



universität
wien

MASTERARBEIT

Titel der Masterarbeit

IT-Risikoanalyse für kleine und mittlere
Unternehmen

Verfasser

Robert Kopka, BSc

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl. Ing.)

Wien, 2010

Studienkennzahl lt. Studienblatt:

A 066 926

Studienrichtung lt. Studienblatt:

Wirtschaftsinformatik

Betreuer:

Uni.-Prof. DDr. Gerald Quirchmayr

Inhaltsverzeichnis

Abbildungsverzeichnis	4
1 Einleitung	6
1.1 Aufgabenstellung und Zielsetzung.....	7
2 Risiko.....	7
2.1 Risiken in der Informationstechnologie.....	7
2.2 Risikoanalyse und Risikomanagement	10
2.3 Quantitative und qualitative Ansätze der Risikoanalyse.....	12
2.4 Make-or-buy	14
3 Kleine und mittlere Unternehmen	15
3.1 Einsatz von Informationstechnologie in Klein- und Mittelbetrieben	20
3.2 Anforderungen an eine Risikoanalyse aus Sicht von KMU	21
4 Datenschutzgesetz	21
5 Existierende Ansätze der Risikoanalyse	24
5.1 Österreichisches Informationssicherheitshandbuch	24
5.2 ISO/IEC 27005	27
5.2.1 ISO 27001.....	27
5.2.2 ISO 27002.....	28
5.2.3 ISO 27005.....	28
5.3 IT-Grundschutz.....	37
5.3.1 Vorgehensweise.....	38
5.3.2 Beispiel.....	40
5.4 Mehari.....	42
5.4.1 Bewertung der natürlichen Gefährdung.....	45
5.4.2 Bewertung der tatsächlichen Auswirkungen	46
5.4.3 Risikomindernde Faktoren	47
5.5 OCTAVE SM	51
5.5.1 Phase 1 - Erstellung der Gefahrenprofile.....	52
5.5.2 Phase 2 - Schwachstellenanalyse.....	55
5.5.3 Phase 3 - Sicherheitsstrategieplan	55
5.6 NIST SP800-30.....	56
5.6.1 Risikobewertung.....	57
5.6.2 System Characterization.....	59
5.6.3 Threat Identification	59
5.6.4 Vulnerability Identification	60
5.6.5 Control Analysis.....	60

5.6.6	Likelihood Determination	61
5.6.7	Impact Analysis	61
5.6.8	Risk Determination.....	61
5.6.9	Control Recommendations	62
5.6.10	Results Documentation	62
5.7	Vergleich der Ansätze.....	62
6	Schlussfolgerungen und Empfehlungen für KMU	67
7	Risikoanalyse für kleine Unternehmen.....	69
7.1	Theoretische Grundlagen der Methode.....	70
7.2	Die Methode im Überblick	72
7.2.1	Unternehmen	72
7.2.2	Gefahren	72
7.2.3	IT-Infrastruktur.....	73
7.2.4	Datenschutz	75
7.2.5	Sicherheitsvorkehrungen	77
7.3	Auswertung.....	79
7.3.1	Bewertung der Gefährdungslage	80
7.3.2	Unternehmen	84
7.3.3	Gefahren	84
7.3.4	IT-Infrastruktur.....	85
7.3.5	Datenschutz	89
7.3.6	Sicherheitsvorkehrungen	89
7.4	Erweiterung der Methode	96
7.5	Beispielfirmen.....	98
7.5.1	Beispiel Einpersonnenunternehmen (EPU)	98
7.5.2	Beispiel Kleinstunternehmen.....	107
8	Zusammenfassung und Ausblick.....	115
	Abkürzungen.....	116
	Literaturverzeichnis.....	117
	Anhang I – Abstract	123
	Anhang II – Kurzfassung	124
	Anhang III – Lebenslauf	125

Abbildungsverzeichnis

ABBILDUNG 1 ZUSAMMENHANG ZWISCHEN RISIKOANALYSE UND RISIKOMANAGEMENT	11
ABBILDUNG 2 SCHWELLENWERTE ZUR EINTEILUNG DER UNTERNEHMEN.....	17
ABBILDUNG 3 UNTERNEHMENSSTRUKTUR IN ÖSTERREICH BEZOGEN AUF DIE ANZAHL DER MITARBEITER IM JÄNNER 2008	18
ABBILDUNG 4 KORRELATION DER ANZAHL DER MITARBEITER ZUR ZUGEHÖRIGKEIT EINES UNTERNEHMENS ZUM PRIMÄREN, SEKUNDÄREN BZW. TERTIÄREN WIRTSCHAFTSSEKTOR	19
ABBILDUNG 5 INFORMATION SECURITY RISK MANAGEMENT PROCESS	29
ABBILDUNG 6 SCHRITTE DER RISIKOIDENTIFIZIERUNG UND DER RISIKOABSCHÄTZUNG.....	31
ABBILDUNG 7 ABLAUF DER GRUNDSCHUTZANALYSE	39
ABBILDUNG 8 TYPISCHE GEFÄHRDUNGEN FÜR MOBILE DATENTRÄGER	41
ABBILDUNG 9 MANIPULATION/ ZERSTÖRUNG VON IT-GERÄTEN ODER ZUBEHÖR.....	42
ABBILDUNG 10 BESTANDTEILE DER MEHARI WISSENSDATENBANK	43
ABBILDUNG 11 RISIKOANALYSEPROZESS UND UNTERSTÜTZUNG DURCH MEHARI	45
ABBILDUNG 12 STANDARDGEFÄHRDUNGSTABELLE	46
ABBILDUNG 13 TABELLE DER IMMANENTEN AUSWIRKUNGEN.....	47
ABBILDUNG 14 BEWERTUNGSRASTER FÜR STATUS-RI	49
ABBILDUNG 15 BEWERTUNGSRASTER ZU STATUS-P FÜR SZENARIEN.....	50
ABBILDUNG 16 PROZESSE UND AKTIVITÄTEN DER PHASE 1	52
ABBILDUNG 17 ARBEITSBLATT FÜR DIE AKTIVITÄT "ESTABLISH IMPACT EVALUATION CRITERIA"	53
ABBILDUNG 18 GEFAHRENPROFIL FÜR DAS PATIENTENINFORMATIONSSYSTEM (PIDS) BEI ZUGRIFF ÜBER DAS NETZWERK	54
ABBILDUNG 19 PROZESSE UND AKTIVITÄTEN VON PHASE 2	55
ABBILDUNG 20 PROZESSE UND AKTIVITÄTEN VON PHASE 3	56
ABBILDUNG 21 SOFTWARE DEVELOPMENT LIFE CYCLE.....	57
ABBILDUNG 22 RISK ASSESSMENT METHODOLOGY FLOWCHART	58
ABBILDUNG 23 RISIKOLEVEL MATRIX	62
ABBILDUNG 24 AUFBAU DER EXCEL DATEI	70
ABBILDUNG 25 HINZUFÜGEN EINER NEUEN GEFAHR.....	96
ABBILDUNG 26 KONFIGURATION DER AUSWAHLBOX „GEFAHREN“	96
ABBILDUNG 27 HINZUFÜGEN EINER NEUEN SICHERHEITSVORKEHRUNG	97
ABBILDUNG 28 KONFIGURATION DER AUSWAHLBOX "SICHERHEITSVORKEHRUNG"	97
ABBILDUNG 29 AUSWERTUNG INKLUSIVE NEU HINZUGEFÜGTER GEFAHR.....	98
ABBILDUNG 30 ANGABEN ZUM UNTERNEHMEN - EINPERSONENUNTERNEHMEN.....	99
ABBILDUNG 31 BEWERTUNG DER GEFAHREN - EINPERSONENUNTERNEHMEN	100
ABBILDUNG 32 ANGABEN ZUR IT-INFRASTRUKTUR - EINPERSONENUNTERNEHMEN	101
ABBILDUNG 33 ANGABEN ZUM DATENSCHUTZ - EINPERSONENUNTERNEHMEN	102
ABBILDUNG 34 VORHANDENE SICHERHEITSVORKEHRUNGEN -EINPERSONENUNTERNEHMEN	104
ABBILDUNG 35 AUSWERTUNG - EINPERSONENUNTERNEHMEN.....	106
ABBILDUNG 36 ANGABEN ZUM UNTERNEHMEN - KLEINSTUNTERNEHMEN	107
ABBILDUNG 37 BEWERTUNG DER GEFAHREN - KLEINSTUNTERNEHMEN.....	108
ABBILDUNG 38 ANGABEN ZUR IT-INFRASTRUKTUR - KLEINSTUNTERNEHMEN	109
ABBILDUNG 39 ANGABEN ZUM DATENSCHUTZ - KLEINSTUNTERNEHMEN.....	110
ABBILDUNG 40 VORHANDENE SICHERHEITSVORKEHRUNGEN - KLEINSTUNTERNEHMEN	112

ABBILDUNG 41 AUSWERTUNG - KLEINSTUNTERNEHMEN	114
--	-----

1 Einleitung

Der Erfolg und das Fortbestehen von Unternehmen hängen immer stärker von der verwendeten Informationstechnologie (IT) und den darauf gespeicherten Daten ab. Bei den Daten kann es sich um firmenspezifische Informationen, Forschungsergebnisse oder personenbezogene Daten handeln. Sie alle müssen vor unberechtigtem Zugriff, vor Veränderung und vor Zerstörung geschützt werden. Bei personenbezogenen Daten besteht dazu sogar ein rechtlicher Zwang (Bundesgesetz über den Schutz personenbezogener Daten - DSG 2000). Um Daten umfassend schützen zu können, ist es wichtig, die verwendeten Systeme ganzheitlich zu betrachten, das heißt, es müssen die Software, die Hardware und das Umfeld berücksichtigt werden. Gerade kleinen und mittleren Unternehmen (KMU) fehlen oft das Risikobewusstsein und die Ressourcen um eine vollständige Risikoanalyse der IT-Infrastruktur durchführen zu können. KMU entstehen oft aus innovativen Ideen mit sehr beschränkten finanziellen und personellen Mitteln. Dieser innovative Charakter führt oft zu einer ungeplanten und inkonsistenten IT-Landschaft. Fälschlicherweise sind viele Unternehmer der Meinung, dass ihr Unternehmen zu klein sei um für Kriminelle von Interesse zu sein. IT-Sicherheit bezieht sich aber nicht nur auf Kriminelle, sondern auch auf Naturkatastrophen, Missgeschicke und Unfälle. Wenn ein kleines Unternehmen seine Kundendaten auf einem Rechner speichert und die Festplatte dieses Rechners ausfällt, kann dies das Ende des Unternehmens bedeuten sofern kein Backup vorhanden ist. Das Image und die Vertrauenswürdigkeit von Unternehmen gewinnen immer mehr an Bedeutung und ein sicherheitsrelevanter Zwischenfall kann die Reputation eines Unternehmens auf lange Zeit beschädigen und dadurch zu finanziellen Einbußen führen.

Eine IT-Risikoanalyse dient der systematischen Identifizierung, Analyse und Bewertung der Risiken, welchen die IT-Infrastruktur eines Unternehmens ausgesetzt ist. Erst nachdem die Risiken bekannt und bewertet sind, können sinnvolle Gegenmaßnahmen, beispielsweise die Installation einer Firewall oder die Verwendung von Verschlüsselung, ergriffen werden. Die Risiken für IT-Systeme sind vielfältig und reichen von Erdbeben und Hochwassern über Bedienungsfehler der Mitarbeiter bis zu Spionage durch Konkurrenten und Regierungen. Eine Risikoanalyse ist ein komplexer Prozess, welcher viel Expertenwissen erfordert. Die Durchführung einer vollständigen Risikoanalyse benötigt oft Wochen bis Monate und ist meist mit großem bürokratischen Aufwand verbunden. Große Betriebe, die über die notwendigen finanziellen und personellen Mittel verfügen, können diese Art von Risikoanalyse durchführen. Um KMU bestmöglich zu schützen, müssen diese umfangreichen Ansätze auf ihre wichtigsten Bestandteile reduziert, der bürokratische Aufwand verringert und der zeitliche Aufwand dadurch auf wenige Tage beschränkt werden. All diese Einschränkungen dürfen die Effektivität der Analyse nur geringfügig negativ beeinflussen.

1.1 Aufgabenstellung und Zielsetzung

Diese Diplomarbeit soll vorhandene Ansätze der Risikoanalyse für IT-Systeme untersuchen und vergleichen. Die untersuchten Risikoanalysen sind:

- Österreichisches Informationssicherheitshandbuch
- ISO/IEC 27005
- IT-Grundschutz
- Mehari
- OCTAVE
- NIST SP800-30

Ziel der Diplomarbeit ist es, aufbauend auf den Ergebnissen des Vergleichs einen neuen Ansatz, welcher speziell auf die Bedürfnisse kleiner und mittlerer Unternehmen zugeschnitten ist, zu entwerfen. Dieser Ansatz soll sicherstellen, dass mit vertretbarem finanziellen und materiellen Aufwand die bedrohlichsten Risiken für das Unternehmen identifiziert und bewertet werden. Dabei wird von einer durchschnittlichen Gefährdung der Unternehmen ausgegangen. Besonders gefährdete Unternehmen sollten stets eine vollständige Analyse durchführen, auch wenn dies mit hohen Kosten verbunden ist.

2 Risiko

Das Wort Risiko wird im täglichen Sprachgebrauch und in den Medien häufig verwendet, die Herkunft des Wortes ist aber nicht restlos geklärt. [Kluge, 2002] hält einen Zusammenhang mit dem spanischen Wort „risco“, welches Klippe bedeutet, und mit dem früh-romanischen Wort „rixicare“, welches streiten bedeutet, für möglich. [Consequa, 2009] definiert Risiko als Funktion „der Wahrscheinlichkeit des Eintreffens einer gegebenen Bedrohung für ein Objekt unter Berücksichtigung der vorhandenen Verwundbarkeiten und Kontrollmechanismen“ und „dem nachfolgenden Schadenspotential falls die Bedrohung nicht abgewendet werden kann.“

Von einer Risikosituation spricht man im Allgemeinen dann, wenn der Entscheidungsträger „jedem denkbaren Umweltzustand eine (objektive oder subjektive) Eintrittswahrscheinlichkeit zuordnen“¹ kann. Eine Sicherheitssituation liegt vor, wenn für jede Alternative das Ergebnis bekannt ist. Bei einer Ungewissheitssituation kann der Entscheidungsträger lediglich angeben welche Zustände eintreten können, nicht jedoch deren Eintrittswahrscheinlichkeit².

2.1 Risiken in der Informationstechnologie

Jedes IT-System ist vielfältigen Risiken ausgesetzt. Es gibt elektronische Angriffe wie Viren und Spam, physische Angriffe wie Einbrüche und Diebstähle und soziale

¹ vgl. Dockner, 2007 S.29

² vgl. Dockner, 2008 S.29

Angriffe wie Social-Engineering und Phishing³. Ein Angriff kann entweder von einem Mitarbeiter oder einer betriebsfremden Person durchgeführt werden. [Verizon, 2008] und [Byres, 2004] zeigen, dass über 70% aller Angriffe von außerhalb des Unternehmens durchgeführt werden, die Angriffe von Mitarbeitern aber verheerendere Auswirkungen haben. Es gibt eine Vielzahl an Studien, die zu unterschiedlichen Prozentsätzen kommen. [Schneier, 2008] führt diese Unterschiede auf rein semantische Gründe zurück und verweist auf die schiere Anzahl von Angreifern außerhalb des Unternehmens verglichen mit der Anzahl der Mitarbeiter. Auch [Rothman, 2008] ist der Meinung, dass es unbedeutend sei, ob 27% oder 70% der Angriffe von Mitarbeitern ausgeführt werden. Wichtig sei, dass beide Arten von Angriffen bei der Risikoanalyse beachtet werden.

Doch nicht nur bösartige Angriffe sind ernst zu nehmende Bedrohungen für die IT-Landschaft eines Unternehmens, viel häufiger unterlaufen Mitarbeitern unbeabsichtigte Fehler während der Arbeit. Jedem Menschen passieren Fehler, es werden Dateien versehentlich gelöscht oder Kaffee wird über den Laptop geschüttet. Eine weitere Kategorie von Bedrohungen sind Naturkatastrophen wie Hochwasser oder Erdbeben und Probleme mit der Infrastruktur, zum Beispiel der Stromversorgung oder dem Internetanbieter. Eine Risikoanalyse sollte idealerweise alle Bedrohungen umfassen.

Um Schaden anrichten zu können, muss eine Schwachstelle im IT-System vorhanden sein und eine Bedrohung, welche diese Schwachstelle ausnutzt. Eine Schwachstelle kann ein schlechter Passwortmechanismus, ein Implementierungsfehler, mangelnder baulicher Schutz oder unzureichende Ausbildung der Mitarbeiter sein⁴.

[Avizienis et. al., 2004] definieren Sicherheit als das Vorhandensein von Verfügbarkeit, Vertraulichkeit und Integrität. Verfügbarkeit ist die Bereitschaft zum Ausführen eines Dienstes, wenn er benötigt wird; Vertraulichkeit bedeutet, dass Informationen nicht an unauthorisierte Personen weitergegeben werden und Integrität ist die Abwesenheit von missbräuchlichen Veränderungen⁵.

Im Folgenden werden einige reale Beispiele von sicherheitsrelevanten Zwischenfällen beschrieben um einen Überblick über die große Bandbreite möglicher Bedrohungen zu geben. In jedem Beispiel wurde zumindest eine der drei Sicherheitseigenschaften (Verfügbarkeit, Vertraulichkeit, Integrität) verletzt.

Immer wieder werden Laptops und Festplatten mit sensiblen Daten gestohlen. In England wurde zum Beispiel eine unverschlüsselte Festplatte mit sensiblen Daten von rund 500 Royal Air Force (RAF) Mitarbeitern gestohlen⁶. Diese Festplatte enthielt unter anderem Angaben zur Verschuldung und zu den sexuellen Vorlieben der Mitarbeiter. Diese Informationen könnten dazu verwendet werden, die betreffenden Personen zu erpressen und stellen eine ernst zu nehmende Gefahr für die Mitarbeiter und die RAF dar.

³ vgl. Mantl, 2007

⁴ vgl. BKA, 2007 Seite 42

⁵ vgl. Avizienis et.al., 2004 Seite 2

⁶ vgl. BBC, 2009

Ebenfalls in England wurde ein Laptop mit den Daten von zirka 43 000 Mitgliedern der Wigan School gestohlen⁷.

Die Deutsche Lufthansa konnte ihr online Anmeldesystem durch einen Fehler beim Einspielen eines Updates mehrere Stunden nicht nutzen, was zu Verspätungen auf etwa 200 Flughäfen weltweit führte⁸. Die Mitarbeiter der Fluglinie mussten Flugscheine händisch ausfüllen, wodurch es zu erheblichen Behinderungen und Verzögerungen kam. Dieser Zwischenfall hat dem Ansehen der größten europäischen Luftlinie geschadet und hohe Kosten verursacht.

Im Jahr 2008 wurde auf dem Flughafen Heathrow ein neuer Terminal eröffnet und schon am ersten Tag kam es zu weitreichenden Problemen bei der Gepäckannahme⁹. Die Ermittlungen ergaben, dass ein nicht entfernter Datenfilter, welcher für die Testphase verwendet wurde, und zu geringe Serverkapazitäten für den folgeschweren Zwischenfall verantwortlich waren. Der Chief Executive Officer (CEO) von British Airways, Willie Walsh, gab zu gewusst zu haben, dass das Programm nicht einwandfrei funktionierte, dieses Risiko aber wissentlich in Kauf genommen zu haben, weil eine Verzögerung der Eröffnung mit sehr hohen Kosten verbunden gewesen wäre. Außerdem konnte die Einschulung der Mitarbeiter nicht abgeschlossen werden, was dazu führte, dass 20% der Mitarbeiter nicht mit dem System vertraut waren. In diesem Fall wurde ein Restrisiko akzeptiert, aber anscheinend falsch eingeschätzt.

Aber auch technisch einwandfreie Systeme können angegriffen werden. Hacker haben über 10 000 Passwörter des E-Mail-Anbieters Hotmail auf einer Internetseite veröffentlicht¹⁰. Sie sind durch eine so genannte Phishing-Attacke an diese Passwörter gelangt. Bei Phishing-Angriffen werden Benutzer auf eine gefälschte Seite gelockt und aufgefordert, ihre E-Mail-Adresse und ihr Passwort einzugeben. Diese Informationen können von den Betrügern anschließend verwendet werden, um auf die E-Mailkonten der Betroffenen zuzugreifen. Diese Art des Angriffs kann bei Internetseiten von Banken besonders verheerend sein.

Die weltweite Vernetzung der Computersysteme hat dazu geführt, dass Angreifer von einem beliebigen Punkt auf der Erde Rechner weltweit angreifen können. Diesen Angriffen sind nicht nur Firmen, sondern auch Regierungen ausgeliefert. Im Jahr 2007 wurden nach einem diplomatischen Konflikt mit Russland, estnische Internetseiten mit Denial-of-Service (DoS) Angriffen lahm gelegt¹¹. Bei DoS-Angriffen werden mehr Anfragen simultan an einen Server geschickt als dieser zu beantworten in der Lage ist. Betroffen waren die Webseiten von Regierungsstellen, Banken, Firmen und Zeitungen. Es wird vermutet, dass die Angriffe aus Russland ausgeführt wurden.

Auch Stromversorger setzen mehr und mehr auf Computersysteme zur Steuerung ihrer Infrastruktur. In den Vereinigten Staaten von Amerika (USA) wurde auf diesen Rechnern Schadsoftware entdeckt, welche es ermöglichen könnte, die

⁷ vgl. ZDNet, 2009

⁸ vgl. FTD, 2009

⁹ vgl. IEEE Spectrum, 2008

¹⁰ vgl. BBC, 2009a

¹¹ vgl. Spiegel, 2007

Stromversorgung zu unterbrechen. Angeblich wurden diese Programme von Russland und China aus eingeschleust¹². Auch das US-amerikanische Verteidigungsministerium ist vor Hackern nicht sicher. Besonders peinlich ist, dass mehrere Terabyte des teuersten militärischen Kampfflugzeuges aller Zeiten, des F35 Lightning II, von Hackern entwendet wurden. Die Entwicklung des Flugzeuges soll 300 Milliarden US-Dollar kosten¹³. Die gestohlenen Informationen waren auf Rechnern von Zulieferfirmen gespeichert und wurden von dort an einen unbekannten Ort übertragen. Es wird vermutet, dass dieser unbekannte Ort irgendwo in China liegt. Beweise für diese Vermutung wurden jedoch nicht veröffentlicht.

