalien pro Tag. Es handelt sich aber meistens um ein „Rauschen“ im Internet wie z.B. Scans von Skriptkiddies und kann ruhig ignoriert werden. Natürlich registrieren wir auch Angriffsversuche wie z.B. Bruteforce Attacken mit mehr als 10000 Versuchen auf unsere Webserver. Doch solche Angriffe erleben wir nicht jeden Tag.

Q: Sehen sie den Einsatz von Netzwerk IDS als ausreichend?

Natürlich nicht. Neben dem Einsatz von Netzwerk IDS haben wir noch auf jeden wichtigen Server ein hostbasiertes Intrusion-Detection-System installiert. Ein Host IDS erkennt einen Angriff von der Innenseite besser. Außerdem Erkennt HIDS Angriffe, bevor sie das Netzwerk erreicht.

Q: Wie sehen sie das Problem bei der Überwachung mit IDS

Ein IDS ist nur so sicher, wie es der Kenntnisstand der Administratoren und Entwickler erlaubt. Außerdem wird ein IDS von Menschen entwickelt und administriert. Man soll sich nicht immer blind auf ein IDS verlassen. Wir verbessern laufend die Regeln für unsere IDS, um die Erkennungsrate zu optimieren sowie den Anzahl von False Positives bzw. False Negatives so gering wie möglich zu halten.

A.6. Interview mit Software Security Team

Q: Welche Aufgabe hat das Software Security Team?

Wie der Name sagt, ist das Software Security Team für die Sicherheit der eingesetzten Software in der Firma zuständig. Wir sorgen dafür, dass unsere Server, Workstations, Laptops und PDAs optimal vor einen Angriff geschützt sind. Wir arbeiten mir mehreren IT Abteilungen

zusammen, um ein umfassendes Sicherheitskonzept der eingesetzten Software zu erstellen und zu verbessern.

Neben der Erstellung und Verbesserung von Sicherheitskonzepte sind wir zuständig für die Installation von Sicherheitsupdates. Wir beobachten laufend die aktuellen Meldungen bezüglich Softwaresicherheit. Falls ein von uns eingesetztes Produkt ein Sicherheitsloch hat, veranlassen wir die Installation von Updates. Die Updates werden von uns vorher gründlich getestet, bevor sie für die Installation freigegeben werden. Falls ein Update aus welchem Grund auch immer nicht zur Verfügung steht, greifen wir selbständig ein und schreiben ein eigenes Updateprogramm.

Wir testen regelmäßig auch Anwendungen, die von der Abteilung Standardsoftware erstellt wurden. Für diese Aufgabe setzen wir verschiedene Tools ein, um z.B. mögliche Schwachstellen für ein Buffer Overflow zu finden.

Q: Wie funktioniert die Installation von Sicherheitsupdates?

Die Installation von Sicherheitspatches wird zentral gesteuert mit diversen Skripts. Alle Geräte außer PDAs installieren die Updates automatisch und starten neu, falls ein Neustart nach der Installation erforderlich ist.

Q: Warum erfolgt die Installation von Updates bei PDAs nicht automatisch?

Die Installation von Updates im mobilen Geräte gestaltet sich als ziemlich schwierig. Wir haben verschiedenste Geräte mit unterschiedlichen OS wie z.B. WM6, Blackberry oder Symbian im Einsatz. Außerdem gibt’s es nicht so oft Updates für mobile Geräte. Um die mobile Geräte zu schützen, setzen wir Sicherheitstools von führende Mobile Security Hersteller ein, damit sie nicht von Malware infiziert werden.

A.7. Interview mit Servicecenter

Q: Was ist die wichtigste Aufgabe des IT Servicecenters?

Das IT Servicecenter hat sehr viele verschiedene Aufgaben zu bewältigen. Die wichtige Aufgabe ist jedoch das sogenannte First Level Service. Die Mitarbeiter des Servicecenters stehen den Mitarbeitern des Unternehmens zur Verfügung und beantworten diverse Fragen. Bei Spezialfragen werden sie an das zuständige Fachpersonal weitergeleitet. Falls das Problem

nicht sofort gelöst werden kann, wird ein Trouble Ticket eröffnet und an die zuständige Mitarbeiter des Servicecenters weitergeleitet.

Q: Welche Aufgaben hat das IT Servicecenter noch?

Neben den First Level Service hat das IT Servicecenter noch viele Aufgaben. Das IT Servicecenter ist für die administrativen Aufgaben wie die Warenannahme (für IT Abteilung) und -ausgabe (z.B. Notebook für Mitarbeiter) zuständig. Eine weitere Aufgabe des Servicecenters ist die Vergabe oder die Änderung der Benutzerdaten. Die Mitarbeiter des Unternehmens können das Passwort gegen die Vorlage des Mitarbeiterausweises ändern lassen, falls das alte Passwort vergessen wurde.