2.2 Risikoanalyse und Risikomanagement

Die Risikoanalyse (engl. Risk Assessment) ist der erste Teil des Risikomanagements (engl. Risk Management Process). Die Risikoanalyse (RA) dient der Identifizierung, Analyse und Bewertung von Risiken. Sie wird zu bestimmten Zeitpunkten, zum Beispiel einmal jährlich, ausgeführt und ist anschließend für einen gewissen Zeitraum gültig. Eine Risikoanalyse sollte periodisch und bei jeder größeren Veränderung der verwendeten Hard- und/ oder Software vorgenommen werden. Das Risikomanagement (RM) hingegen ist ein kontinuierlicher Prozess, welcher sich neben der Risikoanalyse auch mit der Implementierung des Sicherheitskonzeptes, der Überwachung des Umsetzungsfortschritts und der Kontrolle möglicher Abweichungen beschäftigt¹⁴. Abbildung 1 zeigt den Zusammenhang zwischen Risikoanalyse und Risikomanagement grafisch. Ob die Planung noch Teil der Risikoanalyse ist oder nicht hängt vom betrachteten Ansatz ab¹⁵.

¹² vgl. Network Computing, 2009

¹³ vgl. Network Computing, 2009a

¹⁴ vgl. ENISA 2006

¹⁵ vgl. Alberts 2005

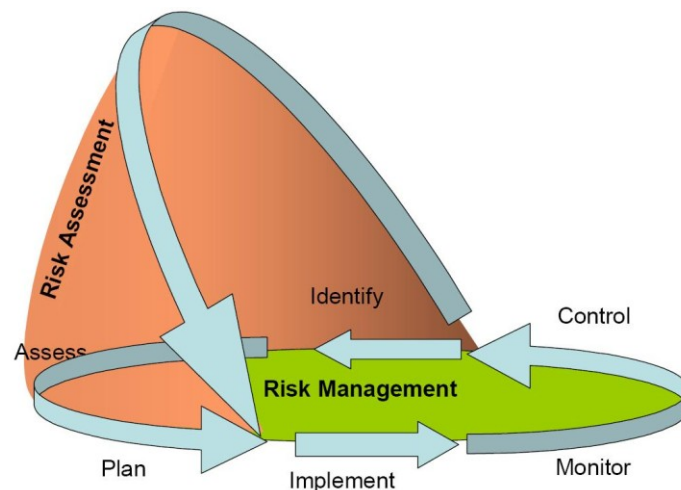


Abbildung 1 Zusammenhang zwischen Risikoanalyse und Risikomanagement¹⁶

Risikoanalysen werden in vielen Bereichen, wie zum Beispiel in der Betriebswirtschaftslehre und bei Banken und Versicherungen, eingesetzt. Ziel ist es, Risiken zu identifizieren und angemessene Gegenmaßnahmen zu entwickeln. Prinzipiell geht jeder Entscheidung in einer Risikosituation eine Risikoanalyse voraus. Jeder Mensch führt täglich (meist unbewusst) Risikoanalysen durch, dies beginnt bei der Entscheidung in ein öffentliches Verkehrsmittel zu steigen und endet beim genussvollen Verzehr von Sushi. Bei all diesen Entscheidungen wird auf Erfahrungen aus der Vergangenheit zurückgegriffen und darauf beruhend werden Annahmen über die Zukunft getroffen. Die Wahrnehmung von Gefahren kann durch verschiedene Faktoren wie Medienberichte und Erzählungen von Freunden beeinflusst werden. Statistisch gesehen ist es wahrscheinlicher von einer Kokosnuss erschlagen als von einem Hai gefressen zu werden¹⁷. Da blutrünstige Haifische aber eine bessere Schlagzeile abgeben als von der Schwerkraft angezogene Kokosnüsse, wird in den Medien darüber überproportional häufig berichtet, was die Wahrnehmung dieser Gefahr in der Öffentlichkeit verändert.

Auf Risiken kann unterschiedlich reagiert werden. Sie können akzeptiert, durch die Verwendung von Alternativen vermieden oder auf andere Parteien übertragen werden. Das Übertragen von Risiken auf andere Parteien ist das Kerngeschäft von Versicherungen.

Der in Abbildung 1 gezeigte Prozess der Risikoanalyse und des Risikomanagements liegt den meisten heute gebräuchlichen Ansätzen zugrunde, er wird jedoch um Branchen- oder Firmenspezifika erweitert bzw. an nationale Richtlinien angepasst. Der IT-Grundschutzkatalog des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) ist zum Beispiel eine Instanz des

¹⁶ vgl. ENISA, 2006 Seite 15

¹⁷ vgl. Welt 2002

allgemeinen Risikomanagements, welche an die nationalen Erfordernisse der Bundesrepublik Deutschland angepasst wurde. Dem Standard 27005 der International Organization of Standardization (ISO) unterliegt der gleiche Risikomanagementprozess, er ist jedoch auf einen weltweiten Einsatz ausgelegt und deshalb allgemeiner gehalten¹⁸.

Um ein Informationssicherheitskonzept erfolgreich in einem Unternehmen etablieren zu können, sind folgende Faktoren ausschlaggebend¹⁹:

- Hundertprozentige Unterstützung durch das Management
- Zentrale Organisation und einheitliche Richtlinien für das gesamte Unternehmen
- Die Sicherheitsrichtlinien müssen sich an den Bedürfnissen der Organisation orientieren
- Kontinuierliches Training und Einbeziehung der Mitarbeiter

2.3 Quantitative und qualitative Ansätze der Risikoanalyse

Grundsätzlich werden bei Risikoanalysen quantitative und qualitative Ansätze unterschieden. Quantitative Verfahren beruhen auf den mathematischen Modellen der Statistik und der Wahrscheinlichkeitsrechnung. Diese werden beispielsweise von Versicherungen eingesetzt um Versicherungsprämien zu berechnen. Voraussetzung für die quantitative Bewertung von Risiken ist ausreichendes Wissen über die Eingangsparameter und Zugriff auf aussagekräftige historische Daten. Waldbrände und Erdbeben sind Beispiele für Risiken, welche für bestimmte Regionen quantitativ relativ gut beziffert werden können, weil eine Vielzahl historischer Daten vorhanden ist. Schwieriger bzw. unmöglich ist die Quantifizierung von Risiken über die keine historischen Daten vorliegen oder Risiken, welche von neuen Technologien (Nanotechnologie, Genmanipulation) oder Entwicklungen (Klimawandel) ausgehen²⁰.

Die Vorteile quantitativer Modelle sind²¹:

- Ergebnisse beruhen auf objektiven mathematischen Modellen
- Durchführung einer Kosten-Nutzen-Analyse möglich
- Ergebnisse sind leicht verständlich (z. B. finanzieller Verlust pro Jahr)

Die Nachteile quantitativer Verfahren sind²²:

- Hoher Aufwand
- Komplexe Berechnungen
- Einschulungen sind sehr zeitaufwändig
- Out-of-Scope Aktivitäten können nur schwer berücksichtigt werden

¹⁸ vgl. ENISA, 2009

¹⁹ vgl. ENISA, 2009a

²⁰ vgl. Schaumann, 2008

²¹ vgl. Peltier, 2005 Seite 80

²² vgl. Peltier, 2005 Seite 80

Wenn quantitative Ansätze nicht angewendet werden können, wird oft auf qualitative Ansätze zurückgegriffen. Hierbei geht es weniger um die Vorwegnahme zukünftiger Ereignisse, sondern mehr darum, wie auf kostengünstige Art und Weise gegenwärtige Risiken in den Griff zu bekommen sind²³. Häufig werden bei diesem Verfahren Listen mit bekannten Risiken erstellt und ihre Eintrittswahrscheinlichkeit sowie die Auswirkungen subjektiv mit „gering“, „mittel“ und „hoch“ angegeben.

Die Vorteile sind²⁴:

- Einfache Berechnungen
- Monetäre Bewertung der Vermögensgegenstände ist nicht erforderlich
- Hohe Prozessflexibilität
- Nicht-Techniker und Nicht-Sicherheitsexperten können leicht einbezogen werden

Die Nachteile sind²⁵:

- Hohe Subjektivität
- Kosten-Nutzen-Analyse kann nur bedingt durchgeführt werden

Ein sehr aktuelles Thema, welches die Gefahren quantitativer Modelle bei Verwendung unzureichender historischer Daten zeigt, ist die gegenwärtige Finanzkrise, welche im Jahr 2007 begonnen hat. In den letzten Jahren wurden in den Vereinigten Staaten von Amerika viele private Kredite durch Hypotheken auf Grundstücke gesichert. Diese „Mortgage-Backed-Securities“ genannten Hypotheken wurden zu Pools von hunderten oder sogar tausenden Hypotheken zusammengefasst und Investoren angeboten. Das Ausfallrisiko dieser Anleihen wurde mithilfe der „Gaussian-Copula-Formel“²⁶ berechnet. Diese Formel gibt die Korrelation der in der Anleihe vorhandenen Hypotheken an. Mit dieser Korrelationszahl wurde auf das Ausfallrisiko rückgeschlossen. Bei schwacher Korrelation wurde das Ausfallrisiko als niedrig angenommen, weil die Wahrscheinlichkeit, dass viele Ausfälle zusammenfallen gering ist. Es war nun fast immer möglich, einer Anleihe ein Triple-A-rating (= höchste Kreditwürdigkeit) zu verleihen. Da diese Art von Hypotheken neu war und keine historischen Daten vorlagen, wurden die Preise des „Credit-Default-Swap“ (CDS) Marktes als Referenz verwendet. CDSs entsprechen einer Kreditversicherung; kann der Schuldner seine Raten nicht bezahlen, bekommt der Gläubiger eine Ausgleichszahlung²⁷. Diese quantitative Methode war aufgrund ihrer Einfachheit bei Investoren sehr beliebt. Das Sammeln historischer Daten war nicht erforderlich und eine einzige Zahl genügte, um das Ausfallrisiko eines Pools von hunderten Hypotheken zu berechnen. Diese irreführende Objektivität und ein Mangel an mathematischem Verständnis der Verantwortlichen haben ihren Teil zur derzeitigen Krise beigetragen. Problematisch an dieser Vorgangsweise war, dass es

²³ vgl. Schaumann, 2008

²⁴ vgl. Peltier, 2005 Seite 80

²⁵ vgl. Peltier, 2005 Seite 80

²⁶ vgl. Port, 2009

²⁷ vgl. InvW, 2009

CDSs erst seit einigen Jahren gab und das genau die Zeit war, in der die Grundstückspreise ständig gestiegen sind. Außerdem wurde die Korrelation als konstant angenommen, was jedoch nicht der Fall ist. Die Korrelation war zu dieser Zeit sehr gering, weil der Ausfall eines Schuldners keine Rückschlüsse auf die restlichen Hypotheken zuließ. Wenn eine Person arbeitslos wurde oder aufgrund persönlicher Probleme die Hypothek nicht zurückzahlen konnte, stellte das für den gesamten Pool noch kein Problem dar. Gefährlich wurde die Situation erst als die Grundstückspreise fielen. Dieser Effekt betraf sehr viele Hypothekenzahler zur gleichen Zeit, was zu einer hohen Korrelation und vielen Ausfällen führte²⁸. Tausende Investoren haben sich durch die Korrelationszahl zu unsicheren Investitionen verleiten lassen und sehr viel Geld verloren. Die „Gaussian-Copula-Formula“ hat als quantitatives Instrument zur Bewertung von Ausfallrisiken versagt.

Vergleicht man diese Situation nun mit der Informationstechnologie, muss man feststellen, dass auch hier historische Daten fehlen und quantitative Analysen für sehr seltene Phänomene nicht sinnvoll einsetzbar sind. Die Wahrscheinlichkeit eines Hacker-Angriffs oder einer Sabotage durch Mitarbeiter kann nicht genau genug bestimmt werden um quantitative Verfahren sinnvoll einsetzen zu können. Außerdem kommen durch den schnellen Wandel der Technologien ständig neue Gefahren zu den bereits bekannten. Um eine nicht zu rechtfertigende Objektivität zu vermeiden, werden im Folgenden nur qualitative Verfahren der Risikoanalyse diskutiert.

2.4 Make-or-buy

Jedes Unternehmen muss grundsätzlich entscheiden, ob es das Risikomanagement im Unternehmen durch eigene Mitarbeiter durchführen lassen möchte oder dieses auf Vertragspartner auslagert („make-or-buy“). Es gibt auch die Möglichkeit einer partiellen Auslagerung, das heißt, dass die erste Risikoanalyse von einer externen Firma in Zusammenarbeit mit eigenen Mitarbeitern durchgeführt wird, die Wartung aber ausschließlich intern stattfindet²⁹.

Die Vor- und Nachteile der drei Alternativen für ein Unternehmen sind in nachfolgender Tabelle zusammengefasst.

	Interne Risikoanalyse	Externe Risikoanalyse	Partielle Risikoanalyse
Vorteile	Aufbau von RM-Kompetenzen Keine Beratungskosten Keine Abhängigkeit von externen Firmen	Hohe Objektivität Nur ein interner Mitarbeiter (Projektmanager) gebunden Kein technisches Wissen erforderlich	Geringe Abhängigkeit vom Vertragspartner Geringere Beratungskosten Zugriff auf Expertenwissen

²⁸ vgl. Port, 2009

²⁹ vgl. ENISA, 2007

Nachteile	Technische und analytische Expertise erforderlich Gefahr geringer Objektivität Mitarbeiter gebunden	Hohe Abhängigkeit vom Vertragspartner Hohe Kosten Kein Wissenstransfer von externer Firma	Geringere Objektivität durch Mitarbeit interner Angestellter Hoher Wissensstand der Mitarbeiter erforderlich
-----------	---	---	---

Tabelle 1 Vor- und Nachteile der make-or-buy Entscheidung für ein Unternehmen³⁰

Bei externen Risikoanalysen hat das Unternehmen meist nur geringen Einfluss auf den von der beauftragten Firma eingesetzten Risikomanagementprozess³¹. Bei einer partiellen Auslagerung kann der RM-Ansatz meist vereinbart werden. Wichtig dabei ist, dass das Unternehmen in die Lage versetzt wird, die Wartung selbstständig durchführen zu können.

Der in dieser Arbeit vorgeschlagene Ansatz der Risikoanalyse soll so viele Unternehmen als möglich befähigen, die Analyse intern durchführen zu können. Dies ist deshalb wichtig, weil Kleinst- und Kleinunternehmen das Geld für Berater nicht investieren können oder wollen. Es ist sehr viel wahrscheinlicher, dass sie eine Analyse, welche sie selbst mit geringem Aufwand durchführen können, einsetzen, als dass sie eine externe Firma damit beauftragen. Die in der Tabelle beschriebenen Nachteile werden wissentlich akzeptiert.

3 Kleine und mittlere Unternehmen

Kleine und mittlere Unternehmen sind das Rückgrat der europäischen Wirtschaft. In Österreich, Deutschland und der Schweiz liegt der Anteil der KMU an der Gesamtwirtschaft bei über 99%. Im Jahr 2008 waren mehr als 60% aller unselbstständig beschäftigten Personen in Österreich bei einem kleinen oder mittleren Unternehmen angestellt³². Die aktuelle Empfehlung der Europäischen Kommission nennt vier Eigenschaften nach denen Unternehmen in Kleinst-, Klein- und mittlere Unternehmen unterteilt werden³³. Diese Eigenschaften sind:

- Anzahl der Mitarbeiter
- Umsatz
- Bilanzsumme
- Unabhängigkeit

³⁰ vgl. ENISA, 2007

³¹ vgl. ENISA, 2007

³² vgl. KMUForschung, 2009 Seite 7

³³ vgl. EK, 2006

Abbildung 2 zeigt die Schwellenwerte für die Einteilung der Unternehmen. Die Anzahl der Mitarbeiter, der Umsatz und die Bilanzsumme können relativ einfach ermittelt werden; komplizierter sind die Regeln zur Unabhängigkeit eines Unternehmens. Werden mehr als 25% des Kapitals oder der Stimmanteile von einer oder mehreren Nicht-KMU gehalten, dann gilt das Unternehmen nicht mehr als KMU. Außerdem darf ein kleines oder mittleres Unternehmen nicht mehr als 25% an einem anderen Unternehmen halten. Es gibt nur zwei Ausnahmen von dieser Regel³⁴:

1. 25% - 50% werden von folgenden Investoren gehalten:

- Staatliche Beteiligungen, Risikokapitalgesellschaften und „Business Angels“
- Universitäten und Forschungseinrichtungen ohne Gewinnzweck
- Institutionelle Anleger einschließlich regionaler Entwicklungsfonds
- Autonome Gebietskörperschaften mit einem Haushalt von weniger als €10 Mio. und weniger als 5000 Einwohnern

2. Partnerunternehmen:

- Das eigene Unternehmen hält zwischen 25% und 50% des Kapitals oder der Stimmrechte an einem anderen Unternehmen
- Ein anderes Unternehmen hält zwischen 25% und 50% des Kapitals oder der Stimmrechte am eigenen Unternehmen

Mit einer Partnerschaft werden umfangreiche Finanzpartnerschaften eingegangen, die beiden Unternehmen sind aber nicht miteinander verbunden und üben keine Kontrolle aufeinander aus.

Zur Unterscheidung von KMU sollten alle vier Eigenschaften berücksichtigt werden, in der Praxis ist dies aber sehr aufwändig, da kleine Unternehmen von der Meldepflicht vieler primärstatistischer Erhebungen entbunden sind³⁵. Es wird oft nur die Anzahl der Vollzeitbeschäftigten bei der Einteilung der Unternehmen berücksichtigt. Im Jahr 2008 gab es in Österreich insgesamt 232 302 Unternehmen, von denen 233 599 (das entspricht zirka 99,4%) weniger als 250 Mitarbeiter hatten³⁶.

Unternehmen mit mehr als 249 Mitarbeiter oder einem Jahresumsatz von mehr als €50 Mio. bzw. einer Jahresbilanzsumme von mehr als €43 Mio. zählen zu den so genannten Großbetrieben. In Österreich gibt es rund 1300 Großbetriebe.

³⁴ vgl. EK, 2006

³⁵ vgl. WKO, 2008a

³⁶ vgl. WKO, 2009

Größenklasse	Mitarbeiterzahl: Jahresarbeits- einheit (JAE)	Jahresumsatz	Jahresbilanz- summe
Mittleres Unternehmen	< 250	≤ 50 Mio. EUR (1996: 40 Mio. EUR)	≤ 43 Mio. EUR (1996: 27 Mio. EUR)
Kleines Unternehmen	< 50	≤ 10 Mio. EUR (1996: 7 Mio. EUR)	≤ 10 Mio. EUR (1996: 5 Mio. EUR)
Kleinstunternehmen	< 10	≤ 2 Mio. EUR (bisher nicht definiert)	≤ 2 Mio. EUR (bisher nicht definiert)

Abbildung 2 Schwellenwerte zur Einteilung der Unternehmen³⁷

Abbildung 3 zeigt die Unternehmensstruktur in Abhängigkeit der Mitarbeiteranzahl in Österreich. Den bei weitem größten Teil machen Kleinstunternehmen mit bis zu neun Mitarbeitern aus; ihr Anteil betrug 2008 rund 83% an der Gesamtwirtschaft Österreichs. Rund 14% aller Unternehmen zählten 2008 zu den Kleinbetrieben und rund 2,8% der Firmen hatten zwischen 50 und 249 Mitarbeiter.

³⁷ vgl. EK, 2006

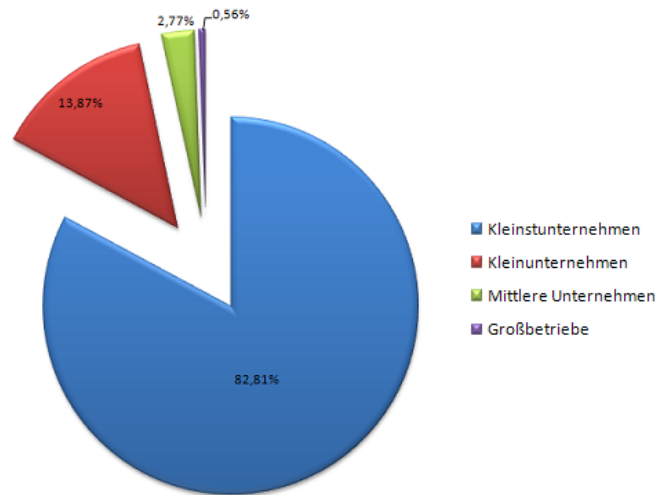


Abbildung 3 Unternehmensstruktur in Österreich bezogen auf die Anzahl der Mitarbeiter im Jänner 2008³⁸

Unternehmen werden oft nach ihrer Zugehörigkeit zum primären, sekundären oder tertiären Sektor unterschieden. Die Sektoren umfassen folgende Unternehmen³⁹:

Primärsektor (Urproduktion):

- Land- und Forstwirtschaft
- Bergbau und Gewinnung von Steinen und Erden

Sekundärsektor (Industrieller Sektor):

- Sachgütererzeugung
- Energie- und Wasserversorgung
- Bauwesen

Tertiärsektor (Dienstleistungssektor):

- Handel, Reparatur von KFZ und Gebrauchsgütern
- Beherbergungs- und Gaststättenwesen
- Verkehr und Nachrichtenübermittlung
- Kredit- und Versicherungswesen
- Realitätenwesen, Unternehmensdienstleistungen
- Öffentliche Verwaltung, Landesverteidigung, Sozialversicherung
- Unterrichtswesen

³⁸ vgl. WKO, 2009

³⁹ vgl. WKO, 2008b

- Gesundheits-, Veterinär- und Sozialwesen
- Erbringung von sonstigen Dienstleistungen
- Private Haushalte
- Exterritoriale Organisationen und Körperschaften

Abbildung 4 zeigt den Zusammenhang zwischen der Anzahl der Mitarbeiter und der Zugehörigkeit eines Unternehmens zum primären, sekundären bzw. tertiären Sektor.