Q: Wie ist das Arbeitsleben im Servicecenter?

Nach meiner Meinung hat das IT Servicecenter eine der schwierigsten Aufgabe in der IT Organisation. Das Servicecenter ist der „IT Kommunikationspartner" der Mitarbeiter des Unternehmens. Viele Mitarbeiter rufen uns an, sind frustriert, weil etwas nicht geht. Der Umgangston ist manchmal auch nicht sehr höflich. Neben dem fachlichen Wissen müssen wir auch noch Geduld und Höflichkeit aufbringen. Es gibt aber auch sehr lustige Fälle, die man nicht ganz schnell wieder vergisst.

Q: Lustige Fälle?

Ja lustig! Aber das hängt von der Betrachtungsweise ab. Für uns ist sowas selbstverständlich, jedoch für manche Mitarbeiter, die nicht so gut mit dem Computer umgehen können, ist das ein Horror. Ich erzähle Ihnen hier ein Beispiel:

Ein ranghoher Mitarbeiter im Außerdienst ruft uns an und meint, dass das WLAN seines Laptops nicht mehr funktioniert. Er kann nicht mehr auf das Funknetzwerk im Unternehmen zugreifen. Er möchte den Laptop bei uns vorbeibringen und anschließend ein neuen Laptop holen. Daraufhin hat unser Mitarbeiter einfach höflich angefragt, ob der kleine Schalter für WLAN an der rechten Seite des Geräts in der Position „ON" befindet. Er antwortet darauf hin: „Gibt's sowas?". Das WLAN hat nicht funktioniert, weil die Schalter versehentlich auf OFF geschaltet wurden.

Ein anderes Beispiel: Eine Mitarbeiterin ruft von zuhause an und fragt warum seine XDSL Leitung nicht geht. Kein weiterer Kommentar dazu.

Q: Wie sehen sie die Zukunft des IT Servicecenters?

Wir sind dabei, weitere Prozessoptimierung durchzuführen, sodass die Abläufe mehr automatisiert werden können. Ein Beispiel: Ein neuer Mitarbeiter bekommt automatisch alle notwendigen Konten angelegt, nachdem er in die Personaldatenbank eingetragen wurde. Zurzeit müssen die Accounts manuell vergeben werden und es erleichtert uns die Arbeit wenn alles automatisiert ablaufen kann.

Neben der Prozessoptimierung soll die Kommunikation verstärkt werden. Es ist nötig, die Mitarbeiter mehr aufzuklären, um sie gegen diverse Angriffe wie z.B. Social Engineering zu schützen

A.8. Interview Abteilung Network Access und Hardware

Q: Beschreiben Sie die Aufgabe der Abteilung

Der Name unserer Abteilung sagt bereits vieles über die wichtigsten Aufgaben aus. Die Abteilung ist zuständig für die eingesetzte Hardware des Unternehmens. Neben der Abwicklung der Beschaffung bzw. der Reparatur der Hardware planen wir noch die Hardwarestruktur des Unternehmens. Eine weitere wichtige Aufgabe ist die Verwaltung des Netzwerkes, dazu gehört etwa die Anbindung des Unternehmens ans Internet und Network Access Control der Workstations.

Q: Wie ist die Netzwerk des Unternehmen im allgemein aufgebaut?

Die Endgeräte (PC und Laptops) sind mit WLAN oder Netzwerkkabel mit dem Switch der Abteilung verbunden. Je nach Größe kann eine Abteilung mehrere Switches besitzen. Diese Switches werden zu den Endpunkten des Stockwerkes verbunden. Sie werden mit dem zentralen Switch in unseren Serverraum angeschlossen und ins Internet weitergeleitet.

Q: Wie funktioniert Network Access Control im Unternehmen?

Im Bereich Network Access Control arbeiten wir mit einer der führenden Firma im Bereich Sicherheit zusammen, die auch die notwendige Software liefert. Wenn ein Computer versucht eine Verbindung zum Netzwerk herzustellen, wird zunächst überprüft, ob der Computer bekannt ist. Falls der Computer unbekannt ist, landet er gleich in Quarantäne. Falls der

Computer bekannt ist, wird er anhand von diversen Richtlinien überprüft. Falls der Computer die Richtlinienüberprüfung bestanden hat, wird der Zugriff auf Unternehmensnetzwerk gewährt. Andernfalls landet der Computer wie ein unbekannter PC in Quarantäne.

Q: Wie ist die Firma ans Internet gebunden?

Zurzeit sind wir mit einer 50 MBit Leitung angebunden. Die Leitung stößt jedoch bald an ihre Grenzen und wir werden demnächst ein Upgrade auf 100 MBit durchführen.

Q: Wie sind sie gegen einen Ausfall der Internetleitung geschützt?