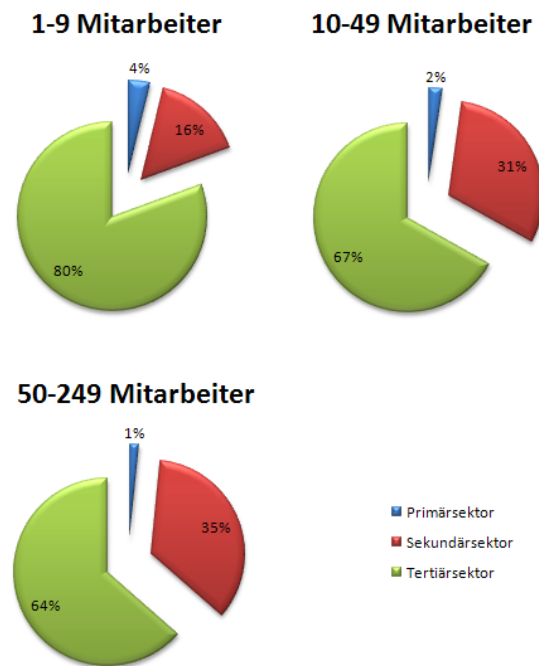


Abbildung 4 Korrelation der Anzahl der Mitarbeiter zur Zugehörigkeit eines Unternehmens zum primären, sekundären bzw. tertiären Wirtschaftssektor

Bei Unternehmen mit bis zu neun Mitarbeitern handelt es sich zu 80% um Dienstleistungsunternehmen. Der Anteil der Unternehmen in der Dienstleistungsbranche und der Urproduktion nimmt mit zunehmender Mitarbeiterzahl ab, Unternehmen des industriellen Sektors nehmen zu. Der in dieser Arbeit vorgestellte Ansatz zur Risikoanalyse richtet sich vordergründig an Unternehmen mit bis zu 49 Mitarbeitern. Dabei handelt es sich bei der überwiegenden Mehrheit um Dienstleistungsunternehmen. Der Ansatz sollte für möglichst viele Unternehmen anwendbar sein, deshalb wird die Zugehörigkeit des Unternehmens zu einem Wirtschaftssektor nicht berücksichtigt. Das Problem eines generischen Ansatzes ist die breite Streuung der Unternehmen, diese reichen von Bergbauunternehmen bis zu hoch spezialisierten IT-Firmen. Die Vielfalt innerhalb der Sektoren ist ebenfalls äußerst groß. Bei Dienstleistungsunternehmen kann es sich

um das Einpersonenunternehmen eines Tischlers oder um eine Anwaltskanzlei mit mehreren Mitarbeitern handeln. Sie alle stellen unterschiedliche Anforderungen an ihre IT-Systeme.

3.1 Einsatz von Informationstechnologie in Klein- und Mittelbetrieben

Statistische Daten zur Verwendung von Informationstechnologie in Unternehmen besagen, dass 96,6% der Kleinunternehmen und 99,7% der mittleren Unternehmen im Jahr 2008 Zugang zum Internet hatten⁴⁰. 76,5% der Klein- und 92,1% der mittleren Unternehmen betrieben 2008 eine Website⁴¹. 41% der Klein- und 52,2% der mittleren Unternehmen haben 2008 Einkäufe über elektronische Netzwerke abgewickelt⁴².

Diese statistischen Daten, welche leider für Kleinstunternehmen nicht vorhanden sind, zeigen, dass der größte Teil der KMU in Österreich Systeme zur elektronischen Datenverarbeitung (EDV) verwendet. Gerade bei kleinen Unternehmen ist das Risikobewusstsein oft nur schwach ausgeprägt. In vielen dieser Unternehmen gibt es keine eigenständige IT-Abteilung und Computersysteme werden nur als Mittel zum Zweck betrachtet, was deren strategischen Bedeutung nicht gerecht wird. Wenn die Festplatte aufgrund eines Hardware-Fehlers in einem kleinen Unternehmen ausfällt und es kein Backup gibt, kann dies leicht zum Verlust wichtiger Daten führen. Auch Angriffe von außen werden oft mit der Bemerkung: „wir sind viel zu klein um für Hacker interessant zu sein“ abgetan. Hierbei handelt es sich jedoch um einen fatalen Irrglauben. Schadsoftware infiziert jeden Rechner, der eine gewisse Schwachstelle aufweist. Da kleine und große Unternehmen oft die gleichen Programme (Betriebssysteme, Textverarbeitung, Browser etc.) verwenden, ist jede Firma diesen Gefahren ausgesetzt. Großbetriebe verfügen meist über höhere finanzielle Mittel und eine eigene IT-Abteilung mit Spezialisten, weshalb sie oft besser geschützt sind als kleine Unternehmen. Die Eigentümer von kleinen Unternehmen haben oft noch nie etwas über Sicherheitsstandards gehört und glauben, dass IT-Sicherheit nur mit Virenschutz und Sicherheitskopien zu tun hat⁴³.

In 56% der KMU ereignete sich im Jahr 2006 ein sicherheitsrelevanter Zwischenfall und viele dieser Unternehmen erholten sich nie wieder davon⁴⁴. Die Steigerung des Risikobewusstseins und die Verdeutlichung der Abhängigkeit des Betriebserfolgs von den IT-Systemen sind essentiell und eine einfache, leicht durchführbare Risikoanalyse kann ein erster Schritt in diese Richtung sein.

⁴⁰ vgl. StatA, 2009a

⁴¹ vgl. StatA, 2009b

⁴² vgl. StatA, 2009c

⁴³ vgl. ENISA, 2007

⁴⁴ vgl. ENISA, 2007

3.2 Anforderungen an eine Risikoanalyse aus Sicht von KMU

Eine Risikoanalyse, welche von kleinen und mittleren Unternehmen durchgeführt werden soll, muss folgende Anforderungen erfüllen:

- Günstige Durchführung (Beratungskosten sollen so gering wie möglich gehalten werden)
- Durchführung durch das eigene Personal (max. zwei Mitarbeiter)
- Durchführbar in ein bis zwei Tagen
- Effektive Analyse der bedrohlichsten Risiken
- Leicht adaptierbar um auf Branchen- und Firmenspezifika und unterschiedliche gesetzliche Anforderungen eingehen zu können
- Leicht wartbare und auch für unerfahrene Personen verständliche Dokumente
- Checklisten um sicherzustellen, dass alle wichtigen Bereiche beachtet werden
- Beispiele zum leichteren Verständnis

Die Intention dieser Diplomarbeit ist es, einen nach diesen Gesichtspunkten ausgerichteten Ansatz der Risikoanalyse zu entwerfen.

4 Datenschutzgesetz

Der in dieser Arbeit vorgestellte Ansatz der Risikoanalyse beinhaltet unter anderem zwölf Fragen zum Datenschutz. Dieses Kapitel soll das österreichische Datenschutzgesetz kurz vorstellen und einige Kernaussagen beleuchten.

Die Staaten der Europäischen Union waren aufgrund der Richtlinie 95/46/EG⁴⁵ gezwungen, die nationalen Datenschutzgesetze zu vereinheitlichen. Das Ziel war es, den freien Datenfluss innerhalb der Union sicherzustellen. In Österreich ist das Datenschutzgesetz 2000 am 1.1.2000 in Kraft getreten.

Das österreichische Datenschutzgesetz (DSG) unterscheidet in §4 zwischen personenbezogenen Daten (z. B. Geburtsdatum, Adresse, Lichtbild) und sensiblen Daten. Sensible Daten sind „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse und philosophische Überzeugung, Gesundheit und ihr Sexualleben.“⁴⁶ Für sensible Daten gilt ein grundsätzliches Verarbeitungsverbot, welches nur zur Wahrung wichtiger öffentlicher Interessen verletzt werden darf⁴⁷. In §4 wird außerdem zwischen Betroffenen und Auftraggebern unterschieden. Auftraggeber sind „natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen

⁴⁵ vgl. Graf, 2004 Seite 9

⁴⁶ vgl. Stärker, 2008 Seite 45

⁴⁷ vgl. Graf, 2004 Seite 36

bestimmten Zweck zu verarbeiten (Z9) und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem Anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten⁴⁸. Betroffener ist „jede vom Auftraggeber (Z4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z8) werden“⁴⁹. Das bedeutet, dass auch Unternehmensdaten dem DSG unterliegen.

Das Gesetz definiert eine Datei als „strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind“⁵⁰. Darunter fallen auch manuelle Dateien wie Karteikarten und Listen. Das bedeutet, dass Karteikarten und Listen, welche personenbezogenen Daten enthalten, ebenfalls hinreichend zu schützen sind. So müssen beispielsweise Karteikarten mit den Namen und Adressen von Kunden in einem verschlossenen Schrank aufbewahrt werden.

Unter dem Verarbeiten von Daten versteht man: „das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister“⁵¹. Dienstleister sind „natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden“⁵². Ausnahmen gelten für journalistische (§48) und statistische Zwecke (§46).

Jeder Betroffene hat das Recht auf Auskunft (§26) sowie Richtigstellung und Löschung (§27) der ihn betreffenden Daten. Wird eine Auskunft verlangt, müssen „die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen“⁵³ sowie der Zweck der Datenanwendung und die rechtliche Grundlage innerhalb von acht Wochen bekannt gegeben werden. Werden unrichtige Daten verarbeitet oder ist die Verarbeitung der Daten unzulässig beziehungsweise erfolgt ein Antrag auf Richtigstellung oder Löschung, ist der Auftraggeber verpflichtet, diese Daten zu löschen oder richtig zu stellen. Dies betrifft jedoch nur „Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist“⁵⁴. Ein Auftraggeber muss in der Lage sein diesen Pflichten nachzukommen, dies erfordert eine gewissenhafte Dokumentation jedes Datums.

⁴⁸ vgl. Stärker, 2008 Seite 45

⁴⁹ vgl. Stärker, 2008 Seite 45

⁵⁰ vgl. Stärker, 2008 Seite 46

⁵¹ vgl. Stärker, 2008 Seite 45

⁵² vgl. Stärker, 2008 Seite 46

⁵³ vgl. RIS, 2009b

⁵⁴ vgl. RIS, 2009a

Die Übermittlung von Daten in Länder außerhalb der Europäischen Union ist grundsätzlich genehmigungspflichtig. Ausnahmen von dieser Regel sind so genannte sichere Drittstaaten, in denen der Datenschutz gewährleistet ist. Nicht genehmigungspflichtige Drittstaaten sind laut Europäischer Union⁵⁵:

- Argentinien
- Kanada
- Guernsey
- Isle of Man
- Jersey
- Schweiz
- Vereinigte Staaten – nur Unternehmen die sich den „Safe Harbour“ Vereinbarungen unterworfen haben

Bei Übermittlung von Daten in andere als die oben genannten Staaten ist eine Genehmigung durch die Datenschutzkommission einzuholen (§13).

Jeder Auftraggeber ist verpflichtet, vor Aufnahme einer Datenanwendung, eine Meldung an die Datenschutzkommission zu erstatten. Diese Meldung muss unter anderem auch die vorhandenen Schutzmaßnahmen umfassen (§19). Nicht meldungspflichtig sind die Verarbeitung öffentlicher oder nur indirekt personenbezogener Daten, die Verarbeitung zu persönlichen oder familiären Zwecken und Standardanwendungen. Zu den Standardanwendungen zählen⁵⁶:

- Rechnungswesen und Logistik
- Personalverwaltung
- Mitgliederverwaltung
- Verwaltung von Benutzerkennzeichen
- Kundenbetreuung und Marketing für eigene Zwecke
- Patientenverwaltung und Honorarabrechnung
- Personentransport und Hotelreservierung
- Zutrittskontrollsysteme
- KFZ-Zulassung durch beliehene Unternehmen

Diese kurze Zusammenfassung des Datenschutzgesetzes stellt keinen Anspruch auf Vollständigkeit, vielmehr sollten einige wichtige Punkte angesprochen werden, um die in der Risikoanalyse (siehe Kapitel 7) gestellten Fragen besser zu verstehen.

⁵⁵ EK, 2008

⁵⁶ vgl. Graf, 2004 Seite 59ff

5 Existierende Ansätze der Risikoanalyse

Es gibt sehr viele unterschiedliche Ansätze der IT-Risikoanalyse. Die meisten sind jedoch sehr umfangreich und mit hohen Kosten verbunden. Die „European Network and Information Security Agency“ (ENISA) hat etliche Ansätze der Risikoanalyse und des Risikomanagements auf ihre Anwendbarkeit bei KMU untersucht. Folgende Ansätze der Risikoanalyse eignen sich auch für den Einsatz in KMU⁵⁷:

- Österreichisches Informationssicherheitshandbuch
- ISO/IEC 27005
- IT-Grundschutz
- Mehari
- OCTAVE-S
- NIST SP800-30

Diese Ansätze werden nun kurz vorgestellt und am Ende des Kapitels verglichen.

5.1 Österreichisches Informationssicherheitshandbuch

Das österreichische Bundeskanzleramt (BKA) hat zusammen mit der Österreichischen Computergesellschaft (OCG) im Jahr 2007 das „Österreichische Informationssicherheitshandbuch“ in der Version 2.3 veröffentlicht⁵⁸. Dieses besteht aus zwei Teilen: Teil 1 befasst sich mit dem Informationssicherheitsmanagement und Teil 2 mit den Informationssicherheitsmaßnahmen. Kapitel 4 aus Teil 1 ist der Risikoanalyse gewidmet.

Ziel einer Risikoanalyse ist es die identifizierten Risiken „so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird“⁵⁹. Im Handbuch werden drei Arten von Risikoanalysen unterschieden:

- Detaillierte Analyse
- Grundschutzansatz
- Kombiniertes Ansatz

Die detaillierte Analyse ist aus Zeit- (Wochen bis Monate für die Erstdurchführung) und Kostengründen für KMU nicht anwendbar und wird hier deshalb nur schemenhaft beschrieben. Folgende Schritte sind erforderlich um eine detaillierte Analyse durchzuführen:

- Abgrenzung der zu analysierenden IT-Systeme und Objekte
- Erfassung aller bedrohten Objekte im Analysebereich
- Ermittlung der Werte der bedrohten Objekte
- Durchführung einer Bedrohungsanalyse

⁵⁷ vgl. ENISA, 2006b

⁵⁸ vgl. BKA, 2007

⁵⁹ vgl. BKA, 2007 Seite 35

- Identifikation der Schwachstellen
- Überprüfung der existierenden Sicherheitsmaßnahmen
- Bewertung der Einzelrisiken und des Gesamtrisikos
- Auswertung und Aufbereitung der Ergebnisse

Bei einer detaillierten Analyse werden alle IT-Systeme des zu analysierenden Bereichs untersucht. Dies gewährleistet einen größtmöglichen Schutz und effektive Sicherheitsmaßnahmen. Aufgrund der hohen Kosten, des erforderlichen Expertenwissens und der langen Dauer ist sie für KMU im Allgemeinen ungeeignet.

Der Grundschutzansatz geht von einer pauschalisierten Gefährdungslage für alle IT-Systeme aus. Dadurch kann die Analyse schneller und günstiger durchgeführt werden, das gleiche Maß an Sicherheit wie bei einer detaillierten Analyse aber nicht immer gewährleistet werden. Dieser Ansatz sollte ausschließlich dann gewählt werden, wenn die IT-Systeme nur niedrigen oder mittleren Schutzbedarf haben. Die Grundschutzanalyse besteht aus den folgenden zwei Aufgaben:

- Modellierung
- Soll-Ist Vergleich

Die Modellierung dient der möglichst realitätsnahen und vollständigen Abbildung der IT-Systeme mithilfe so genannter Baustein- und Maßnahmenkataloge. Das Handbuch verweist auf die Kataloge des Deutschen Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik⁶⁰. Eine ausführlichere Beschreibung des IT-Grundschutzes folgt in Kapitel 5.3.

Beim Soll-Ist Vergleich dient das Modell als Ist-Zustand und die in den einzelnen Bausteinen beschriebenen Schutzmaßnahmen als Soll-Zustand. In der abschließenden Dokumentation müssen alle durchgeführten (eventuell über den Soll-Vorschlag hinausgehenden) Schutzmaßnahmen dokumentiert und nicht durchgeführte Empfehlungen gerechtfertigt werden. Der Grad der Umsetzung kann mit „ja/ nein/ teilweise/ entbehrlich“ angegeben werden, des Weiteren muss ein Verantwortlicher, ein Umsetzungszeitpunkt und eine Kostenabschätzung vermerkt sein.

Der kombinierte Ansatz versucht das Beste aus den beiden zuvor beschriebenen Ansätzen zu vereinen. Dabei werden die IT-Systeme zuerst nach Schutzbedarf in „niedrig“ und „mittel“ bzw. „hoch“ und „sehr hoch“ unterteilt. Dazu müssen alle IT-Systeme erfasst, die vorhandenen Anwendungen den einzelnen System zugeordnet und eine Schutzbedarfsfeststellung für jedes IT-System durchgeführt werden⁶¹.

Für Systeme mit niedrigem oder mittlerem Schutzbedarf wird eine Analyse nach dem Grundschutzansatz durchgeführt. Auf die verbleibenden Systeme wird eine detaillierte Analyse angewendet. Dieser Ansatz ermöglicht es rasch ein hohes Maß an Sicherheit zu gewährleisten und besonders schützenswerte Systeme trotzdem bestmöglich zu schützen. Ein kritischer Punkt des kombinierten Ansatzes ist es, die Schutzbedarfskategorien festzulegen. Das österreichische IT-Sicherheitshandbuch

⁶⁰ vgl. BSI-Kataloge, 2009

⁶¹ vgl. BKA, 2007 Seite 52

liefert hierfür sieben Beispiele⁶², welche in Tabelle 2 abgebildet sind. Zu beachten ist, dass diese Tabelle nur ein Beispiel darstellt und nicht unreflektiert für jedes Unternehmen anwendbar ist.

	Schutzbedarfskategorie „niedrig bis mittel“	Schutzbedarfskategorie „hoch bis sehr hoch“
Verstoß gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Gesetze und Vorschriften mit geringfügigen Konsequenzen, geringfügige Vertragsverletzungen mit geringen Konventionalstrafen	schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung), Vertragsverletzung mit hohen Konventionalstrafen oder Haftungsschäden
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung scheint nicht möglich.	Eine über Bagatellverletzungen hinausgehende Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen. Eine Zielerfüllung ist mit vertretbarem Mehraufwand möglich.	Es kann zu einer schweren Beeinträchtigung bis hin zur Handlungsunfähigkeit einer Organisation kommen. Bedeutende Zielabweichung in Qualität und/oder Quantität
Vertraulichkeit der verarbeiteten Information	Es werden nur Daten der Sicherheitsklassen „offen“ und „eingeschränkt“ verarbeitet bzw. gespeichert.	Es werden auch Daten der Sicherheitsklassen „vertraulich“, „geheim“ und/oder „streng geheim“ verarbeitet bzw. gespeichert.
Dauer der Verzichtbarkeit	Die maximal tolerierbare Ausfallzeit der Anwendung beträgt mehrere Stunden bis mehrere Tage.	Die maximal tolerierbare Ausfallzeit der Anwendung beträgt lediglich einige Minuten.
Negative Auswirkungen	Eine geringe bzw. nur interne Ansehen- bzw. Vertrauensbeeinträchtigung ist zu erwarten.	Eine breite Beeinträchtigung des Vertrauens in die Organisation oder ihres Ansehens ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden ist (z. B.) kleiner als €50 000.	Der zu erwartende finanzielle Schaden ist (z. B.) größer als €50 000.

⁶² vgl. BKA, 2007 Seite 50

Tabelle 2 Beispiele für die Festlegung der Schutzbedarfskategorien⁶³

Alternativ zu der obigen Festlegung der Schutzbedarfskategorien kann auch eine Dreiteilung in „normal“, „hoch“ und „sehr hoch“ erfolgen. Da jede Gegenmaßnahme auf dieser Schutzbedarfskategorie beruht, ist es unerlässlich, diese Festlegung gründlich und vollständig durchzuführen.

Zusammenfassend kann gesagt werden, dass die Vorschläge des Österreichischen Informationssicherheitshandbuchs sehr abstrakt sind und kaum konkrete Vorschläge für die Umsetzung vorhanden sind. Bei der Grundschutzanalyse wird auf die Vorgangsweise und Kataloge des BSI verwiesen.

5.2 ISO/IEC 27005

Die internationale Norm ISO/IEC 27005 ist Teil der ISO 2700x Serie, welche sich mit Informationssicherheit beschäftigt. Bisher veröffentlichte Normen dieser Serie sind⁶⁴:

- ISO 27000 Overview and vocabulary
- ISO 27001 Requirements
- ISO 27002 Code of practice for information security management
- ISO 27005 Information security risk management
- ISO 27006 Requirements for bodies providing audit and certification of information security management systems

Die Normen ISO 27001 und 27002 sind in Österreich übernommen worden und als ÖNORM verfügbar. Laut Information von Herrn Dipl. Ing. Stumwöhrer von „Austrian Standards plus“ wird die ISO-Norm 27005 nicht als ÖNORM übernommen werden⁶⁵.

5.2.1 ISO 27001

Der Standard 27001 „spezifiziert die Anforderungen an das Festlegen, Umsetzen, Betreiben, Überwachen, Überprüfen, Instandhalten und Verbessern eines dokumentierten ISMS im Kontext zu den allgemeinen Geschäftsrisiken der Organisation“⁶⁶. Ein ISMS ist ein Informationssicherheits-Managementsystem. Zur Einrichtung eines ISMS sind folgende Schritte erforderlich⁶⁷:

- Definition des Anwendungsbereichs und der Grenzen des ISMS
- Definition der ISMS-Politik (Zielsetzung und Anforderungen)

⁶³ vgl. BKA, 2007 Seite 50

⁶⁴ vgl. ISO, 2009

⁶⁵ mdl. Stumwöhrer, 2009

⁶⁶ vgl. ÖNORM 27001, 2008

⁶⁷ vgl. ÖNORM 27001, 2008

- Definition der Vorgangsweise für die Risikobewertung
- Identifizierung der Risiken
- Analyse und Evaluierung der Risiken
- Optionen der Risikobehandlung (Akzeptanz, Vermeidung, Übertragung)
- Auswahl der Maßnahmenziele

Zur Identifizierung der Risiken müssen die organisatorischen Vermögenswerte, die Bedrohungen und die Schwachstellen ermittelt werden. Anschließend müssen die Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit bewertet werden.

5.2.2 ISO 27002

Der Standard 27002 beschäftigt sich mit Möglichkeiten ein ISMS einzuführen, aufrechtzuerhalten und zu verbessern. Hierfür ist die Norm in elf Abschnitte unterteilt⁶⁸:

- Sicherheitspolitik
- Organisation der Informationssicherheit
- Management von Vermögenswerten
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebs
- Zugriffskontrolle
- Beschaffung, Entwicklung und Instandhaltung von Informationssystemen
- Umgang mit Informationssicherheits-Vorfällen
- Betriebliches Kontinuitätsmanagement
- Einhaltung der Verpflichtung

Jede Maßnahme ist in Hauptsicherheitskategorien unterteilt, welche mit Hinweisen zur Implementierung versehen sind. Diese Hinweise sind jedoch oft abstrakt und nicht direkt umsetzbar. Bei einer konsequenten Umsetzung aller Hauptsicherheitskategorien kann ein hohes Maß an Sicherheit erzielt werden.

5.2.3 ISO 27005

Im Mittelpunkt der ISO 27005 Norm steht der Information Security Risk Management Process. Dieser kontinuierliche Prozess besteht aus der Definition des Kontexts, einer Risikobewertung, einer Risikobehandlung und der Umsetzung der Entscheidungen (siehe Abbildung 5). Dieses Konzept kann auf die gesamte Organisation, auf Teilbereiche und auf jedes geplante oder existierende Informationssystem angewendet werden.

⁶⁸ vgl. ÖNORM 27002, 2008

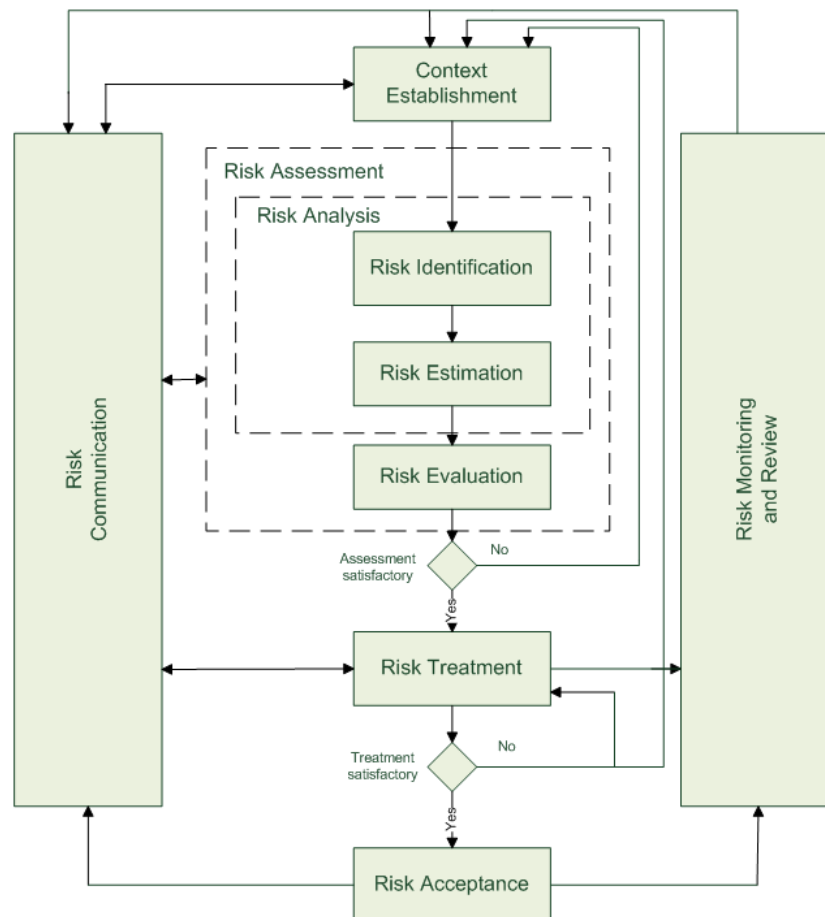


Abbildung 5 Information Security Risk Management Process⁶⁹

Die Risikoakzeptanz am Ende jeder Iteration ist erforderlich, um das Restrisiko durch das verantwortliche Management abzeichnen zu lassen. Wie die Skizze zeigt, ist die Weitergabe der Risiken (Risk Communication) entscheidend und muss in jeder Phase des Prozesses vorhanden sein. Die Beobachtung der Risiken nach der Risikobehandlung bzw. nach der Akzeptanz der Risiken ist ebenfalls erforderlich. Risiken ändern sich im Laufe der Zeit und neue Risiken können entstehen. Nur durch kontinuierliche Überwachung ist es möglich, das Sicherheitsniveau langfristig auf einem akzeptablen Niveau zu halten.

Im Folgenden werden die einzelnen Schritte des Prozesses kurz beschrieben. Besonderes Augenmerk wird dabei auf die Risikoanalyse gelegt, weil diese der Schwerpunkt dieser Arbeit ist.

⁶⁹ Nach ISO 27005, 2008

Definition des Kontexts (Context Establishment): Der Kontext enthält alle für die Durchführung notwendigen Informationen. Unter anderem sind dies:

- Risikobewertungs-, Auswirkungs-, Risikoakzeptanzkriterien
- Umfang und Grenzen des ISMS
- Organisation des ISMS
- Verantwortlichkeiten im ISMS

Die Risikobeurteilung (Risk Assessment) besteht aus⁷⁰:

- Risikoanalyse (Risk Analysis)
- Risikoidentifikation (Risk Identification)
- Risikoabschätzung (Risk Estimation)
- Risikobewertung (Risk Evaluation)

Die Risikoanalyse ist in diesem Ansatz Teil der Risikobeurteilung und umfasst die Risikoidentifikation und die Risikoabschätzung, wobei die Erkenntnisse der Risikoidentifikation als Eingabeparameter für die Risikoabschätzung dienen.

Die Schritte zur Durchführung der Risikoidentifikation und der Risikoabschätzung sind in Abbildung 6 dargestellt.

⁷⁰ vgl. ISO 27005, 2008 Seite 10

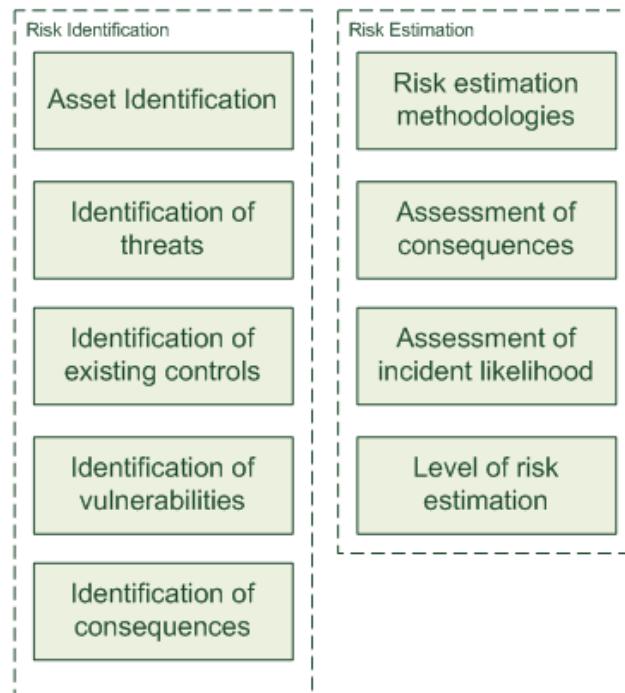


Abbildung 6 Schritte der Risikoidentifizierung und der Risikoabschätzung

Die Risikoidentifikation umfasst folgende fünf Schritte (siehe Abbildung 6):

- Identifizierung der Vermögenswerte (Asset Identification)
Identifizierung aller Vermögenswerte, welche sich im Umfang des ISMS befinden. Die Verantwortlichkeiten für jeden Vermögenswert müssen klar geregelt sein. Es werden primäre Vermögenswerte (Business Processes & Activities und Informationen) und sekundäre Vermögenswerte (Hardware, Software, Netzwerk, Personal, Gebäude und Organisationsstruktur) unterschieden. Zur Identifikation der Vermögenswerte werden Arbeitsgruppen bestehend aus Managern, IT-Spezialisten und Anwendern vorgeschlagen.
- Gefahrenidentifizierung (Identification of Threats)
Gefahren haben das Potential einen Vermögenswert negativ zu beeinflussen. Es werden allgemein natürliche und menschliche Gefahren unterschieden. Menschliche Handlungen können absichtlich oder unabsichtlich sein, beides sollte berücksichtigt werden. Gefahren können auch danach unterschieden werden, ob sie von innerhalb des

Unternehmens oder von außerhalb ausgehen. Im Standard werden die in Tabelle 3 aufgelisteten Gefahren genannt. Die Buchstaben A, D und E in der Spalte „Origin“ stehen für „accidental“, „deliberate“ und „environmental“.

Type	Threat	Origin
Physical damage	Fire	A,D,E
	Water damage	A,D,E
	Pollution	A,D,E
	Major accident	A,D,E
	Destruction of equipment or media	A,D,E
	Dust, corrosion, freezing	A,D,E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A,D
	Loss of power supply	A,D,E
	Failure of telecommunication equipment	A,D
Disturbance due to radiation	Electromagnetic radiation	A,D,E
	Thermal radiation	A,D,E
	Electromagnetic pulses	A,D,E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A,D
	Data from untrustworthy	A,D

	sources	
	Tampering with hardware	D
	Tampering with software	A,D
	Position detection	D
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A,D
	Software malfunction	A
	Breach of information system maintainability	A,D
Unauthorized actions	Unauthorized use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A,D
	Corruption of data	D
	Illegal processing of data	D
Compromise of function	Error in use	A
	Abuse of rights	A,D
	Forging rights	D
	Denial of actions	D
	Breach of personnel availability	A,D,E

Tabelle 3 Liste der typischen Gefahren⁷¹; D – deliberate, A – accidental, E – environmental

- Sicherheitsvorkehrungen (Identification of Existing Controls)
In diesem Schritt werden die vorhandenen und die in Planung befindlichen Sicherheitsvorkehrungen erfasst und evaluiert. Um diesen Vorgang zu erleichtern, sollten vorhandene Dokumente über installierte Sicherheitsvorkehrungen, Personen aus dem Bereich Informationssicherheit, und Audit-Dokumente herangezogen werden.
- Schwachstellenanalyse (Identification of Vulnerabilities)
Schwachstellen sollten in den folgenden Bereichen identifiziert werden:
 - Organisation

⁷¹ vgl. ISO 27005, 2008 Seite 39f

- Prozesse und Prozeduren
- Managementroutinen
- Personal
- Physische Umgebung
- Konfiguration des Informationssystems
- Hardware, Software und Kommunikationsausrüstung
- Abhängigkeit von externen Akteuren

Eine Schwachstelle kann nur dann Schaden anrichten, wenn eine Gefahr besteht, welche diese Schwachstelle ausnutzen kann.

➤ Konsequenzen (Identification of Consequences)

Als Konsequenzen werden der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit angesehen. Es gilt herauszufinden, was passieren könnte, wenn ein sicherheitsrelevanter Zwischenfall eintritt. Die Konsequenzen sollten unter anderem die folgenden Punkte berücksichtigen:

- Nachforschungs- und Reparaturzeit
- Arbeits(zeit)verlust
- Opportunitätskosten
- Gesundheit und Sicherheit
- Finanzielle Kosten und Fähigkeiten, welche für die Reparatur erforderlich sind
- Ruf des Unternehmens

Die Risikoabschätzung besteht aus vier Schritten (siehe Abbildung 6):

➤ Risikoabschätzungsmethoden (Risk Estimation Methodologies)

Hierbei werden qualitative und quantitative Methoden für die Eintrittswahrscheinlichkeit und die Auswirkungen unterschieden. Die Empfehlung ist, in einem ersten Schritt eine meist kostengünstigere und leichtverständliche qualitative Methode durchzuführen und erst danach, bei Bedarf, eine quantitative. Der Nachteil der qualitativen Beurteilung ist die enthaltene Subjektivität. Quantitative Methoden verwenden meist historische Daten, was dazu führt, dass neue Risiken nur schwer zu bewerten sind. Außerdem täuschen die numerischen Ergebnisse eine Objektivität vor, die oft nicht gerechtfertigt ist.

➤ Bewertung der Konsequenzen (Assessment of Consequences)

Um die Auswirkungen zu beurteilen, müssen den Vermögenswerten Geldwerte zugeordnet werden. Jeder Vermögenswert wird mit seinem

Wiederbeschaffungswert (Replacement Costs) bewertet. Dieser Wert umfasst sowohl die Anschaffung als auch die Wiederherstellung der verlorenen Informationen - falls dies möglich ist.

Neben dieser monetären Betrachtungsweise gibt es auch die Geschäftsauswirkungen (Business Consequences), welche sich aufgrund rechtlicher Vorgaben ergeben können. Diese Geschäftsauswirkungen sind meist viel höher als die reinen Wiederbeschaffungskosten.

➤ Zwischenfallswahrscheinlichkeit (Assessment of Incident Likelihood)

In diesem Schritt wird die Wahrscheinlichkeit eines Zwischenfalls bewertet. Dazu werden die Zwischenfälle in Szenarien unterteilt und diese qualitativ und quantitativ bewertet. Zur Bewertung der Eintrittswahrscheinlichkeit, der Motivation der Täter bei absichtlichen Taten, und geografischen Faktoren bei Unfällen, wird auf Erfahrungswerte zurückgegriffen.

➤ Risikobeurteilung (Level of Risk Estimation)

Aufbauend auf den vorhandenen Daten (bewertete Konsequenzen und Wahrscheinlichkeiten) wird in diesem Punkt die Risikobeurteilung durchgeführt. Diese Beurteilung kann qualitativ oder quantitativ erfolgen.

Die weiteren Schritte des Informationssicherheits-Managementprozesses werden im Folgenden kurz erklärt.

Risikobewertung (Risk Evaluation)

Die zuvor durchgeführte Risikobeurteilung wird nun mit den Risikoevaluierungskriterien (Risk Evaluation Criteria) und den Risikoakzeptanzkriterien (Risk Acceptance Criteria) verglichen. Diese Kriterien wurden bereits bei der Definition des Kontexts festgelegt. Am Ende dieses Schrittes sind alle Risiken mit Prioritäten versehen.

Risikobehandlung (Risk Treatment)

Bei der Risikobehandlung wird ein Risikobehandlungsplan erstellt, welcher für die identifizierten und bewerteten Risiken Handlungen definiert. Diese Handlungen können Reduktion (Risk Reduction), Akzeptanz (Risk Retention), Vermeidung (Risk Avoidance) oder Übertragung (Risk Transfer) sein. Welche Handlung gesetzt wird, hängt von der Analyse und den Kosten ab. Ist eine hohe Reduktion zu geringen Kosten möglich, sollte diese durchgeführt werden. Das Ziel ist es, die Auswirkungen so weit wie möglich und so günstig wie möglich zu verringern. Dies kann entweder durch eine Reduktion der Eintrittswahrscheinlichkeiten oder durch eine Reduktion der zu erwartenden Konsequenzen erreicht werden.

Risikoakzeptanz (Risk Acceptance)

Ein hundertprozentiger Schutz kann fast nie erreicht werden. Das bestehende Restrisiko muss dem Management in geeigneter Form vorgelegt und durch eine Unterschrift zur Kenntnis genommen werden. Für das Akzeptieren wurden bereits im Kontext Kriterien festgelegt. Wichtig dabei ist festzulegen, weshalb welches Risiko akzeptiert wurde.

Risikokommunikation (Information Security Risk Communication)

Es ist wichtig, dass das Management Informationen über die Risiken mit allen Interessenten (Stake Holder) teilt. Dadurch wird Vertrauen aufgebaut und die Interessenten können das Gesamtrisiko besser abschätzen.

Risikoüberwachung und -überprüfung (Information Security Risk Monitoring and Review)

Schwachstellen, Eintrittswahrscheinlichkeiten und Auswirkungen unterliegen einem ständigen Wandel. Um frühzeitig auf Veränderungen reagieren zu können, müssen die Risiken überwacht werden. Dabei ist es wichtig, die Risiken gesamtheitlich zu betrachten. Außerdem muss der gesamte Informationssicherheits-Managementprozess periodisch auf seine Wirksamkeit überprüft werden. Jede

Adaptierung muss schriftlich festgehalten und von einem zuständigen Manager genehmigt werden.

Zusammenfassend kann gesagt werden, dass die ISO Norm 2700x sehr umfassend ist und in sehr vielen Bereichen eingesetzt werden kann. Die Umsetzung erfordert viel Wissen und einen hohen Personal- und Zeitaufwand. Durch die größtenteils abstrakte Beschreibung ist eine direkte Umsetzung nur bedingt möglich. Im Anhang der Norm befinden sich jedoch einige sehr hilfreiche Checklisten. Ein großer Vorteil ist die Möglichkeit der Zertifizierung.

5.3 IT-Grundschutz

Der IT-Grundschutz wurde vom deutschen Bundesamt für Sicherheit in der Informationstechnik herausgegeben. Die Vorschläge des BSI richten sich vorrangig an Bund, Länder und Kommunen in Deutschland, sie können aber auch von privaten Unternehmen angewendet werden.

Der Grundschutz besteht aus vier Dokumenten⁷²:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

Die Idee ist, einzelne, häufig verwendete Geschäftsprozesse, Anwendungen und IT-Systeme in so genannten Bausteinen abzubilden. Für jeden Baustein werden die Bedrohungen und die Eintrittswahrscheinlichkeiten beschrieben. Das bedeutet, dass bei einer Risikoanalyse nach IT-Grundschutz die Infrastruktur eines Unternehmens mithilfe der Bausteine nachgebildet werden muss, das Abschätzen der Eintrittswahrscheinlichkeiten aber entfällt. Die durchzuführende Analyse besteht aus einem Soll-Ist Vergleich zwischen den in den Bausteinen empfohlenen und den bereits realisierten Maßnahmen⁷³. Durch Anwendung des IT-Grundschutzes kann die Erstellung des Sicherheitskonzeptes deutlich beschleunigt werden. Der Standard 100-3 (Risikoanalyse) ist nur für Komponenten mit sehr hohem Schutzbedarf anzuwenden. Eine Risikoanalyse im klassischen Sinne (Bedrohungsanalyse, Feststellung der Eintrittswahrscheinlichkeiten, usw.) ist beim IT-Grundschutz nicht erforderlich, da dies für die einzelnen Bausteine bereits vom BSI durchgeführt wurde.

⁷² vgl. BSI, 2009b

⁷³ vgl. BSI, 2009a

5.3.1 Vorgehensweise

Um eine Analyse durchzuführen, muss zuerst der Geltungsbereich festgelegt werden. Dies können beispielsweise Organisationseinheiten oder Geschäftsprozesse sein. Sinnvollerweise sollten besonders gefährdete bzw. außerordentlich wichtige Bereiche zuerst geschützt werden. Dies ist beispielsweise dann hilfreich, wenn eine vollständige Analyse aus Kostengründen nicht durchführbar ist.

Ist der Geltungsbereich festgelegt, wird eine Strukturanalyse durchgeführt. Diese umfasst vernetzte und nichtvernetzte IT-Systeme (inkl. Druckern, Telekommunikationsanlagen, etc.) sowie deren Kommunikationsverbindungen und alle Verbindungen nach außen. Des Weiteren müssen die Geschäftsprozesse inklusive der Anwendungen, die sie unterstützen, und organisatorische und personelle Rahmenbedingungen berücksichtigt werden. Zuerst werden die Anwendungen und Geschäftsprozesse, anschließend die Netzpläne und IT-Systeme und zuletzt die Räume erfasst. Wenn viele gleichartige Objekte (z. B. Windows-XP Arbeitsplätze) vorhanden sind, können diese zu Gruppen zusammengefasst werden. Wichtig dabei ist, dass sie vom gleichen Typ sind, vergleichbare Anwendungen verwendet werden, sie ähnlich in das Netzwerk eingebunden sind und sie den gleichen Schutzbedarf aufweisen. Bei der Strukturanalyse sollte auf Datenträger wie USB-Stick und Backup-Datenträger nicht vergessen werden.

Der nächste Schritt ist eine Schutzbedarfsfeststellung. Hierbei wird der Schutzbedarf der technischen Infrastruktur, der verarbeiteten Informationen und der Geschäftsprozesse - ausgehend von den zu erwartenden Schäden - ermittelt. Die Schutzbedarfskategorien für die Schutzbedarfsklassen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ werden mit „normal“, „hoch“ und „sehr hoch“ angegeben. „Sehr hoch“ bedeutet, dass der zu erwartende Schaden für das Unternehmen existenzbedrohend ist. Nachdem der Schutzbedarf für alle Komponenten bekannt ist, kann das Informationssystem mithilfe der Bausteine modelliert werden.

Es sind fünf Gruppen von Bausteinen definiert⁷⁴:

- B1: Übergreifende Aspekte der Informationssicherheit
- B2: Sicherheit der Infrastruktur
- B3: Sicherheit der IT-Systeme
- B4: Sicherheit im Netz
- B5: Sicherheit in Anwendungen

Fünf Gefährdungskataloge beschreiben die in den Bausteinen beschriebenen Gefährdungen⁷⁵:

- G1: Höhere Gewalt
- G2: Organisatorische Mängel
- G3: Menschliche Fehlhandlungen

⁷⁴ vgl. BSI, 2009a

⁷⁵ vgl. BSI, 2009a

- G4: Technisches Versagen
- G5: Vorsätzliche Handlungen

Des Weiteren gibt es sechs Maßnahmenkataloge, welche die empfohlenen Sicherheitsmaßnahmen beschreiben⁷⁶:

- M1: Infrastruktur
- M2: Organisation
- M3: Personal
- M4: Hard- und Software
- M5: Kommunikation
- M6: Notfallvorsorge

Das Baukastensystem ermöglicht es, auch Informationssysteme, welche sich noch in Planung befinden, zu modellieren. Dadurch können schon während der Konzeptionierung neuer Systeme die notwendigen Sicherheitssysteme berücksichtigt werden und das Modell als Entwicklungsplan verwendet werden. Abbildung 7 zeigt den Ablauf der Grundschutzanalyse grafisch.

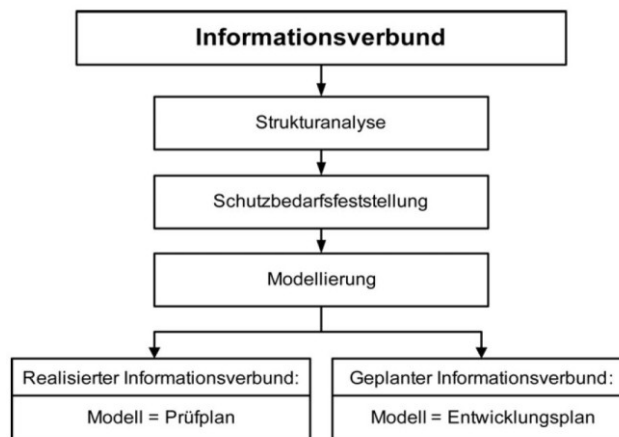


Abbildung 7 Ablauf der Grundschutzanalyse⁷⁷

Der letzte Schritt ist der Soll-Ist Vergleich; hier werden die in den Maßnahmenkatalogen empfohlenen Maßnahmen mit den bereits umgesetzten verglichen. Der Umsetzungsstatus wird mit „entbehrlich“, „ja“, „teilweise“ und „nein“ angegeben. Um den Umsetzungsstatus zu erheben, muss für jeden Baustein ein Gesprächspartner gewählt und befragt werden. Der Gesprächspartner ergibt sich dabei aus dem Inhalt des Bausteins. Für den Baustein B1.6 Computer-Viren-Schutzkonzept wird beispielsweise ein Mitarbeiter der IT-Abteilung befragt werden.