In der Firmenzentrale laufen alle E-Commerce Anwendungen des Unternehmens. Daher verursacht ein Ausfall der Internetanbindung sehr große Unannehmlichkeiten. Um die Wahrscheinlichkeit eines Totalausfalles zu minimieren, besitzen wir eine Backup SDSL Leitung mit 32 MBit Geschwindigkeit. D.h. wir haben eine komplette redundante Anbindung vom Router zu den nationalen Knotenpunkten des Internets. Unser Router ist so konfiguriert, dass ein Wechsel zur Backup Leitung automatisch und reibungslos im Hintergrund durchführt. Wenn die Hauptleitung ausfällt, wird der IP Traffic automatisch durch dynamische Routingprotokolle auf die Backupleitung umgeroutet.

Neben der Absicherung mit einer Backupleitung haben wir auch mit unserem Access Anbieter einen SLA abgeschlossen. Im SLA wurden eine Reaktionszeit von 1 Stunde und eine Wiederherstellungsdauer der Internetanbindung innerhalb von 3 Stunden vereinbart.

Q: Wie schaut die Beschaffung von Hardware aus?

Wir kaufen schon seit einiger Zeit keine Hardware mehr. Wir leasen sie. Das Leasing von Hardware hat sehr viele Vorteile. Neben den finanziellen Vorteilen des Leasings (Liquidität, ausgeglichene Bilanz des Leasings, Entsorgung der Geräte u.a.) können die vorhandenen Workstations schneller ausgetauscht werden.

A.9. Interview mit Abteilung Standardsoftware

Q: Beschreiben Sie die Aufgaben der Abteilung.

Die Abteilung Standardsoftware berät Abteilungen bei der Auswahl und dem Einsatz von spezieller Software. Wenn eine Abteilung der Firma eine Software Sonderlösung benötigt,

führen wir eine genaue Anforderungsanalyse durch und helfen bei der Beschaffung und Integration in die Workstations.

Neben der Beratung im Bereich Software sind wir auch für die Weiterentwicklung von derzeitigen E-Commerce Lösungen des Unternehmens und die Weiterentwicklung des unternehmensinternen Verwaltungsprogramms zuständig.

Q: Beschreiben sie die „unternehmensinternen Verwaltungsprogramm“ genauer.

Wir haben eine webbasierte ERP-Anwendung selbst entwickelt, um die Geschäftsprozesse des Unternehmens in den Bereichen wie z.B. Beschaffung, Verkauf, Marketing oder Buchhaltung aktiv zu unterstützen. Die Anwendung ist auf einem Server im Intranet installiert und wird direkt von uns betreut.

Q: Warum gibt es keine eigene Entwicklungsabteilung für diese Anwendungen?

Zurzeit sehe ich noch keinen Bedarf, die Softwareentwicklung in eine eigene Abteilung auszugliedern. Jedoch beschäftigt die Abteilung Standardsoftware bereits fast die Hälfte der Angestellten in der IT. Wenn die Firma wie erwartet gute Software weiter entwickelt, werden wir mehr Programmierer benötigen und dann über eine Ausgliederung nachdenken.

A.10. Interview Abteilung Systemadministration

Q: Beschreiben Sie die Aufgaben der Abteilung.

Die Abteilung administriert die sogenannten „Zentrale Services“ der Firma. Wir sorgen dafür, dass diese Services sowie deren Backupsysteme einwandfrei laufen. Falls eine Störung auftaucht, soll der Downtime so gering wie möglich gehalten werden.

Q: Was sind die „Zentrale Services“?

Die zentralen Services sind z.B. WWW, FTP oder E-Mail Dienste. Die wichtigen Dienste haben einen sogenannten „Service Manager“. Der Service Manager kümmert sich ausschließlich um seine zugewiesenen Services.

Es gibt jedoch einen Service, der nicht in unsere Zuständigkeit fällt. Es gibt eine eigene Abteilung für die Datenbankservices. Diese Abteilung wurde vor ca. einem Jahr ausgegliedert und hat nur Datenbankspezialisten.

Q: Wie werden die Services überwacht?

Wir verwenden die Software Nagios, um die zentralen Services zu überwachen. Es werden verschiedene Parameter wie Service-Verfügbarkeit, Festplattenspeicher, Speicher- und CPU Auslastung und viele andere überwacht. Falls ein Service nicht erreichbar ist bzw. ein Parameter einen kritischen Wert überschritten hat, alarmiert das Programm den zuständigen Servicemanager über E-Mail und SMS.

Q: Welche Aufgabe hat der FTP Service?

Im FTP-Service liegen die verschiedensten Aufgabebereiche wie beispielsweise das Backup bis hin zur Übermittlung der Produktdaten. Wir stellen einfach viel Speicherplatz zur Verfügung und die Abteilungen können sie zum Beispiel. zum Austausch von Daten nutzen. Ein anonymes Login ist selbstverständlich nicht gestattet. Jede Abteilung hat ihr eigenes Verzeichnis und kann die Rechte selbst gestalten.