⁷⁶ vgl. BSI, 2009a

⁷⁷ Vgl. BSI, 2009c

Das BSI bietet, neben den Bausteinen und Maßnahmenkatalogen, zwei Arten von Hilfen für die Umsetzung an. Einerseits gibt es das kostenpflichtige Programm GSTOOL, welches den gesamten Vorgang von der Erhebung der Daten bis zur Umsetzung der Maßnahmen unterstützt, andererseits stehen für jeden Schritt Formulare zur Verfügung.

Der eben beschriebene Vorgang der Risikoanalyse eignet sich für alle Standardanwendungen. Für besonders schützenswerte Bereiche sollte eine erweiterte Analyse nach Standard 100-3 durchgeführt werden. Dabei werden die Gefährdungen analysiert, bewertet und Risikobehandlungen erarbeitet. Bei der Risikobehandlung können Risiken entweder auf ein erträgliches Maß reduziert, vermieden bzw. verlagert oder akzeptiert werden. Im Unterschied zu den Bausteinen muss der Anwender hierbei die Eintrittswahrscheinlichkeiten selbst einschätzen, was bei unerfahrenen Benutzern oft problematisch ist.

Nach der Umsetzung der Maßnahmen ist es wichtig, dass ein kontinuierlicher Informationssicherheitsprozess implementiert wird. Dieser Prozess stellt die fortlaufende Aktualisierung der Dokumente und die Überprüfung der Effizienz der umgesetzten Sicherheitsmaßnahmen sicher. Das Sicherheitsmanagement nach BSI-Grundsatz kann auch zertifiziert werden. Dazu wird von einer externen Stelle bestätigt, dass die Maßnahmen nach IT-Grundsatz auf der Basis von ISO 2700x umgesetzt wurden. Dies ist möglich, weil der Grundsatzansatz auf der internationalen ISO-Norm 2700x aufbaut. Der Grundsatzansatz ist bei der Umsetzung jedoch sehr viel konkreter und erfordert weniger Zeitaufwand und Wissen. Eine Zertifizierung kann das Vertrauen der Geschäftspartner in die Informationssicherheit des Unternehmens steigern, ist aber mit erheblichen Kosten verbunden.

Der IT-Grundsatz ist so konzipiert, dass er in vielen Branchen angewendet werden kann. Es ist aber immer darauf zu achten, die Vorgaben nicht stur zu befolgen, sondern zu überlegen, ob sie im konkreten Fall sinnvoll und hilfreich, und mit der Gesetzeslage vereinbar sind. Die empfohlenen Maßnahmen sollten sinngemäß umgesetzt werden und alle Abweichungen sollten dokumentiert werden um sie auch später noch nachvollziehen zu können.

5.3.2 Beispiel

Im Folgenden wird der Baustein *B5.14 Mobile Datenträger* vorgestellt um die Vorgangsweise der Analyse zu veranschaulichen. Dieser Baustein umfasst drei Seiten; begonnen wird mit einer kurzen Beschreibung der unterschiedlichen mobilen Datenträger wie CDs, Magnetbändern, USB-Sticks und ähnlichem. Abbildung 8 zeigt die typischen Gefährdungen für mobile Datenträger. Stellvertretend für alle beschriebenen Gefährdungen ist in Abbildung 9 die Beschreibung der Gefährdung *G5.1 Manipulation/ Zerstörung von IT-Geräten oder Zubehör* abgebildet. Der Baustein enthält auch Informationen über Gegenmaßnahmen, so wird z. B. für den Betrieb die Maßnahme *M3.60 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten* empfohlen.

Höhere Gewalt:

- [G 1.9](#) Datenverlust durch starke Magnetfelder
- [G 1.15](#) Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel:

- [G 2.2](#) Unzureichende Kenntnis über Regelungen
- [G 2.10](#) Nicht fristgerecht verfügbare Datenträger

Menschliche Fehlhandlungen:

- [G 3.1](#) Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- [G 3.3](#) Nichtbeachtung von IT-Sicherheitsmaßnahmen
- [G 3.44](#) Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:

- [G 4.7](#) Defekte Datenträger
- [G 4.52](#) Datenverlust bei mobilem Einsatz

Vorsätzliche Handlungen:

- [G 5.1](#) Manipulation/Zerstörung von IT-Geräten oder Zubehör
- [G 5.2](#) Manipulation an Informationen oder Software
- [G 5.4](#) Diebstahl
- [G 5.9](#) Unberechtigte IT-Nutzung
- [G 5.23](#) Computer-Viren
- [G 5.141](#) Datendiebstahl über mobile Datenträger
- [G 5.142](#) Verbreitung von Schadprogrammen über mobile Datenträger

Abbildung 8 Typische Gefährdungen für mobile Datenträger⁷⁸

⁷⁸ vlg. BSI, 2008c Seite 317

G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, IT-Geräte, Zubehör, Schriftstücke oder ähnliches zu manipulieren oder zu zerstören. Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen, die erhebliche Ausfallzeiten nach sich ziehen können.

Beispiel:

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteil Lüfter mit einem hinter dem Server aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt und der Server fiel für mehrere Tage aus. Hinterher behauptete der Angreifer, dass es sich um ein Versehen handelte.
- Ein Mitarbeiter hat sich über das erneute Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Hierbei wurde durch Fußtritte gegen den Rechner die Festplatte so stark beschädigt, dass sie unbrauchbar wurde. Die hier gespeicherten Daten konnten nur teilweise wieder durch ein entsprechendes Backup vom Vortag rekonstruiert werden.

Abbildung 9 Manipulation/ Zerstörung von IT-Geräten oder Zubehör⁷⁹

5.4 Mehari

Mehari ist eine Risikobewertungsmethode des „Club de la Sécurité de l'Information Français“ (Clusif). Die Methode wurde entwickelt um Chief Information Security Officers (CISOs) beim Risikomanagement zu unterstützen. Sie ermöglicht unter anderem die Erstellung von Sicherheitsplänen (Security Plans), die Erhebung des aktuellen Sicherheitsniveaus, die Implementierung von Sicherheitsrichtlinien (Security Policies) und legt besonderes Augenmerk auf die Durchführung von Risikoanalysen.

Das Framework besteht aus mehreren Modulen (Dokumenten) zur Erhebung des aktuellen Sicherheitsniveaus und zur Durchführung einer Risikoanalyse. Je nach aktuellem Stand des Risikomanagements des Unternehmens, können diese Module beliebig kombiniert werden. Durch den modularen Aufbau ist ein Einsatz in kleinen wie in großen Unternehmen möglich. Mehari bietet Richtlinien für jegliche Art von Risikoanalysen und ist nicht auf die IT-Branche beschränkt.

⁷⁹ vgl. BSI, 2008c Seite 742

Das erste Modul befasst sich mit den vorhandenen Sicherheitsvorkehrungen und ermittelt das Sicherheitsniveau. Dazu kann eine Schnellaufnahme oder eine detaillierte Aufnahme durchgeführt werden⁸⁰. Die Schnellaufnahme versucht herauszufinden, ob Sicherheitsmaßnahmen eingeführt wurden ohne konkrete Risiken zu bekämpfen. Die detaillierte Aufnahme untersucht jede Sicherheitsmaßnahme auf mögliche Schwachstellen. Die Schnellaufnahme kann jederzeit durch die Methoden der detaillierten Aufnahme vertieft werden. Unterstützt wird die detaillierte Methode durch eine kostenlose Wissensdatenbank in Excel-Format⁸¹. Diese Datenbank besteht aus 12 Szenarien, 16 Sicherheitsthemen (von „A1 Roles and Organization“ bis „H1 Incident Management“) und Auditfragebögen für 12 Bereiche. Der Aufbau der Datenbank ist in Abbildung 10 grafisch dargestellt.



Abbildung 10 Bestandteile der MEHARI Wissensdatenbank

Das zweite Modul dient der Bedrohungsanalyse⁸². Um die Vermögenswerte eines Unternehmens schützen zu können, muss bekannt sein, welchen Bedrohungen diese ausgesetzt sind und welche Konsequenzen sich daraus ergeben. Dabei werden Bedrohungen als Ergebnisse von Ereignissen angesehen, welche die Geschäftstätigkeit einer Organisation negativ beeinflussen.

⁸⁰ vgl. Mehari, 2007a Seite 6

⁸¹ vgl. Mehari, 2009

⁸² vgl. Mehari, 2007a

Die Bedrohungsanalyse liefert zwei Ergebnisse⁸³:

- eine Bewertungsskala von Störungen
- eine Klassifizierung von Informationen und IT-Ressourcen

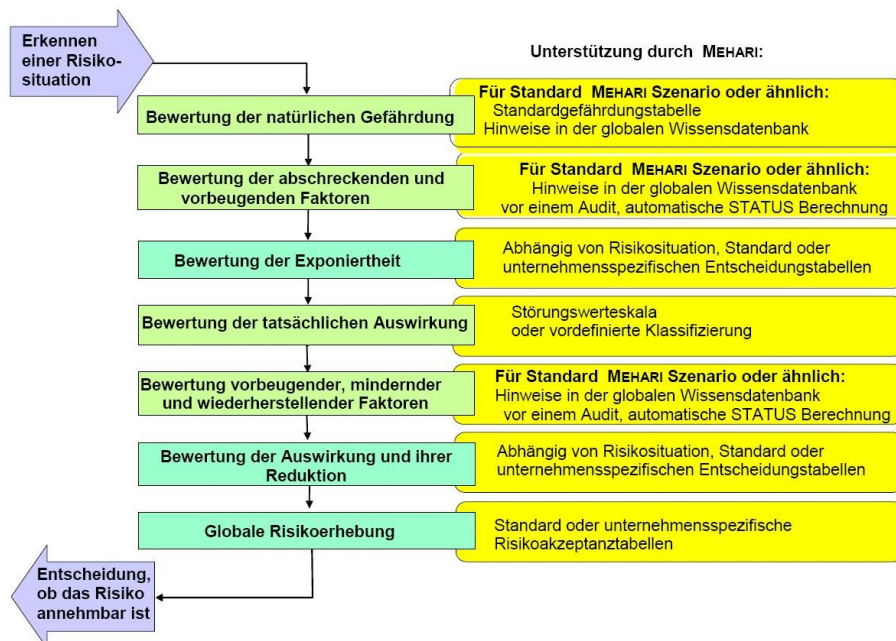
Zur Erstellung der Bewertungsskala werden mögliche Störungen aufgelistet, beeinflussende Parameter definiert und kritische Schwellenwerte für diese Parameter beschrieben. Zur Klassifizierung wird für jeden Typ von Information und für jede IT-Ressource aufgezeigt, was passiert, wenn die Verfügbarkeit, Integrität oder Vertraulichkeit verletzt werden.

Die Bedrohungsanalyse ist Ausgangspunkt für das dritte Modul - die Risikoanalyse. Hier muss zuerst ein Vulnerability Review bzw. ein Sicherheitsaudit erstellt werden, um den Zustand der Sicherheitsmaßnahmen (z. B. Zugriffskontrollen, Virenschutz) in der Organisation zu untersuchen. Die Sicherheitsmaßnahmen werden nach den Kriterien „Effizienz“, „Robustheit“ und „Permanency“ mit den Zahlen „1“ bis „4“ bewertet. Je höher die Zahl ist, desto höher ist der Aufwand, die Sicherheitsmaßnahme zu umgehen. Eine Maßnahme mit der Bewertung „1“ kann von einem Benutzer ohne besondere Kenntnisse umgangen werden, wogegen eine Maßnahme mit der Bewertung „4“ nur von Spezialisten mit besonderen Hilfsmitteln ausgehebelt werden kann.

Das Audit wird mithilfe der zur Verfügung gestellten Fragebögen (siehe Abbildung 10) durchgeführt. Ziel ist es, einen guten Überblick über die Schwachstellen der Organisation zu bekommen. Darauf folgend werden Risikoszenarien erstellt. Die Wissensdatenbank liefert hierfür rund 200 Beispiele. Wenn eine analysierte Situation mit einem Szenario aus der Wissensdatenbank übereinstimmt, können direkt risikominimierende Faktoren erkannt werden.

Abbildung 11 zeigt den Risikoanalyseprozess und die Unterstützung durch Mehari.

⁸³ vgl. Mehari, 2007a

Abbildung 11 Risikoanalyseprozess und Unterstützung durch Mehari⁸⁴

5.4.1 Bewertung der natürlichen Gefährdung

Die Wissensdatenbank (Excel-Tabelle: Expo „Evaluation of the Natural Exposure“) stellt eine ausführliche Liste (~ 50 Einträge) der natürlichen Gefährdung für ein Unternehmen zur Verfügung und gibt einen Standardgefährdungswert vor. Die Risiken werden in „Unfälle“, „Böswilligkeit“, „bewusste, nicht böswillige Aktionen“ und „Fehler“ unterteilt. Abbildung 12 zeigt einen Ausschnitt dieser Wissensdatenbank für den Bereich „Unfälle“.

⁸⁴ vgl. Mehari, 2007d Seite 4

Bewertung der Exponiertheit / des Ereignisspotentials		sehr unwahr-scheinlich	unwahr-scheinlich	wahr-scheinlich	sehr wahr-scheinlich	Status -Expo
Unfälle						
AC01	Kurzschluss: entweder Kabel oder Komponenten		X			2
AC02	Blitzschlag		X			2
AC03	Feuer: interne Ursache: Papierkorb, Aschenbecher, etc.		X			2
AC04	Beeinträchtigung durch Wasser oder Flüssigkeiten (undichte Leitungen, Verschütten, etc.).		X			2
AC05	Überschwemmung wegen Wasserrohrbruch		X			2
AC06	Überschwemmung wegen ansteigendem Wasserspiegel (Fluss, etc.)		X			2
AC07	Überschwemmung durch Löscharbeiten		X			2
AC08	länger dauernde Stromknappheit wegen externen Gründen		X			2
AC09	Nichterreichbarkeit von Gebäuden (Räumen): Zutritt behördlich verboten (Verschmutzung, Streik, Aufruhr, etc.)		X			2
AC10	Verlust von strategischem Personal		X			2
AC11	Verschiedene Geräteausfälle (Energieversorgung, Klimaanlage, etc.)		X			2
AC12	IT oder Telekommunikationsausfälle		X			2
AC13	Ausfall von IT oder Telekommunikationshardware, die nicht durch Wartung gedeckt ist oder der Wartungspartner nicht verfügbar ist.		X			2
AC14	unlösbarer Software deadlock: Entwickler oder Wartungspartner nicht verfügbar		X			2
AC15	ungewollte Auslastung von Ressourcen (CPU, Speicher, Platten, etc.)			X		3
AC16	Datenzerstörung durch Betriebsunfälle			X		3
AC17	Daten oder Konfigurationszerstörung (unbrauchbar) durch einen Virus			X		3
AC18	Verlust von Dateien durch Unfälle in automatisierten Prozessen			X		3
AC19	Verlust von Dateien durch Unfälle wegen Überalterung oder Verschmutzung		X			2
AC20	Verlust von Dateien durch Unfälle wegen Geräteausfällen (dick ersch, etc.)		✓			2

Abbildung 12 Standardgefährdungstabelle⁸⁵

Diese Werte sind erste Anhaltspunkte, dürfen aber nicht unreflektiert übernommen werden. Für eine Firma, welche sehr weit vom nächsten Fluss, See oder Meer entfernt ist, kann die Wahrscheinlichkeit für eine Überschwemmung aufgrund steigender Wasserspiegel (AC06) auch sehr gering sein. Die Wissensdatenbank liefert gute Hinweise auf mögliche Gefahren, muss aber immer an die Gegebenheiten angepasst werden.

5.4.2 Bewertung der tatsächlichen Auswirkungen

Hier werden die Auswirkungen eines Zwischenfalls ohne Rücksichtnahme auf vorhandene Sicherheitsmaßnahmen eruiert. Die Wissensdatenbank liefert Szenarien (Tabellenname: Classif), wobei es für jedes Szenario ein Angriffsziel gibt. Die untersuchten Kriterien sind „Verfügbarkeit“, „Integrität“ und „Verlässlichkeit“. Abbildung 13 zeigt einen Ausschnitt dieser Szenarien.

⁸⁵ vlg. Mahari, 2007d Seite 19

TABELLE DER IMMANENTEN AUSWIRKUNGEN			
Klassifizierungsebenen von Daten, Informationen, Infrastrukturkomponenten			
	A	I	C
Daten und Informationen			
D01 Applikationsdateien oder -datenbanken			
D02 Bürodateien und -daten (im Netzwerk)			
D03 Persönliche Dateien (lokal auf dem PC)			
D04 Geschriebene und gedruckte Informationen und Daten, die von Benutzern verwaltet werden sowie persönliche Archive			
D05 Listen und gedruckte Informationen			
D06 Nachrichten, Bildschirmansichten, etc. (Datenausschnitte)			
D07 Mails und Faxe			
D08 Alte ('ererbte') Archive oder anerkannte Dokumente			
D09 Veröffentlichte oder auf internen Webseiten publizierte Daten und Informationen			
D10 Dateien auf PDAs, etc.			
Infrastruktur: Telekommunikation und Systeme			
R01 WAN Equipment und Leitungen (Netzwerksysteme und -software)			
R02 WAN Equipment und Verkabelung (Netzwerksysteme und -software)			
R03 WAN Konfigurationsdaten			

Abbildung 13 Tabelle der immanenten Auswirkungen⁸⁶

Die Tabelle wird ausgefüllt indem man die Höhe der Konsequenzen bzw. die Auswirkungen auf die Verfügbarkeit, Integrität oder Vertraulichkeit einsetzt. Dies wird durch Werte zwischen „0“ (keine Auswirkung) und „4“ (hohe Auswirkung) angegeben, wobei die grau hinterlegten Kästchen nicht ausgefüllt werden. Da alle weiteren Schritte auf diesen Werten beruhen, sollte diese Tabelle sehr sorgfältig ausgefüllt werden. Die Szenarien können nach eigenem Ermessen erweitert werden. Es wäre beispielsweise möglich, zwischen mehreren Datenbanken zu unterscheiden oder nur die Datenbank, welche für die Durchführung der Geschäftstätigkeit am wichtigsten ist, in die Tabelle aufzunehmen. Dieser Vorgang kann durch die kostenpflichtige Software RisicareTM unterstützt werden.

5.4.3 Risikomindernde Faktoren

Um die erkannten Risiken zu verringern, können abschreckende oder vorbeugende Maßnahmen ergriffen werden. Sollte es zu einem Zwischenfall kommen, dienen schützende, abschwächende und wiederherstellende Aktionen dazu, die Auswirkungen so gering wie möglich zu halten. Die Wissensdatenbank bewertet die Güte der risikomindernden Faktoren durch die Berechnung von Effizienzindikatoren und risikomindernden Faktoren.

Die Effizienz jeder risikomindernden Methode wird folgendermaßen dargestellt (in der Wissensdatenbank werden die ausgeschriebenen englischen Begriffe als Überschrift angegeben):

- EFF-DISS dissuasive = abschreckend
- EFF-PREV preventive = vorbeugend

⁸⁶ vgl. Mehari, 2007d Seite 21

- EFF-PROT protection = schützend
- EFF-PALL palliative = abschwächend
- EFF-RECUP recuperative = wiederherstellend

Die Werte für diese Faktoren finden sich in der Tabelle „Base_scen“ und werden auf zwei Arten angegeben:

- Wenn es sich nur um eine Maßnahme handelt, welche diesen Effekt hat, wird direkt ein Identifikator angegeben, z. B. EFF-PALL = 01C02. Das bedeutet, dass es sich in der Tabelle der immanenten Auswirkungen (Excel-Tabelle „Classif“) um die Auswirkung C02 „Nichteinhaltung von Finanzkontrollen“ handelt, der Präfix „01“ ist die Domänennummer.
- Sind mehrere Maßnahmen für die Effizienz einer risikominimierenden Methode zuständig, wird eine Formel in der Form MIN(arg1, arg2,...) oder MAX(arg1, arg2,...) angegeben. argX steht hierbei für einen Identifikator aus der Wissensdatenbank.

Beispiel: EFF-PREV = MIN(03A01;03A04)

Das bedeutet, dass die Effizienz von der Applikationssoftware, Software-Paketen und Middleware (A01) und von der Benutzer- oder Kundensoftware und Anwendungen (A04) abhängt. Durch die Operation MIN wird angezeigt, dass der geringere Wert der beiden Methoden maßgeblich ist. Methoden, welche durch eine MAX Operation verbunden sind, können als Alternativen angesehen werden.

Anschließend wird ein risikomindernder Faktor für jede der Methoden (DISS, PREV, PROT, PALL, RECUP) berechnet; dieser Faktor wird STATUS plus zugehöriger Methode, z. B. „STATUS-DISS“, genannt. Er setzt sich aus den Werten der Tabelle der immanenten Auswirkungen zusammen und wird auf eine Ganzzahl zwischen „1“ und „4“ auf- bzw. abgerundet. Bei diesen Zahlen handelt es sich um berechnete Werte, das heißt, dass sie nicht auf ein spezielles Unternehmen zugeschnitten sind und deshalb mit Vorsicht zu genießen sind. So können präventive Maßnahmen in einem Unternehmen eine geringere Wirkung haben als in einem anderen.

Der nächste Schritt ist die Bewertung der Exponiertheit (STATUS-EXPO). Es werden drei Standardbewertungstabellen berechnet; eine für Naturereignisse und Unfälle, eine für menschliche Fehler und eine für absichtliche Taten.