Q: Gibt es öfter Attacke auf den FTP Service?

Ja es gibt sehr oft Attacken auf unseren FTP Service. Es wird öfters, durch die Anwendung eines Exploits oder über Bruteforce Attacke versucht, Zugang zum FTP zu gelangen. Wir haben jedoch Security Teams, die das Firmennetzwerk überwachen und die Software patchen, falls eine Sicherheitslücke erkannt wurde.

Q: Beschreiben sie den Mail Service.

Das E-Mail Service kann man wohl als eines der wichtigsten Kommunikationsdienste der Firma bezeichnen. Wir bieten neben dem Versand und Empfand auch einige Zusatzdienste wie z.B. einen Webmail Client.

Q: Wie schaut die Spam Statistik aus?

Wir verwenden Spamassassin und Amavis zur Filterung von Spams. Der Mailserver verarbeitet ca. 10.000 E-Mails pro Tag. 70% der E-Mails werden als Spam erkannt. 20 % der E-Mails als möglicher Spam. Nur ca. 10% der E-Mails werden als clean markiert.

Q: Warum verwenden Sie Greylisting nicht?

Greylisting kann so gut gegen die Spambekämpfung sein, aber im Business Bereich finde ich diese Methode nicht geeignet. In manchen Situationen ist es erforderlich, dass eine E-Mail vom Kunden so schnell wie möglich bei uns einlangt. Greylisting verzögert jedoch die Zustellung der E-Mails. Natürlich kann man das Problem durch Whitelist lösen. Aber man kann wirklich nicht alle Kunden darin eintragen, denn sonst hat Greylisting keinen Sinn mehr.

Q: Wie ist das Mail System gegen Ausfall gesichert?

Ganz einfach: Beim Ausfall des primären Mailservers wird der Mailverkehr über den Backupserver abgewickelt. Der Backupserver ist jedoch nicht so leistungsfähig wie Hauptserver und man muss mit längeren Zustellzeiten rechnen.

Q: Gibt es öfters Angriffsversuche auf den Mail Service?

Ja es gibt sehr oft Angriffsversuche auf den Mail Service. Es gibt sehr oft Relay-Versuche auf unserem Server. Diese Angriffe sind jedoch harmlos und man kann sie eigentlich nur als ein „Rauschen“ im Internet bezeichnen.

Es gibt natürlich auch ernste Zwischenfälle. Dies ist jedoch auf eine unsichere Auswahl von Passwörtern zurückzuführen. Ein Konto eines Mitarbeiters wurde gecrackt wegen eines unsicheren Passworts. Dadurch wurde der Server zur Spamschleuder. Dank der Überwachung des Systems haben wir das ganz schnell erkennen können und ein Eintrag in der RBL Liste wurde verhindert.

Q: Welche Seite liegen auf den Webservern?

Von Internet aus sind nur die Homepage und die Seiten der E-Commerce Anwendungen erreichbar. Vom Intranet aus sind noch andere Webanwendungen wie z.B. die Mitarbeiterseite erreichbar. Falls ein Mitarbeiter die unternehmensinterne Webseite aufrufen möchte, muss er sich mittels VPN im firmeninternen Netzwerk anmelden und kann dann darauf zugreifen.

Q: Gibt es oft Angriffe auf Webserver?

Es gibt täglich viele Scanversuche auf unsere Webserver bzw. die Applikationen der Webserver. Aufgrund der hervorragenden Zusammenarbeit mit den Security Teams gibt es zurzeit noch keine ernsten Zwischenfälle.

Q: Wie schaut die Backup Strategie aus?

Wir betreiben auch Data Storages mit mehreren Terabyte Speicher. Die Data Storages sind natürlich mit dem neusten Stand der Technik ausgestattet, um einen Datenverlust zu vermeiden. Das Backup wird per Skript gesteuert und das Intervall ist abhängig von der Wichtigkeit der Daten. Die wichtigsten Daten werden täglich gespeichert. Die „weniger“ wichtigen Daten werden meistens nur zweimal pro Woche gesichert.