Anschließend wird eine Bewertung der Auswirkung durchgeführt. Hierfür werden ein auswirkungsreduzierender Indikator (STATUS-RI) und eine Auswirkungsbewertung (STATUS-I) berechnet. STATUS-RI gibt die Abschwächung der Konsequenzen eines Zwischenfalls an (Excel-Tabelle: I_P Grid). Um den STATUS-RI zu ermitteln, werden drei Tabellen verwendet (siehe Abbildung 14); eine für den Verlust der Verfügbarkeit, eine für den Verlust der Integrität und eine für den Verlust der Vertraulichkeit. Die Bewertungsraster für den STATUS-P für Szenarien ist in die Bereiche „Unfall“, „Fehler“ und „willentliche Aktionen“ unterteilt (siehe Abbildung 15).

1. Szenarien betreffend der Verfügbarkeit (Availability)																			
SCHUTZ=1					SCHUTZ=2					SCHUTZ=3					SCHUTZ=4				
V	4	3	3	3	V	4	3	3	3	V	4	3	3	3	V	4	3	3	3
E	3	2	2	3	E	3	2	2	3	E	3	2	3	3	E	3	3	3	4
R	2	1	2	3	R	2	1	2	3	R	2	1	2	3	R	2	2	3	4
S	1	1	2	3	S	1	1	2	3	S	1	1	2	3	S	1	2	3	4
		1	2	3			1	2	3			1	2	3			1	2	3
R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V
2. Szenarien betreffend der Integrität (Integrity)																			
SCHUTZ=1					SCHUTZ=2					SCHUTZ=3					SCHUTZ=4				
V	4	3	3	3	V	4	3	3	3	V	4	3	3	3	V	4	3	3	4
E	3	2	2	2	E	3	2	2	2	E	3	2	2	2	E	3	2	2	4
R	2	1	1	1	R	2	1	1	1	R	2	1	1	2	R	2	1	2	4
S	1	1	1	1	S	1	1	1	1	S	1	1	1	2	S	1	1	2	4
		1	2	3			1	2	3			1	2	3			1	2	3
R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V
3. Szenarien betreffend der Vertraulichkeit (Confidentiality)																			
SCHUTZ=1					SCHUTZ=2					SCHUTZ=3					SCHUTZ=4				
V	4	3			V	4	3			V	4	3			V	4	3		
E	3	2			E	3	2			E	3	3			E	3	3		
R	2	1			R	2	2			R	2	3			R	2	3		
S	1	1			S	1	2			S	1	3			S	1	3		
		1					1					1					1		
R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V

Abbildung 14 Bewertungsraster für STATUS-RI⁸⁷⁸⁷ vgl. Mehari, 2007d Seite 26

Jeder Raster korrespondiert mit dem gewählten Wert für die gegebene ('natürliche') Exponiertheit (EXPO)

1. Szenarien basierend auf einem Unfall

	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
A				
B				
S				
C 1	1 1 1 1 1	2 2 2 2 1	3 3 2 1	4 4 2 1
H	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	V O R B	V O R B	V O R B	V O R B

2. Szenarien basierend auf einem Fehler

	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
A				
B				
S				
C 1	1 1 1 1 1	2 2 2 2 1	3 3 2 1	4 4 2 1
H	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	V O R B	V O R B	V O R B	V O R B

3. Szenarien basierend auf einer willentlichen Aktion

	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
A 4	1 1 1 1 1	2 1 1 1 1	3 2 1 1	4 3 2 2
B 3	1 1 1 1 1	2 2 1 1	3 2 2 1	4 3 2 2
S 2	1 1 1 1 1	2 2 2 2 1	3 3 2 1	4 4 3 2
C 1	1 1 1 1 1	2 2 2 2 1	3 3 2 1	4 4 3 2
H	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	V O R B	V O R B	V O R B	V O R B

Abbildung 15 Bewertungsraster zu STATUS-P für Szenarien⁸⁸

Um auf STATUS-I, die verbleibende Auswirkung, zu kommen, muss man folgende Formel anwenden: $I = \text{MIN}(\text{tatsächliche Auswirkung}, 5 - \text{STATUS-RI})$. Daraus folgt, dass die maximale Auswirkungshöhe durch den Wert von STATUS-RI begrenzt wird. Ist STATUS-RI gleich „4“ (hohe Auswirkungsminderung), kann die Auswirkung maximal „1“ sein.

Um die Qualität der Ergebnisse zu erhöhen, wird empfohlen, die Beurteilung durch ein Expertenkomitee und automatisch mithilfe der Wissensdatenbank durchzuführen und die Ergebnisse zu vergleichen.

Mehari ist eine Methode, welche sofort umgesetzt werden kann. Sie ist ausreichend konkret und die frei verfügbare Wissensdatenbank enthält alle benötigten

⁸⁸ vgl. Mehari, 2007d Seite 26

Informationen für eine effiziente Risikoanalyse. Der große Nachteil von Mehari ist, dass es relativ lange dauert die verschiedenen Berechnungen zu verstehen und die benötigten Faktoren zu berechnen. Außerdem sollte die Analyse von einem Expertenkomitee und mittels der Datenbank durchgeführt werden. Wenn aber Experten erforderlich sind, ist dies mit Kosten verbunden. Auch sind die Dokumente besonders in Bezug auf die Berechnungen manchmal schwer zu verstehen, was die Einarbeitungszeit verlängert. Kleine und mittlere Unternehmen werden aufgrund der Komplexität und der erforderlichen Experten eher davor zurückschrecken diese Methode anzuwenden.

5.5 OCTAVESM

Die Abkürzung OCTAVE steht für “Operationally Critical Threat, Asset, and Vulnerability Analysis⁸⁹”. Diese Methode wurde an der Carnegie Mellon University entwickelt und alle Informationen stehen kostenlos zur Verfügung. OCTAVE ist ein umfangreicher Ansatz zur Erstellung von Sicherheitsstrategien und richtet sich vor allem an große Unternehmen. Für Unternehmen mit weniger als 100 Mitarbeitern wurde der Ansatz vereinfacht und OCTAVE-S genannt. OCTAVE rückt die Vermögenswerte (Assets) eines Unternehmens in den Mittelpunkt. Ein Asset ist „something of value to the enterprise“⁹⁰. Diese Vermögenswerte können Hardware, Informationen oder Mitarbeiter mit besonderem Wissen sein. Bei OCTAVE-S führt ein drei bis fünf Personen umfassendes so genanntes „analysis team“ die Analyse durch. Da diese Personen einen guten Einblick in das Unternehmen haben müssen, kann von einem einführenden Informationsbeschaffungsprozess, welcher bei OCTAVE erforderlich ist, abgesehen werden. Einer der grundlegendsten Unterschiede zwischen OCTAVE und OCTAVE-S ist die Tiefe des Wissens des analysis teams über die Organisation. Es ist bei OCTAVE-S unerlässlich, dass die Mitarbeiter, welche das analysis team bilden, einen sehr tiefen Einblick in die Organisation haben. Außerdem sollte die Hierarchie flach und die IT-Infrastruktur überschaubar sein.

Die Dokumentation zu OCTAVE-S ist in zehn Volumes unterteilt, wobei Volume 10⁹¹ ein über 200 Seiten starkes Beispiel ist.

Wie OCTAVE ist auch OCTAVE-S in drei Phasen unterteilt⁹²:

- Phase 1: Erstellung Vermögenswerte-basierter Gefahrenprofile
- Phase 2: Identifizierung von Schwachstellen in der Infrastruktur
- Phase 3: Entwicklung eines Sicherheitsstrategieplans

⁸⁹ vgl. Alberts, 2005

⁹⁰ vgl. Hutt 1995

⁹¹ vgl. OCTAVE-S V10, 2005

⁹² vgl. OCTAVE-S V1, 2005 Seite 5f

5.5.1 Phase 1 - Erstellung der Gefahrenprofile

Phase 1 dient der Evaluierung des Unternehmens. Dabei werden die wichtigsten Vermögenswerte (Informationen, Systeme, Applikationen, Personen) und die vorhandenen Sicherheitsprozeduren der Organisation untersucht. Im Gegensatz zu OCTAVE wird diese Evaluierung bei OCTAVE-S ausschließlich vom analysis team und nicht von sehr vielen Mitarbeitern des Unternehmens durchgeführt. Für die kritischen Vermögenswerte werden anschließend Gefahrenprofile erstellt.

Abbildung 16 zeigt die Aktivitäten von Phase 1:

Phase	Process	Activity
Phase 1: Build Asset-Based Threat Profiles	Process S1: Identify Organizational Information	S1.1 Establish Impact Evaluation Criteria
		S1.2 Identify Organizational Assets
		S1.3 Evaluate Organizational Security Practices
	Process S2: Create Threat Profiles	S2.1 Select Critical Assets
		S2.2 Identify Security Requirements for Critical Assets
		S2.3 Identify Threats to Critical Assets

Abbildung 16 Prozesse und Aktivitäten der Phase 1⁹³

Für jeden Prozess und jede Aktivität wird ein Arbeitsblatt zur Verfügung gestellt, welches die Vorgangsweise der Umsetzung erklärt und unterstützt. Abbildung 17 zeigt das Arbeitsblatt für die Aktivität 1.1 „Establish Impact Evaluation Criteria“.

⁹³ vgl. OCTAVE-S Vol.3, 2005 Seite 21

Activity S1.1: Establish Impact Evaluation Criteria		Phase 1, Process S1, Step 1
<u>Activity Worksheets</u> Impact Evaluation Criteria (Vol. 4)		<u>Reference Worksheets</u> none
<u>Background/Definitions</u> Impact – the effect of a threat on an organization’s mission and business objectives Impact value – a qualitative measure of a specific risk’s impact to the organization (high, medium, or low) Impact evaluation criteria – a set of qualitative measures against which each risk’s effect on an organization’s mission and business objectives is evaluated. Impact evaluation criteria define ranges of high, medium, and low impacts for an organization.		
<u>Instructions</u> Step 1 - Define a qualitative set of measures (impact evaluation criteria) against which you will be able to evaluate a risk’s effect on your organization’s mission and business objectives. Document your criteria on the <i>Impact Evaluation Criteria Worksheet</i> (Vol. 4). At a minimum, consider the following impact areas: - reputation/customer confidence - life/health of customers - finances/legal penalties - financial - productivity - other (e.g. Administrative actions such as audits and downsizing) Fill in any blanks in the criteria to make them meaningful to your organization. You can also change the words provided or add additional words as necessary. <i>Note:</i> Within each impact area, there is an option entitled “other” to insert a unique set of criteria. There is also an impact area entitled “other” available for new or unique impact areas. - Cross out any impact areas that do not apply to your organization on the <i>Impact Evaluation Criteria Worksheet</i> (Vol. 4).		

Abbildung 17 Arbeitsblatt für die Aktivität "Establish Impact Evaluation Criteria"⁹⁴

Mithilfe der Arbeitsblätter können nun alle Aktivitäten abgearbeitet werden. Am Ende von Phase 1 sollte für jeden kritischen Vermögenswert ein Gefahrenprofil vorhanden sein. Abbildung 18 zeigt ein Beispiel wobei PIDS (Patient Information Data System) der kritische Vermögenswert ist, und alle Gefahren, welche über einen Netzwerkzugriff möglich sind, aufgelistet, und die Auswirkungen mit L (Low), M (Medium) und H (High) bewertet wurden.

⁹⁴ vgl. OCTAVE-S V3, 2005 Seite 23

Human Actors Using Network Access					Basic Risk Profile						
Step 12					Step 22						
Threat					Impact Values						
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.					What is the potential impact on the organization in each applicable area?						
For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.											
Asset	Access	Actor	Motive	Outcome	Impact Values						
					Reputation	Financial	Productivity	Fines	Safety	Other	
				disclosure	M	M	L	M	L	-	
			accidental	modification	M	M	M	M	H	-	
				loss, destruction	M	M	H	M	H	-	
		inside		interruption	M	M	H	M	H	-	
				disclosure	M	M	L	M	L	-	
			deliberate	modification	M	M	M	M	H	-	
				loss, destruction	M	M	H	M	H	-	
				interruption	M	M	H	M	H	-	
				disclosure	H	H	L	M	L	-	
			accidental	modification	M	M	M	M	H	-	
				loss, destruction	M	M	H	M	H	-	
		outside		interruption	M	M	H	M	H	-	
				disclosure	H	H	L	M	L	-	
			deliberate	modification	M	M	M	M	H	-	
				loss, destruction	M	M	H	M	H	-	
				interruption	M	M	H	M	H	-	

Abbildung 18 Gefahrenprofil für das Patienteninformationssystem (PIDS) bei Zugriff über das Netzwerk⁹⁵

⁹⁵ vgl. OCTAVE-S V10, 2005 Seite 106

5.5.2 Phase 2 - Schwachstellenanalyse

In Phase 2 wird eine Analyse der technischen Infrastruktur des Unternehmens durchgeführt. Dabei wird besonders darauf geachtet, welche Möglichkeiten bestehen, auf kritische Vermögenswerte zuzugreifen. Anschließend werden Klassen von Komponenten abgeleitet und Listen mit den Personen erstellt, die für die Konfiguration und Wartung zuständig sind. Im nächsten Schritt werden die Schwachstellen der identifizierten Komponenten ermittelt. Im Unterschied zu den Aktivitäten S2.3 und S3.1 wird bei Aktivität S3.2 nicht mehr von einer Vermögenswert-Perspektive sondern von einer Infrastruktur-Perspektive ausgegangen. Hier stehen die Infrastruktur und die Prozesse während Konfiguration und Wartung im Vordergrund. Abbildung 19 zeigt die Prozesse und Aktivitäten von Phase 2.

Phase	Process	Activity
Phase 2: Identify Infrastructure Vulnerabilities	Process S3: Examine Computing Infrastructure in Relation to Critical Assets	S3.1 Examine Access Paths
		S3.2 Analyze Technology-Related Processes

Abbildung 19 Prozesse und Aktivitäten von Phase 2⁹⁶

5.5.3 Phase 3 - Sicherheitsstrategieplan

In der dritten und letzten Phase wird eine Schutzstrategie für das Unternehmen und eine Abschwächungsstrategie für die Risiken, welchen die kritischen Vermögenswerte ausgesetzt sind, erstellt. Abbildung 20 zeigt die Aktivitäten dieser Phase.

⁹⁶ vgl. OCTAVE-S V3, 2005 Seite 43

Phase	Process	Activity
Phase 3: Develop Security Strategy and Plans	Process S4: Identify and Analyze Risks	S4.1 Evaluate Impacts of Threats
		S4.2 Establish Probability Evaluation Criteria
		S4.3 Evaluate Probabilities of Threats
	Process S5: Develop Protection Strategy and Mitigation Plans	S5.1 Describe Current Protection Strategy
		S5.2 Select Mitigation Approaches
		S5.3 Develop Risk Mitigation Plans
		S5.4 Identify Changes to Protection Strategy
		S5.5 Identify Next Steps

Abbildung 20 Prozesse und Aktivitäten von Phase 3⁹⁷

Ein wichtiger Bestandteil dieser Phase ist die Evaluierung der Eintrittswahrscheinlichkeiten. Da davon ausgegangen werden muss, dass in kleinen Unternehmen kein Mitarbeiter ausreichendes Wissen und Erfahrung auf diesem Gebiet hat, ist die Bewertung mit Wahrscheinlichkeiten bei OCTAVE-S optional⁹⁸.

Die Ergebnisse der OCTAVE-S Analyse sind eine unternehmensweite Sicherheitsstrategie, eine Abschwächungsstrategie sowie Aktionspläne, welche spezielle Schwachstellen ansprechen. Diese Strategien und Pläne werden dem Management anschließend übergeben.

Bei OCTAVE-S wurde versucht, die hohe Komplexität sowie den hohen Personaleinsatz von OCTAVE zu verringern. Dieses Ziel wurde jedoch nur teilweise erreicht. Es handelt sich immer noch um eine sehr umfassende Analyse und die Durchführung dauert Wochen bis Monate. Das Analyseteam sollte drei bis fünf Personen mit sehr hohem Wissensstand umfassen. In kleinen Unternehmen werden aber gerade diese Mitarbeiter unentbehrlich sein. Für die Erstellung der Zugriffspfade ist sehr hohes technisches Wissen und Erfahrung erforderlich. Ein durchschnittliches kleines oder mittleres Unternehmen wird nur bedingt in der Lage sein, diese Risikoanalyse ohne externe Hilfe durchführen zu können.

5.6 NIST SP800-30

Die 800er Serie der Special Publications (SP) wurde vom „National Institute of Standards and Technology“ (NIST) herausgegeben und beschäftigt sich mit Themen der Computersicherheit. NIST ist eine Dienststelle des U.S. Department of Commerce. Thema der SP800-30 ist das IT-Risikomanagement. Dieses wird in „Risikoanalyse“, „Risikoverringerung“ und „Evaluierung der Ergebnisse“ unterteilt,

⁹⁷ vgl. OCTAVE-S V3, 2005 Seite 59

⁹⁸ vgl. OCTAVE-S V3, 2005 Seite 65

wobei besonderer Wert auf die Beurteilung der Risiken (Risk Assessment) gelegt wird⁹⁹.

Das Risikomanagement wird in den „System Development Life Cycle“ (SDLC) integriert. Dieser Lebenszyklus (siehe Abbildung 21) beschreibt ein Programm von seiner Konzeptionierung bis zur Entsorgung.



Abbildung 21 Software Development Life Cycle

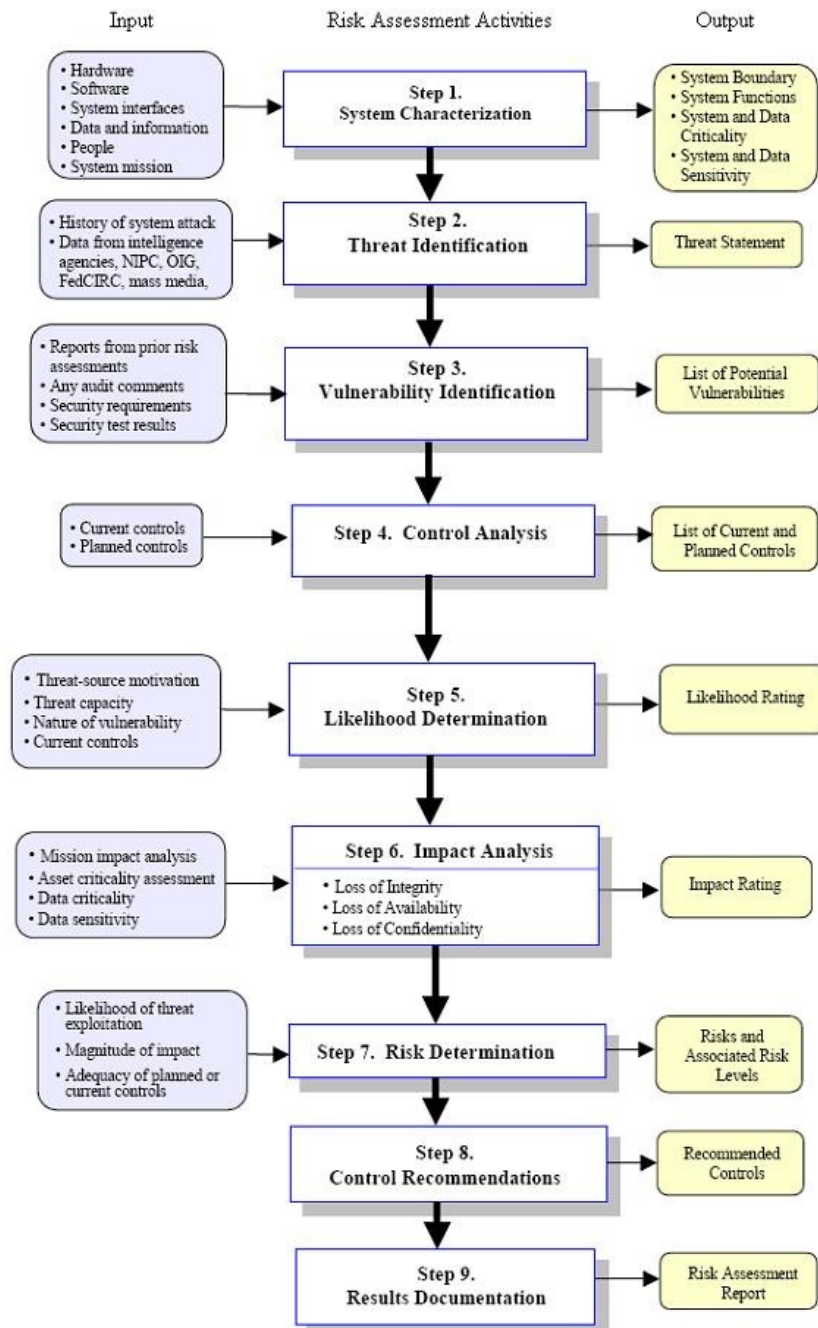
5.6.1 Risikobewertung

Ausgangspunkt für die Bewertung ist die Mission des Unternehmens, das heißt, Risiken sind umso höher zu bewerten, je größer die Wahrscheinlichkeit negativer Auswirkungen auf die Mission eines Unternehmens ist.

Die Risikobewertung wird für alle Komponenten für den gesamten SDLC durchgeführt. Die Auswertung wird immer in Abhängigkeit der Beeinflussung der Mission des Unternehmens betrachtet.

Die Risikobewertung besteht aus neun Schritten (siehe Abbildung 22), wobei die Schritte 2, 3, 4 und 6 nach Abschluss von Schritt 1 parallel ausgeführt werden können.

⁹⁹ vgl. NIST, 2002



¹⁰⁰ vgl. NIST, 2002 Seite 15

5.6.2 System Characterization

Dieser erste Schritt dient dazu, Informationen über das zu beurteilende System zu sammeln. Dabei werden die Grenzen des Systems festgelegt sowie alle beteiligten Ressourcen und Informationen definiert. Um Risiken einschätzen zu können, ist ein gründliches Verständnis des zu beurteilenden Systems unerlässlich. Folgende systemabhängige Informationen müssen in diesem Schritt dokumentiert werden:

- Hardware
- Software
- Interne und externe Verbindungen
- Daten und Informationen
- Wartungspersonal
- Personen, welche das System verwenden
- Zweck des Systems
- Bedeutung des Systems für das Unternehmen
- Anfälligkeit des Systems

Weitere Informationen können nach eigenem Ermessen in die Liste aufgenommen werden (Vorschläge dafür finden sich in [NIST, 2002 Seite 16]).

Befindet sich das System noch in Planung (1. Phase des SDLC), können diese Informationen dem Designplan oder dem Anforderungsdokument entnommen werden. Bei bereits bestehenden Systemen werden die Informationen direkt in der aktuellen Arbeitsumgebung gesammelt. Die Daten umfassen beispielsweise die derzeitige Konfiguration der Hard- und Software sowie die damit durchgeführten Arbeitsabläufe.

Um diese Informationen zu erhalten, werden je nach Entwicklungsstand des Systems Fragebögen, Interviews, Document Reviews (z. B. Systemhandbuch, Designdokument, Auditreport) und der Einsatz von automatischen Scan-Programmen (z. B. Network Mapping Tool) vorgeschlagen. Das Problem beim Einsatz automatischer Scan-Programme ist, dass Standardeinstellungen überprüft werden und die erkannten Schwachstellen vielleicht für das untersuchte System nicht relevant sind. Fragebögen, Interviews und Document Reviews sind zeitaufwändiger und damit teurer, können jedoch auch zu besseren Ergebnissen als automatische Scan-Programme führen.

Am Ende von Schritt 1 sollten die Systemgrenzen klar definiert und die IT-Infrastruktur ausführlich beschrieben sein.

5.6.3 Threat Identification

Eine Gefahrenquelle ist jeder Umstand oder jedes Ereignis, welches das Potential besitzt, die IT-Infrastruktur eines Unternehmens zu beeinträchtigen. Die Gefahrenquellen werden in menschliche (Bedienungsfehler, absichtliche Handlungen), natürliche (Flut, Feuer, Erdbeben) und umweltbezogene (Stromausfall) Gefahren unterteilt.

Da menschliche Gefahren besonders gravierende Auswirkungen für Unternehmen haben können, werden diese noch weiter unterteilt. In diesem Schritt untersucht man die Motivation des Angreifers und die Methoden und Werkzeuge, welche er einsetzen kann, um seinen Angriff durchzuführen. Ein Mitarbeiter kann sich rächen wollen, einfach nur neugierig sein oder Bedienungsfehler begehen. Seine Methoden können beispielsweise Diebstahl, Drohung oder Sabotage sein. Ein Terrorist kann es lediglich auf die Zerstörung der IT-Infrastruktur abgesehen haben und dafür auch Sprengstoff einsetzen.

Am Ende dieses Schrittes sollte ein umfassender Überblick über die Gefahrenquellen vorhanden sein.

5.6.4 Vulnerability Identification

Eine Gefahrenquelle kann ein System nur beeinflussen, wenn Schwachstellen (engl. vulnerabilities) im System vorhanden sind. Die Methode der Identifikation hängt vom Entwicklungsstand des Systems ab. Wurde das System noch nicht entworfen, sollte das Hauptaugenmerk auf bestehende Sicherheitsrichtlinien, Anforderungsdefinitionen und geplante Sicherheitsprozeduren gelegt werden. Ist das System bereits in Verwendung, müssen die Sicherheitseinstellungen und Kontrollmechanismen ebenfalls untersucht werden.

Um Schwachstellen zu identifizieren, können Fragebögen, Interviews, Document Reviews und automatische Scan-Programme verwendet werden. Außerdem sollten die Herstellerhomepages auf bekannte Schwachstellen und Patches untersucht werden. Weitere hilfreiche Quellen zur Identifikation von Schwachstellen sind Dokumente früherer Risikoanalysen und Schwachstellen-Datenbanken. Eine sehr umfangreiche Datenbank ist die National Vulnerability Database (NVD) des NIST¹⁰¹.

Eine effektive aber auch aufwändige Möglichkeit Schwachstellen in bestehenden Systemen aufzuspüren, ist die Durchführung von Tests. Dabei werden Testszenarios erstellt, und überprüft, ob die vorhandenen Vorkehrungen das System im Ernstfall schützen könnten.

Das Ziel der Schwachstellenanalyse ist es, herauszufinden, ob die vorhandenen bzw. geplanten Sicherheitsvorkehrungen ausreichend sind um das Unternehmen im Ernstfall zu schützen. Dazu wird eine Tabelle von Anforderungen und Vorkehrungen erstellt. Die Anforderungen werden in „Management“, „Operational“ und „Technical“ unterteilt.

5.6.5 Control Analysis

Dieser Schritt untersucht vorhandene bzw. geplante Regulierungen, welche die Eintrittswahrscheinlichkeit eines Zwischenfalls verringern sollen. Dabei unterscheidet man technische Vorkehrungen wie Zugriffskontrollen, und operative Vorkehrungen wie Sicherheitsrichtlinien. Das Ergebnis dieses Schrittes ist eine detaillierte Übersicht über die vorhandenen Vorkehrungen.

¹⁰¹ vgl. NVD, 2009

5.6.6 Likelihood Determination

Nun werden die zuvor erkannten Schwachstellen auf ihre Eintrittswahrscheinlichkeit untersucht und diese mit „niedrig“, „mittel“ und „hoch“ klassifiziert. Zu berücksichtigen ist hierbei die Motivation des Angreifers, die Art der Schwachstelle sowie das Bestehen und die Effektivität von Kontrollvorrichtungen.

5.6.7 Impact Analysis

Um zu beurteilen, welchen Effekt ein erfolgreicher Angriff hätte, wird eine Impact Analysis durchgeführt. Dazu muss der Einsatz des Systems, die Wichtigkeit des Systems für das Unternehmen sowie die Art der verarbeitenden Daten berücksichtigt werden. Diese Informationen können von einer vorhandenen Business Impact Analysis bezogen werden oder durch Abschätzung des notwendigen Aufwands für die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit angenähert werden. Je größer der Aufwand ist, desto wichtiger ist das System für das Unternehmen. Dieser Ansatz beschreibt die Auswirkungen ausschließlich qualitativ in den Kategorien „niedrig“, „mittel“ und „hoch“.

Am Ende dieses Schrittes sollten die Auswirkungen erfolgreicher Angriffe qualitativ beschrieben sein.

5.6.8 Risk Determination

Nachdem die Wahrscheinlichkeiten und die Auswirkungen eruiert wurden, kann das Risiko für das IT-System abgeschätzt werden. Dazu werden den Wahrscheinlichkeiten und Auswirkungen Werte zugeordnet. Abbildung 23 zeigt die Risikolevel-Matrix. Risiken mit hoher Eintrittswahrscheinlichkeit und hohen Auswirkungen werden der Matrix zufolge als „High“ bewertet.

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)⁸

Abbildung 23 Risikolevel Matrix¹⁰²

Für Ereignisse mit hohem und mittlerem Gefahrenpotential sollten sofort Gegenmaßnahmen ergriffen werden. Um die Gefahrenlage umfassend zu dokumentieren, müssen auch Gefahren mit niedrigem Schadenspotential vermerkt werden.

5.6.9 Control Recommendations

Nachdem die Gefahren erkannt wurden, können Gegenmaßnahmen ergriffen werden. Dabei ist auf die Kompatibilität, gesetzliche Vorgaben, den Einfluss auf die Organisation und die Zuverlässigkeit zu achten. Diese Vorschläge werden in den Risk Mitigation Process übernommen. In diesem Prozess werden sie evaluiert und implementiert.

5.6.10 Results Documentation

Abschließend wird ein systematischer und analytischer Risikoanalysebericht erstellt und dem Management übergeben. Dieser Report beschreibt die Gefahren und Schwachstellen, liefert eine Einschätzung der Gefahren und empfiehlt Kontrollmechanismen. [NIST, 2002] enthält im Anhang ein Layout für diesen Bericht.

5.7 Vergleich der Ansätze

Nachdem nun sechs Ansätze der Risikoanalyse beschrieben wurden, sollen diese miteinander verglichen werden. Dabei ist bei den qualitativen Kriterien wie „gering“ oder „hoch“ jeweils der Vergleich zu den anderen Methoden gemeint. Wenn eine Beschreibung als abstrakt bezeichnet ist, bedeutet dies, dass keine Implementierungsanweisungen vorhanden sind. Eine als detailliert beschriebene

¹⁰² vgl. NIST, 2002 Seite 31

Methode kann direkt umgesetzt werden. Bei den Referenzen zu weiterführenden Informationen, sind Informationen, welche über den gewählten Ansatz hinausgehen, zu verstehen. Das Österreichische Informationssicherheitshandbuch referenziert beispielsweise auf den IT-Grundschutz, weil die Bausteine für die Umsetzung des Grundschutzansatzes erforderlich sind, es liefert jedoch keine Quellenangaben zu weiterführender Literatur. Als Zielfirmen wurden jene Firmen bezeichnet, bei denen eine Umsetzung der Methode aufgrund finanzieller und personeller Gesichtspunkte am wahrscheinlichsten ist. Dies stimmt nicht immer mit den Angaben der Methode überein. OCTAVE-S richtet sich auch an kleine Unternehmen, wird aber aufgrund des Umfangs nur sehr selten in kleinen Firmen (nach Definition der Europäischen Kommission) angewendet werden können. Der Umfang der Beschreibung der Methode in Seiten liefert nur einen sehr groben Überblick über die Seitenzahl und lässt nur wenige Rückschlüsse über die Komplexität des Verfahrens zu. Die rund 1000 Seiten des OCTAVE-S Ansatzes beinhalten ein über 200-seitiges Beispiel.

	Österreichisches Informations-sicherheitshand-buch	ISO/IEC 27005	IT-Grundschutz	Mehari	OCTAVE-S	NIST SP800-30
Vorgangsweise	von Wahl der Analyse abhängig	Analyse der Vermögenswerte, Bedrohungen, Schwachstellen, Auswirkungen	Modellierung der IT-Infrastruktur, Soll-Ist-Vergleich mit vordefinierten Bausteinen	Feststellung der Sicherheitsvorkehrungen, Bedrohungsanalyse, Risikoanalyse	Analyse der kritischen Vermögenswerte, Zugriffspfadanalyse	Schwachstellenanalyse, Wahrscheinlichkeit des Eintritts, Auswirkungen
Inhaltlicher Schwerpunkt	Informationssicherheit (Risikoanalyse/-management ist nur ein Teil davon)	Etablierung eines Informationssicherheitssystems	Analyse und Modellierung der IT-Infrastruktur	Bedrohungsanalyse mittels Audit und Vulnerability Review	Erstellung von Gefahrenprofilen	Risikobewertung
Risiko-management	ja	ja	ja	nein	ja	ja
Art der Beschreibung	abstrakt	abstrakt	detailliert	detailliert	detailliert	detailliert
Beispiele vorhanden	nein	nein	ja	ja	ja	nein
Vorlagen vorhanden	von Wahl der Analyse abhängig	ja	ja	ja	ja	ja
Zeitlicher Aufwand der RA	von Wahl der Analyse abhängig	hoch	mittel	hoch	hoch	mittel

Finanzieller Aufwand der RA	von Wahl der Analyse abhängig	mittel	mittel	mittel	hoch	gering
Tool Unterstützung	nein	nein	GSTOOL (kostenpflichtig)	Risicare (kostenpflichtig)	nein	nein
Consulting	von Wahl der Analyse abhängig	ja	ja	ja	ja	ja
Benötigte Ressourcen	von Wahl der Analyse abhängig	von Implementierung abhängig	Mitarbeiter, Bausteine, GSTOOL (optional)	Anwender, IT-Mitarbeiter, Wissensdatenbank, Risicare (optional)	3 – 5 Mitarbeiter	Mitarbeiter, Scan-Tool (optional)
Referenzen zu weiterführenden Informationen	nein	Referenzen zu weiteren ISO-Normen	ja	nein	ja	ja
Zielfirmen	klein, mittel, groß	mittel, groß	klein, mittel, groß	mittel, groß	mittel, groß	klein, mittel, groß
Benötigter Wissensstand der Mitarbeiter	von Wahl der Analyse abhängig	mittel	gering	mittel	mittel bis hoch	gering
Umfang der Beschreibung der Methode [Seiten]	350 davon 20 für RA	55	278 (vier Dokumente), exkl. Bausteine	~ 100 (mehrere Dokumente)	~ 1000 (zehn Dokumente) inkl. Beispiel	55
Sprache(n)	Deutsch	Englisch	Deutsch, Englisch	Französisch, Englisch, teilweise Deutsch	Englisch	Englisch
Ursprung	Regierungsstelle	Industrie	Regierungsstelle	Industrie	Industrie	Regierungsstelle
Ursprungsland	Österreich	International	Deutschland	Frankreich	USA	USA

Zertifizierbar	von Wahl der Analyse abhängig	ja	ja	nein	kann als Grundlage für Zertifizierung nach ISO 27005 oder BSI Grundschutz dienen	nein
----------------	----------------------------------	----	----	------	--	------

Tabelle 4 Vergleich der Ansätze

6 Schlussfolgerungen und Empfehlungen für KMU

Jedes Unternehmen - unabhängig von seiner Größe -, welches computergestützte Systeme einsetzt, sollte periodisch IT-Risikoanalysen durchführen. Diese Analysen können dabei helfen, die eigene IT-Infrastruktur besser zu verstehen, Schwachstellen aufzuzeigen und dadurch Risiken besser einschätzen zu können. Wie der Vergleich in Tabelle 4 zeigt, gibt es Unterschiede in der Komplexität, im Umfang, in der Schwerpunktsetzung, im benötigten Wissen der Mitarbeiter und bei den Kosten einer Risikoanalyse. Die richtige Wahl der Analyse ist für den Ausgang und die Akzeptanz durch die Mitarbeiter entscheidend.

Sowohl die Empfehlungen des Österreichischen Sicherheitshandbuches als auch die Empfehlungen der internationalen ISO-Norm 27005 sind sehr abstrakt und können nicht direkt umgesetzt werden. Das Österreichische Sicherheitshandbuch befasst sich sehr umfangreich mit Sicherheitsthemen und beschreibt Risikomanagement nur oberflächlich. Außerdem wird beim Grundschutzansatz häufig auf das BSI verwiesen. Die vom BSI zur Verfügung gestellten Informationen sind umfangreicher und auch mit Beispielen versehen, was bei der Umsetzung sehr hilfreich sein kann. Die ISO-Norm liefert ein sehr gutes und ganzheitliches Konzept und hat den Vorteil, dass die Zertifizierung international anerkannt ist. Da der Ansatz sehr umfangreich ist, die Wahrscheinlichkeiten vom Anwender geschätzt werden müssen und viel Wissen vorausgesetzt wird, eignet sich diese Risikoanalyse nur für einige mittlere und große Unternehmen. Für Kleinst- und Kleinunternehmen ist sie zu aufwändig und dadurch teuer.

Der IT-Grundschutzansatz eignet sich für Unternehmen jeglicher Größe und ist durch seine vorgefertigten Bausteine auch für Nicht-Techniker verständlich. Die Modellierung der IT-Infrastruktur mithilfe der Bausteine ist bei einer überschaubaren Ausstattung relativ einfach. Der anschließende Soll-Ist Vergleich sollte von einem Mitarbeiter mit technischer Ausbildung durchgeführt werden. [BSI, 2008a] liefert ein umfangreiches Beispiel für den Einsatz des Grundschatzes in einer kleinen Institution und [BSI, 2004] enthält ein Beispiel für den Mittelstand. Der Nachteil an dieser Methode ist, dass die Bewertung der Risiken und die Eintrittswahrscheinlichkeiten vorgegeben und deshalb nicht für jedes Unternehmen zutreffend sind. Es besteht jedoch zusätzlich die Möglichkeit, eine Risikoanalyse nach IT-Grundschatz durchzuführen, was aber zu einem erheblich Mehraufwand führt.

Mehari ist mit seinem adaptierbaren Umfang für kleine und mittlere Unternehmen durchaus interessant, beschränkt sich aber lediglich auf die Risikoanalyse. Da jedoch nach der Analyse ein kontinuierliches Risikomanagement unerlässlich ist um die Organisation bestmöglich vor Zwischenfällen zu schützen, muss dies durch eine weitere Methode gewährleistet werden. Die Wissensdatenbank ist sehr hilfreich bei der Erstellung der Risikoanalyse, wird jedoch nicht laufend aktualisiert. Die teilweise schwer verständliche Berechnung der benötigten Werte erschwert die Durchführung dieser Analyse.

OCTAVE-S konzentriert sich sehr stark auf die Zugriffspfade zu kritischen Vermögenswerten. Die Erstellung von Zugriffspfad-Diagrammen erfordert ein hohes Maß an technischem Verständnis, ist arbeitsintensiv und deshalb nur für Firmen mit einer IT-Abteilung interessant. Auch der Einarbeitungsaufwand ist verglichen mit anderen Methoden hoch. Wird jedoch eine Risikoanalyse nach OCTAVE-S durchgeführt, kann dies zu einem sehr hohen Schutz der kritischen Vermögenswerte führen. Außerdem hilft es dabei, den Zugriff auf kritische Vermögenswerte umfassend zu betrachten und dadurch den Wissensstand der Mitarbeiter zu erweitern. Für den Großteil der Kleinst- und Kleinunternehmen ist OCTAVE-S immer noch zu umfangreich und teuer.

Die NIST SP800-30 Methode ist aufgrund der umfangreichen Schwachstellenanalyse und der Abschätzung der Eintrittswahrscheinlichkeiten nur für erfahrenes IT-Personal geeignet. Außerdem sollten für die Einschätzung der Gefahren historische Daten vorhanden sein. Diese Methode kann prinzipiell in jeder Phase des Software-Lebenszyklus verwendet werden und bietet für die einzelnen Phasen Hilfestellungen. Meist wird die Risikoanalyse bei Kleinst- und Kleinunternehmen jedoch nur auf bestehende Systeme angewendet. Leider ist kein durchgängiges Beispiel für die Umsetzung der NIST-Methode vorhanden, was den Einarbeitungsaufwand erhöht.

Kleinst- und Kleinunternehmen, die nicht der IT-Branche zuzurechnen sind, sollten einen Ansatz wählen, bei dem die Einschätzung der Risiken und die Gegenmaßnahmen aus einer Wissensdatenbank (Mehari) oder aus vorgefertigten Bausteinen (IT-Grundschutz) abgelesen werden kann. Dies garantiert zumindest die Abdeckung der bedrohlichsten Gefahren und es können effiziente Gegenmaßnahmen ergriffen werden. Mehari dient jedoch lediglich der Risikoanalyse und muss deshalb mit einem Ansatz zum kontinuierlichen Risikomanagement kombiniert werden. Für mittelgroße Unternehmen könnte eine Zertifizierung nach ISO 2700x oder IT-Grundschutz vorteilhaft sein. Wenn erfahrenes IT-Personal vorhanden ist, trägt die Durchführung einer Analyse nach OCTAVE-S sicher zum besseren Verständnis der IT-Infrastruktur und damit der potentiellen Gefahren bei. Das gleiche gilt für eine Risikoanalyse nach NIST SP800-30.

7 Risikoanalyse für kleine Unternehmen

Ausgehend vom Vergleich der sechs Risikoanalyse-Methoden soll im Folgenden ein neuer Ansatz der Risikoanalyse vorgestellt werden, welcher sich speziell an Kleinst- und Kleinunternehmen richtet. Die österreichische Wirtschaft besteht zu über 82% aus Unternehmen mit weniger als zehn Mitarbeitern und genau dieser Mehrheit an Unternehmen soll hiermit ein Hilfsmittel gegeben werden um die Risiken der verwendeten IT-Geräte abschätzen zu können. Die Methode wurde aus zwei Gründen für diese Unternehmen entwickelt: Erstens bilden sie den Großteil der österreichischen (und der europäischen) Wirtschaft und zweitens sind die vorhandenen Ansätze zu komplex, umfangreich und teuer.

Die Kleinstunternehmen in Österreich sind jedoch keine homogene Gruppe. Sie bestehen zu 4% aus Unternehmen im Primärsektor, zu 16% aus Unternehmen im Sekundärsektor und zu 80% handelt es sich um Dienstleistungsunternehmen (siehe Abbildung 4). In den vielfältigen Branchen, in welchen Kleinstunternehmen vertreten sind, gibt es teilweise unterschiedliche rechtliche Rahmenbedingungen, wie z. B. festgelegte Aufbewahrungspflichten von Patientendaten bei Ärzten. Diese Methode der Risikoanalyse stellt einen generischen Ansatz zur Verfügung und richtet sich somit an alle kleinen Unternehmen. Es ist mit vertretbarem Aufwand nicht möglich, jedes Branchenspezifikum zu berücksichtigen. Daraus folgt, dass jedes Unternehmen, welches diese Methode verwendet, die jeweils für seine Branche geltenden rechtlichen Rahmenbedingungen selbst berücksichtigen muss.

Das Datenschutzgesetz gilt für alle Unternehmen und wurde deshalb in die Methode aufgenommen. Viele Unternehmen speichern und verarbeiten personenbezogene Daten und es ist wichtig, gerade kleinen Unternehmen zu zeigen, wozu sie im Hinblick auf Datenschutz rechtlich verpflichtet sind.

Ziel dieser Methode ist es, Kleinstunternehmen ein Werkzeug in die Hand zu geben um ein Mindestmaß an Sicherheit zu garantieren und dadurch einen positiven Beitrag zum erfolgreichen Weiterbestehen des Unternehmens zu leisten. Firmen, deren Geschäftsprozesse vollkommen von IT-Systemen abhängig sind (z. B. ausschließlicher Online-Vertrieb) sollten eine der in Kapitel 5 vorgestellten Methoden der Risikoanalyse verwenden.

Der Ansatz ist in fünf Punkte gegliedert:

- Unternehmen
- Gefahren
- IT-Infrastruktur
- Datenschutz
- Sicherheitsvorkehrungen

Zur Umsetzung der Methode wurde eine Microsoft Excel Datei entwickelt, welche die Eingabe der Werte erleichtert und die Berechnung der Auswertung durchführt. Der Aufbau dieser Datei ist in Abbildung 24 dargestellt. Das Tabellenblatt „Start“ enthält allgemeine Informationen und zwei Schaltflächen. Eine Schaltfläche heißt

„Start“ und führt zum Arbeitsblatt „Unternehmen“, die andere heißt „Zurücksetzen“ und ermöglicht das Löschen aller eingegebenen Werte. Das Ergebnis der Risikoanalyse wird im Arbeitsblatt „Auswertung“ ausgegeben. Dieses beinhaltet eine Übersicht über die möglichen Gefahren und die berechneten Gefährdungen des Unternehmens durch diese Gefahren. Außerdem werden die Angaben zum Datenschutz und zur IT-Infrastruktur bewertet.