A.11. Aufbau der IT Organisation

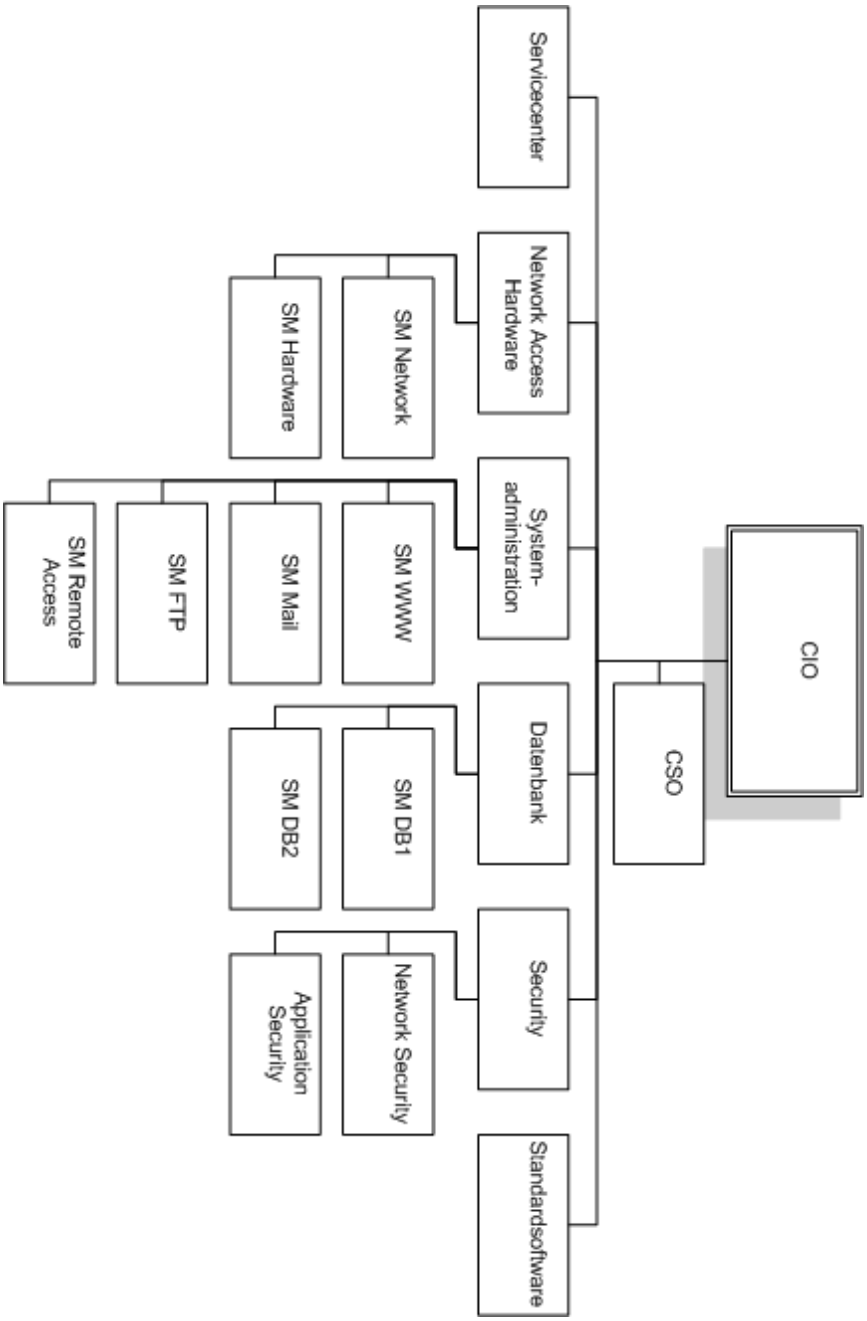


Abbildung 52: Business Case – IT-Struktur (organisatorischer Sicht)

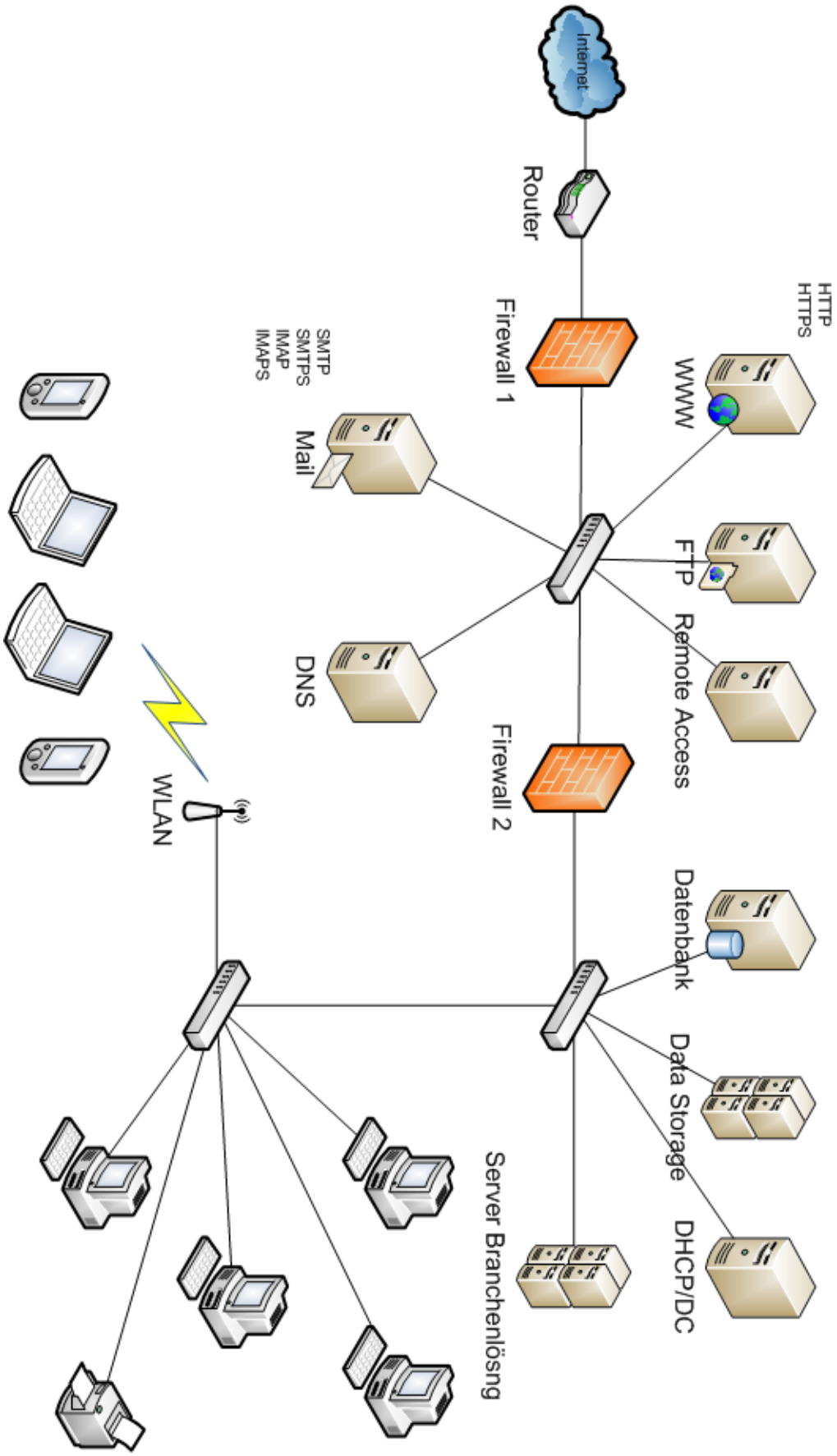


Abbildung 53: Business Case – IT-Struktur

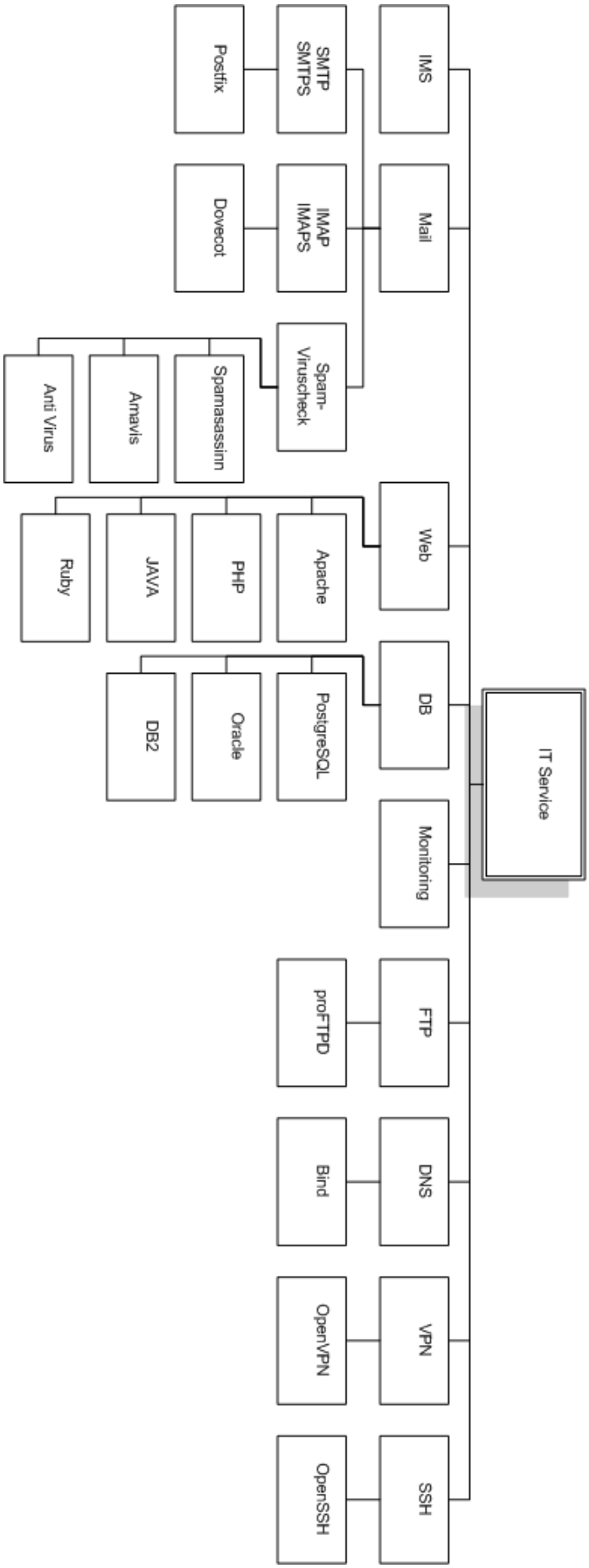


Abbildung 54: Business Case – IT-Services

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Ahrendts, Fabian und Marton, Anita. 2008. *IT-Risikomanagement leben!* Berlin : Springer, 2008. ISSN 1439-5428.

Blakley, Bob, McDermott, Ellen und Geer, Dan. 2001. Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms.* New York : ACM, 2001.

Brunnstein, Jochen. 2006. *ITIL Security Management realisieren.* Wiesbaden : Vieweg & Sohn Verlag, 2006. ISBN-10 3-8348-0165-8.

BSI. 2008. *BSI Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz.* [PDF Dokument] Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2008. Version 2.5.

—. 2007. *IT-Grundschutz-Kataloge.* [PDF Dokument] Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2007. 9. Ergänzungslieferung.

—. 2008. *Webkurs GSTOOL.* [PDF Dokument] 2008. http://bsi.bund.de.

—. 2006. *Webkurs IT-Grundschutz - Druckversion.* [PDF Dokument] Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2006. http://www.bsi.bund.de.

Buchstein, Ralf, et al. 2007. *IT-Management mit ITIL® V3.* Wiesbaden : Viewg & Sohn Verlag, 2007. ISBN 978-3-8348-0270-5.

Bundeskanzleramt Österreich. 2007. *Österreichisches Informationssicherheitshandbuch.* [PDF Dokument] 2007. Version 2.3.

Chavez-Demoulin, V. und Embrechts, P. 2004. *Advanced Extremal Models for Operational Risk.* [PDF Dokument] Zürich : Department of Mathematics - ETH Zentrum, 2004.

DCSSI. 2004. *EBIOS - Abschnitt 1 - Einführung.* [PDF Dokument] Paris : DCSSI, 2004. http://www.ssi.gouv.fr.

—. 2004. *EBIOS - Abschnitt 2 - Methoden.* [PDF Dokument] Paris : DCSSI, 2004. http://www.ssi.gouv.fr.

—. 2004. *EBIOS - Abschnitt 3 - Techniken.* [PDF Dokument] Paris : DCSSI, 2004. http://www.ssi.gouv.fr.

DIN Deutsches Institut für Normung e.V. 2005. *ISO/IEC 17999:2005 - Leitfaden für das Informationssicherheits-Management.* Berlin : Beuth Verlag GmbH, 2005.

—. 2005. *ISO/IEC 27001:2005 - Informationssicherheits-Managementsysteme - Anforderungen.* Berlin : Beuch Verlag GmbH, 2005.

Erben, Roland F. und Romeike, Frank. *Risk-Management-Informationssysteme – Potentiale einer umfassenden IT-Unterstützung des Risk Managements.* [PDF Dokument]

Gaulke, Marks. 2006. CobiT als IT-Governance-Leitfaden. *HMD - Praxis der Wirtschaftsinformatik.* 2006, Heft 250.

Gleißner, Werner und Romeike, Frank. 2005. Anforderungen an die Softwareunterstützung für das Risikomanagement. *Zeitschrift für Controlling & Management.* 2005, 2.

Goltsche, Wolfang. 2006. *COBIT kompakt und verständlich.* Wiesbaden : GWV Fachverlage GmbH, 2006. ISBN-10 3-8348-0141-0.

Grob, Heinz Lothar, Strauch, Gereon und Buddendick, Christian. 2008. Applications for IT-Risk Management – Requirements and Practical Evaluation. *ARES 2008 - Third International Conference on Availability, Reliability and Security - Proceedings.* Los Alamitos : IEEE Computer Society, 2008.

Hödebeck, Heimrich. 2002. IT-Risk-Management: Nie war IT-Sicherheit so wichtig wie heute. *Geldinstitute.* 2002, 6.

Holdenried, Hans-Ulrich. 2008. IT-Sicherheit schafft Mehrwerte. *Die Sparkassen Zeitung.* 2008, Nr. 07.

HULOCON GmbH. 2007. *Rimanis Benutzerhandbuch.* [PDF Dokument] 2007. Programm-Version 1.3.

—. *Rimanis Software.* [HTML Seite] http://www.hulocon.de.

IT-Governance Institute. 2006. *CobiT 4.0 - Deutsche Ausgabe.* [PDF Dokument] 2006.

Jones, Andy und Ashenden, Debi. 2005. *Risk management for computer security.* Burlington : Elsevier, 2005. ISBN 0-7506-7795-3.

Junginger, Markus und Krcmar, Helmut. 2004. Risiken im Informationsmanagement : Implementierungsstand und Herausforderungen des IT-Risk Managements in deutschen Unternehmen. *IM Die Fachzeitschrift für Information Management & Consulting.* 2004, Nr. 3.

Klemen, Marks und Biffl, Stefan. 2004. Economic Aspects and Needs in IT-Security Risk Management for SMEs. Stevenage : ICSE Conference Series, 2004. ISBN 0-86341-424-9.

Königs, Hans-Peter. 2006. *IT-Risiko-Management mit System.* Wiesbaden : Vieweg Verlag, 2006. ISBN-10 3-8348-0256-5.

Krcmar, Helmut und Jahner, Stefanie. 2005. Risikokultur als zentraler Erfolgsfaktor für ein ganzheitliches IT-Risk Management. *Information Management & Consulting.* 2005, Heft 2.

Löbl, Claudia. 2008. *Umfassendes Risikomanagement.* [PDF Dokument] 2008.

Müller, Klaus-Rainer. 2008. *IT-Sicherheit mit System.* Wiesbaden : Vieweg & Sohn Verlag, 2008. ISBN 978-3-8348-0368-9.

National Institute of Standards and Technology. 2008. *Managing Risk from Information Systems.* [PDF Dokument] 2008. NIST Special Publication 800-39 - Second Public Draft.

—. 2002. *Risk Management Guide for Information Technology Systems.* [PDF Dokument] 2002. Special Publication 800-30.

O'Mahony, Declan. 2005. IT-Risk-Management - nicht nur eine Aufgabe der IT-Abteilung. *IM Information Management & Consulting.* 2005, Heft 2.

Oberschmidt, Bernhard. 2005. Risiko IT. *IM Information Management & Consulting.* 2005, Heft 2.

Olbrich, Alfred. 2008. *ITIL kompakt und verständlich.* Wiesbaden : Vieweg+Teubner Verlag, 2008. ISBN 978-3-8348-0492-1.

Rauschen, Thomas und Disterer, Georg. 2004. Identifikation und Analyse von Risiken im IT-Bereich. *HMD - Praxis der Wirtschaftsinformatik.* 2004, Heft 236.

Romeike, Frank und Finke, Robert. 2003. *Erfolgsfaktor Risiko-Management.* Wiesbaden : Gabler Verlag, 2003. ISBN-10 3409122001.

Romeike, Frank und Gleißner, Werner. 2005. *Risikomanagement - Umsetzung, Werkzeuge, Riskobewertung.* München : Rudolf Haufe Verlag, 2005. ISBN 3-48-06209-X.

Salewski, Frank. 2002. IT-Risikomanagement mit CobiT. *IM Die Fachzeitschrift für Information Management & Consulting.* 2002, Nr. 1.

Seibold, Holger. 2005. *IT-Risikomanagement.* München : Oldenbourg GmbH, 2005. ISBN 3-486-58009-4.

Sørstrøm, Lars und Servatius, Hans-Gerd. 2005. IT-Unterstützung des Risikomanagements aus. *IM Information Management & Consulting.* 2005, Heft 4.

Steger, Udo. 2007. Rechtliche Verpflichtungen zur Notfallplanung im IT-Bereich. *CR - Computer und Recht.* 2007, Ausgabe März.

Symantec Corporation. 2008. *Symantec IT Risk Management Report - Volume 2.* 2008.

Symantec Deutschland GmbH. 2008. *IT-Risikomanagement umfasst mehr als Sicherheit.* [Online] 31. 01 2008. http://www.symantec.com/content/de/de/about/downloads/press/619risk.pdf.

Teubner, Rolf Alexander und Terwey, Jan. 2005. IT-Risikomanagement im Spiegel aktueller Normen und Standards. *HMD - Praxis der Wirtschaftsinformatik.* 2005, Heft 244.

Thiel, Cristoph. 2004. Ein Reifegradmodell für das IT-Sicherheitsmanagement. *HMD - Praxis der Wirtschaftsinformatik.* 2004, Heft 236.

Wildhaber, Bruno und Hill, Peter. 2003. IT-Governance – die IT in die Pflicht genommen. *Der Schweizer Treuhänder.* 2003, Heft 9.

Witt, Bernhard C. 2006. *IT-Sicherheit kompakt und verständlich.* Wiesbaden : Friedr. Vieweg & Sohn Verlag, 2006. ISBN 978-3-8348-0410-1.