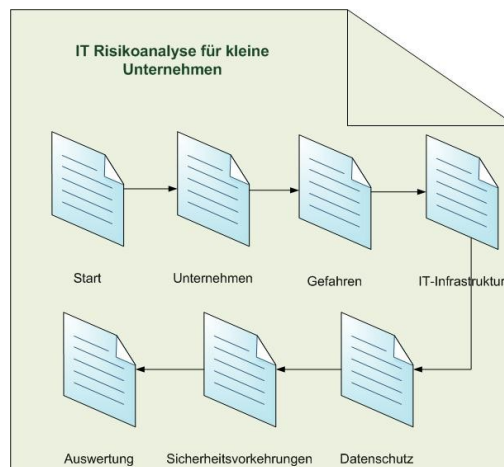


Abbildung 24 Aufbau der Excel Datei

7.1 Theoretische Grundlagen der Methode

Bei der Erstellung dieser Methode wurden Ideen aus den sechs verglichenen Ansätzen herangezogen. Die in Abbildung 6 dargestellten Schritte der Risikoanalyse der ISO-Norm wurden als Referenz verwendet. Die Schritte der ISO-Norm (Asset Identification, Identification of Threats, Identification of Existing Controls, Identification of Vulnerabilities und Identification of Consequences) und die entsprechenden Gegenstücke dieser Methode werden im Folgenden kurz beschrieben.

Die Identifizierung der (IT) Assets wird im Abschnitt IT-Infrastruktur durchgeführt. Normalerweise ist die Identifizierung ein langwieriger Prozess und erfordert die Zusammenarbeit vieler Personen. Bei der hier vorgestellten Methode werden ausschließlich Hardware-Assets berücksichtigt um die Durchführungszeit zu verkürzen. Für jede Komponente (PC, Laptop, Server, mobile Geräte, externe Datenträger) muss der Schutzbedarf für Verfügbarkeit, Integrität und Vertraulichkeit angegeben werden. Je wichtiger Verfügbarkeit, Integrität und Vertraulichkeit für ein Gerät sind, desto wichtiger ist dieses Gerät für das Unternehmen. Für den Schutzbedarf wurden die Eigenschaften Verfügbarkeit, Integrität und Vertraulichkeit gewählt, weil dies auch bei der Mehari-Methode, der NIST SP800-30 Analyse und der ISO-Norm der Fall ist. Außerdem definiert [Avizienis et. al., 2004] Sicherheit als das Vorhandensein von eben diesen Eigenschaften. Ähnlich wie beim

Grundsatzansatz des BSI können auch bei der hier vorgestellten Methode Geräte mit ähnlicher Konfiguration zu Gruppen zusammengefasst werden.

Die Identifizierung der Gefahren erfolgt nicht durch den Anwender. Dieser muss lediglich 15 vordefinierte Gefahren mit ihren Wahrscheinlichkeiten bewerten. Dies entspricht der Vorgehensweise bei der Mehari-Methode. Natürlich kann eine vorgefertigte Liste niemals alle Gefahren abdecken, sie ermöglicht aber auch unerfahrenen Personen, eine Risikoanalyse durchführen zu können. Bei der Bewertung der Wahrscheinlichkeiten sollte der Anwender auf Erfahrungen aus der Vergangenheit zurückgreifen.

Auch die Identifizierung der vorhandenen Sicherheitsvorkehrungen erfolgt durch eine Liste mit insgesamt 34 Einträgen. Der Anwender muss angeben, ob die Sicherheitsvorkehrung derzeit vorhanden ist oder nicht. Außerdem kann er „teilweise“ und „keine Angabe“ wählen, wobei „keine Angabe“ wie ein „nein“ gewertet wird. Auch hier dient die Liste dazu, Personen, die noch nie eine Risikoanalyse durchgeführt haben, die Möglichkeit zu bieten, dies zu tun. Es werden nur vorhandene und keine geplanten Vorkehrungen berücksichtigt, weil diese derzeit keinen risikomindernden Effekt haben und die Durchführungszeit dadurch verkürzt wird.

Die Schwachstellenanalyse wird aufgrund der zuvor gewählten Parameter bei der Auswertung durchgeführt. Dabei werden aus den von der ISO-Norm vorgeschlagenen Bereichen vor allem die Bereiche „Personal“, „Physische Umgebung“, „Konfiguration des Informationssystems“, „Hardware, Software und Kommunikationsausrüstung“ und „Abhängigkeit von externen Akteuren“ berücksichtigt. Die Bereiche „Organisation“, „Prozesse und Prozeduren“ und „Managementroutinen“ können nicht auf einfache Weise durch vordefinierte Listen abgefragt werden und wurden deshalb nicht in die Analyse aufgenommen.

Eine Identifizierung der Konsequenzen wird nicht durchgeführt, weil hierfür die Vermögenswerte (monetär) bewertet werden müssten und dies einige Erfahrung erfordert.

Für die Ermittlung der Übereinstimmung mit dem österreichischen Datenschutzgesetz wurden zwölf Fragen ausgearbeitet, welche die in §14 vorgeschriebenen Sicherheitsvorkehrungen, die Auskunft-, Richtigstellungs- und Löschungspflicht (§26, §27), die Tatsache, dass manuelle Daten auch betroffen sein können, die Bewilligungspflicht bei Übermittlung von Daten ins Ausland und die Meldungspflicht von Datenanwendungen berücksichtigen. Auch diese Liste erhebt keinen Anspruch auf Vollständigkeit, sie umfasst aber sehr wichtige Punkte, welche alle Unternehmen, die personenbezogene Daten verarbeiten, berücksichtigen müssen.

7.2 Die Methode im Überblick

Die fünf Bereiche „Unternehmen“, „Gefahren“, „IT-Infrastruktur“, „Datenschutz“ und „Sicherheitsvorkehrungen“ sollen nun beschrieben werden. Anschließend folgen eine Erklärung der Auswertung und zwei Fallbeispiele.

7.2.1 Unternehmen

Das Arbeitsblatt „Unternehmen“ besteht aus lediglich zwei Fragen, welche beide mit „ja“ oder „nein“ beantwortet werden können. Die erste Frage lautet: „Handelt es sich bei Ihrem Unternehmen um ein Einpersonunternehmen?“ Wird diese Frage mit „ja“ beantwortet, müssen bei der Auswertung alle Fragen, die von Bedrohungen durch Mitarbeiter ausgehen gesondert betrachtet werden. Die zweite Frage lautet: „Haben Sie IT-Dienstleistungen (z. B. Wartungsverträge, Homepage) an andere Unternehmen ausgelagert (Outsourcing)?“ Wird diese Frage mit „nein“ beantwortet, müssen die Fragen, die sich auf Gefahren durch externe Dienstleister beziehen, gesondert betrachtet werden.

7.2.2 Gefahren

Für jede Risikoanalyse ist genaue Kenntnis der Gefahren sowie deren Eintrittswahrscheinlichkeiten erforderlich. Das Identifizieren von Gefahren ist äußerst komplex und für Laien nur schwer möglich. Um ein bestmögliches Ergebnis zu gewährleisten, wurde eine Liste mit 15 Gefahrenquellen (siehe Tabelle 5) zusammengestellt. Der Benutzer muss jede Gefahr mit einer Eintrittswahrscheinlichkeit bewerten, dazu kann „sehr unwahrscheinlich“, „unwahrscheinlich“, „möglich“ und „wahrscheinlich“ gewählt werden. Eine vordefinierte Liste kann selbstverständlich niemals alle Gefahren abdecken, aber es ist eine gute Möglichkeit, zumindest sehr häufige Gefahren aufzuzeigen. Bei den Gefahren 2_1 bis 2_5 handelt es sich um Umweltgefahren. Diesen Gefahren ist prinzipiell jedes Unternehmen ausgesetzt, wobei die Wahrscheinlichkeiten je nach Region sehr stark schwanken können. Die Eintrittswahrscheinlichkeit für Lawinen ist beispielsweise in bergigen Regionen sehr viel höher als im Flachland. Die Gefahren 2_6 bis 2_11 gehören zu den menschlichen Gefahren und die letzten vier Gefahren sind technischer Natur. Der Mensch stellt die bei weitem größte Gefahrenquelle für ein Unternehmen dar, es wird jedoch leider meist zu viel Wert auf technische Gefahren gelegt.

Unter Social Engineering (2_10) versteht man das unbefugte Erfragen von Passwörtern. Es ist bedauerlicherweise oftmals einfacher einen Mitarbeiter anzurufen und nach einem Passwort zu fragen, als dieses zu „knacken“. Dabei gibt sich der Betrüger am Telefon als Vorgesetzter oder Kollege aus und verleitet den Mitarbeiter unter Vortäuschung falscher Tatsachen dazu ihm ein Passwort zu geben. Meist wird vorgetäuscht, dass es sich um einen Notfall und eine einmalige Angelegenheit handelt und dass ohne dieses Passwort etwas Schlimmes passieren werde. Die meisten

Menschen sind hilfsbereit und viele lassen sich dazu verleiten - im Glauben etwas Guten zu tun - ein Passwort weiterzugeben.

Der Verlust von Schlüsselkräften (2_11) kann durch Unfälle, Tod oder Kündigung erfolgen. Wenn dieser Mitarbeiter strategisches Wissen hat (z. B. Root Passwörter), kann dies ein Unternehmen in arge Bedrängnis manövrieren.

Es sind hier nur vier technische Gefahren aufgezählt, die übrigen technischen Gefahren werden im Bereich „IT-Infrastruktur“ abgefragt.

Der Vorteil dieser stark vereinfachten Darstellung der Gefährdungslage ist, dass jeder Durchschnittsbürger diese Gefahren aufgrund seiner persönlichen Erfahrungen einschätzen kann. Außerdem ist somit sichergestellt, dass der Benutzer auch bei einer IT-Risikoanalyse nicht nur technische Gefahren betrachtet.

Nr.	Gefahr
2_1	Feuer
2_2	Wasser/ Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)
2_3	Erdbeben
2_4	Muren/ Lawinen
2_5	Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)
2_6	Sabotage (Zerstörung, Manipulation der IT-Infrastruktur) durch Mitarbeiter
2_7	Spionage (Datendiebstahl) durch Mitarbeiter
2_8	Spionage durch externe Personen
2_9	Vandalismus
2_10	Social Engineering
2_11	Verlust von Schlüsselkräften
2_12	Extern verursachter Ausfall der Internetverbindung
2_13	Fehler durch HW- oder SW-Updates
2_14	Datenverlust aufgrund fehlerhafter Speichermedien
2_15	Durch IT-Dienstleister verursachte Probleme

Tabelle 5 Gefahren für die IT-Infrastruktur

7.2.3 IT-Infrastruktur

Um eine IT-Risikoanalyse sinnvoll durchführen zu können, müssen die einzelnen Komponenten der IT-Infrastruktur bekannt sein und bewertet werden. Manche Ansätze der Risikoanalyse (z. B. OCTAVE) berücksichtigen nur kritische Vermögenswerte. Da die Einteilung in kritische und unkritische Vermögenswerte komplex ist, wurde darauf verzichtet. Wie wichtig eine Komponente ist, wird durch die Angaben zum Schutzbedarf ermittelt. Es werden folgende Komponenten unterschieden:

Nr.	Komponente
-----	------------

3_1	Personal Computer (PC)
3_2	Laptop
3_3	Server
3_4	Mobile Geräte (Handy, Personal Digital Assistant - PDA)
3_5	Externe Datenträger (externe Festplatten, CDs, USB-Sticks)

Tabelle 6 Elemente der IT-Infrastruktur

Mit Personal Computer sind alle Standrechner gemeint; dies sind Geräte bei denen sich sowohl das Gehäuse mit Prozessor, Festplatte und weiteren Komponenten, als auch der Bildschirm am Arbeitsplatz befindet. Laptops sind tragbare Computer, die oft ein besonderes Sicherheitsrisiko darstellen weil sie leicht gestohlen werden können oder verloren gehen. Auch Mobiltelefone und Personal Digital Assistants (PDA) können wichtige Informationen wie Kundendaten oder Kalendereinträge beinhalten und deshalb vor allem für ein kleines Unternehmen sehr wichtig sein. Moderne USB-Sticks können eine Speicherkapazität von mehreren hundert Gigabyte aufweisen und werden immer häufiger als Speichermedium für langfristige Sicherungen benutzt. Aus diesem Grund müssen sie genauso wie CDs und externe Festplatten in einer IT-Risikoanalyse beachtet werden.

Um bei der Auswertung einschätzen zu können wie wichtig ein Gerät für das Unternehmen ist und wie gefährdet es ist, müssen einige Angaben für jedes Gerät ermittelt werden. Um den Aufwand einzuschränken, können gleichartige Geräte, das heißt Geräte mit gleicher Hardware und Software sowie gleicher Art von Netzverbindung, zu Gruppen zusammengefasst werden.

Für jedes Gerät werden folgende Angaben aufgenommen:

- Name
- Netzwerkverbindung
- Internetzugang
- Schutzbedarf - Verfügbarkeit
- Schutzbedarf - Integrität
- Schutzbedarf - Vertraulichkeit

Der Name soll die eindeutige Identifizierung des Geräts sicherstellen. Angaben zur Netzwerkverbindung sind erforderlich, weil Geräte, die sich in einem Netzwerk befinden, zusätzlichen Gefahren ausgesetzt sind. Es wird zwischen „keine Netzwerkverbindung“, „kabelgebunden“ und „kabellos“ unterschieden. Im Gegensatz zur kabelgebundenen Verbindung kann eine kabellose Verbindung auch ohne physischen Zugang zu einem Rechner oder Kabel abgehört werden. Ein weiterer wichtiger Punkt ist der Internetzugang, vor allem Schadsoftware wird häufig über das Internet verteilt. Der Anwender muss zwischen „vorhanden“ und „nicht vorhanden“ wählen. Heutzutage gibt es nur noch wenige Unternehmen, die vollständig auf einen Internetzugang verzichten können.

Beim Schutzbedarf wird zwischen Verfügbarkeit, Integrität und Vertraulichkeit unterschieden. Für jede Eigenschaft muss zwischen „Sehr hoch“, „Hoch“ und

„Gering“ gewählt werden. Handelt es sich um einen Produktionsrechner, auf welchem Betriebsgeheimnisse gespeichert sind, werden alle drei Eigenschaften sehr wichtig sein. Ist es lediglich ein Internetrechner für Recherchen, kann es sein, dass die Verfügbarkeit wichtiger als die Vertraulichkeit ist.

Ausgehend von diesen Daten wird auf die erforderlichen Sicherheitsvorkehrungen geschlossen. Details zur Auswertung werden in Kapitel 7.3 beschrieben.

7.2.4 Datenschutz

Bei der IT-Risikoanalyse soll sichergestellt werden, dass das Unternehmen keine Vorgaben des Datenschutzgesetzes (DSG 2000) verletzt. Es werden nur Tatbestände, bei denen das Unternehmen als Auftraggeber bzw. Dienstleister in Erscheinung tritt, berücksichtigt. Es ist auch hier nicht möglich, anhand einiger Fragen hundertprozentig zu gewährleisten, dass alle Vorgaben des Datenschutzgesetzes eingehalten werden. Dieser Punkt dient vor allem dazu aufzuzeigen, dass es strenge Datenschutzbestimmungen gibt und all diejenigen, die personenbezogene Daten verarbeiten, eine Reihe von Auflagen erfüllen müssen. Jede Frage enthält einen Verweis auf die entsprechende Stelle im Gesetz um dem Anwender das Nachlesen zu erleichtern. Nach Durchsicht des Gesetzes wurden zwölf Fragen formuliert (siehe Tabelle 7). Verarbeitet ein Unternehmen keine personenbezogenen Daten (was sehr selten der Fall sein dürfte), kann dieser Punkt übersprungen werden.

Nr.	Frage
4_1	Ist die Aufgabenverteilung bei der Verwendung personenbezogener Daten zwischen den Mitarbeitern ausdrücklich festgelegt? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".
4_2	Ist die Verwendung personenbezogener Daten an das Vorliegen gültiger Aufträge gebunden? (§14(2))
4_3	Wurde jeder Mitarbeiter über seine Pflichten bezüglich des Datenschutzgesetzes belehrt und kann er die betriebliche Datenschutzvorschrift jederzeit einsehen? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".
4_4	Ist die Zutrittsberechtigung zu ihren Räumlichkeiten klar geregelt? (§14(2))
4_5	Ist die Zutrittsberechtigung zu den Daten und Programmen, welche personenbezogene Daten verarbeiten, klar geregelt? (§14(2))
4_6	Ist eine Berechtigung zum Betrieb der Datenverarbeitungsgeräte erforderlich und ist jedes Gerät durch Vorkehrungen gegen die unbefugte Inbetriebnahme abgesichert? (§14(2))
4_7	Sind Protokolle vorhanden, welche die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) nachvollziehbar machen? (§14(2))
4_8	Ist eine Dokumentation aller Maßnahmen der Fragen 4_1 bis 4_7 vorhanden um die Kontrolle und Beweissicherung zu erleichtern? (§14(2))

4_9	Ist Ihr Unternehmen in der Lage, der Auskunft-, Richtigstellungs- und Löschungspflicht nachzukommen? (§26, §27)
4_10	Ist Ihnen bekannt, dass auch manuelle Dateien (z. B. Karteien, Listen), die nach mindestens einem Suchkriterium (z. B. Name) zugänglich sind, dem Datenschutzgesetz unterliegen? (§1(3))
4_11	Die Übermittlung personenbezogener Daten an Länder außerhalb der EU ist grundsätzlich genehmigungspflichtig (§12, §13). Wurde diese Genehmigung eingeholt? Sollten Sie keine Daten an Länder außerhalb der EU übermitteln, wählen Sie bitte "ja".
4_12	Wurden Ihre meldungspflichtigen Datenanwendungen durch eine Meldung bei der Datenschutzkommission bewilligt? (Nicht meldungspflichtig sind: Rechnungswesen und Logistik, Personalverwaltung, Mitgliederverwaltung, Verwaltung von Benutzerkennzeichen, Kundenbetreuung und Marketing für eigene Zwecke, Patientenverwaltung und Honorarabrechnung, Personentransport und Hotelreservierung, Zutrittskontrollsysteme und KFZ-Zulassung durch beliebige Unternehmen (§17, §19)) Sollten Sie keine meldungspflichtigen Anwendungen verwendet, wählen Sie bitte "ja".

Tabelle 7 Fragen zum Datenschutz

Die Fragen 4_1 bis 4_8 beziehen sich auf §14(2) und zielen darauf ab, die vorgeschriebenen Datensicherheitsmaßnahmen abzufragen. Diese Maßnahmen muss jeder Auftraggeber und Dienstleister unbedingt erfüllen sobald er personenbezogene Daten verwendet.

Jeder Betroffene hat das Recht auf Auskunft (§26) sowie Richtigstellung und Löschung (§27) der ihn betreffenden Daten. Frage 4_9 möchte auf diese Rechte des Betroffenen aufmerksam machen. Um jederzeit in der Lage zu sein, Informationen über die Herkunft der Daten und alle Empfänger bereitstellen zu können, ist eine gewissenhafte und lückenlose Dokumentation erforderlich.

Die Frage 4_10 bezieht sich auf §1(3). Dieser Paragraph besagt, dass auch manuell geführte Dateien dem Datenschutzgesetz unterliegen. Diese Frage wurde aufgenommen, weil es vermutlich nicht jedermann bekannt ist, dass unter Umständen auch Listen und Karteikarten geschützt werden müssen.

Die Frage 4_11 bezieht sich auf die Genehmigungspflicht bei Übermittlung von Daten in Länder außerhalb der EU. Im Zuge der Globalisierung und des Outsourcings steigt die Wahrscheinlichkeit, dass Daten an andere Länder übermittelt werden. Die Frage wurde gewählt um sicherzustellen, dass diese Übermittlungen durch die Datenschutzkommission genehmigt wurden.

Frage 4_12 bezieht sich auf die Meldepflicht des Auftraggebers (§17). Jeder Auftraggeber ist verpflichtet, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission zu erstatten. Diese Meldung muss unter anderem auch die vorhandenen Schutzmaßnahmen umfassen (§19). Nicht meldungspflichtig sind die Verarbeitung öffentlicher oder nur indirekt personenbezogener Daten, die Verarbeitung zu persönlichen oder familiären Zwecken und Standardanwendungen.

Diese zwölf Fragen umfassen sehr wichtige Bereiche des österreichischen Datenschutzgesetzes. Werden alle zwölf Punkte erfüllt, kann davon ausgegangen werden, dass ein durchschnittliches Kleinunternehmen die (meisten) Voraussetzungen ausreichend erfüllt. Alles darüber Hinausgehende sollte von einem Experten geklärt werden.

7.2.5 Sicherheitsvorkehrungen

Dieser Abschnitt umfasst die bereits umgesetzten Sicherheitsvorkehrungen. Jeder Ansatz der Risikoanalyse beinhaltet in irgendeiner Form die Identifizierung der risikomindernden Sicherheitsvorkehrungen. Anders als bei der NIST SP800-30 Methode oder dem Grundsatzansatz des BSI werden jedoch nur realisierte Vorkehrungen beachtet, geplante Vorkehrungen werden nicht berücksichtigt, da sie derzeit keinen risikomindernden Effekt haben. Ausgehend von der Gefährdungslage, welche in den vorhergehenden Punkten abgefragt wurde, kann durch Angaben zu den bereits vorhandenen Sicherheitsvorkehrungen auf das noch bestehende Gefahrenpotential geschlossen werden. In der Auswertung werden die bereits getroffenen Vorkehrungen berücksichtigt und das Gefährdungspotential entsprechend angepasst (Details siehe Kapitel 7.3). Insgesamt werden 34 Sicherheitsvorkehrungen abgefragt. Dabei werden sowohl organisatorische als auch technische Sicherheitsvorkehrungen berücksichtigt.

Nr.	Frage
5_1	Sind Brandschutzeinrichtungen in den Räumen mit IT-Infrastruktur vorhanden und werden diese ordnungsgemäß gewartet?
5_2	Ist sichergestellt, dass in Räumen mit IT-Infrastruktur Wasserleitungen weder in der Decke noch in den Wänden verlaufen?
5_3	Ist sichergestellt, dass sich die IT-Infrastruktur weder im Keller noch direkt unter dem Dach befindet?
5_4	Sind Notfallpläne für die Bewältigung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?
5_5	Sind Schutzeinrichtungen zur Verringerung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?
5_6	Sind die elektrischen Stromkreise durch Sicherungen geschützt und werden diese laufend überprüft?
5_7	Ist ein Notstromaggregat vorhanden?
5_8	Ist der Zutritt in das Unternehmen durch physische Zugangskontrollen (Schlüssel/ Chipkarte) gesichert?
5_9	Sind Richtlinien für den Umgang mit Besuchern/Handwerkern vorhanden?
5_10	Werden Mitarbeiter vor ihrer Einstellung überprüft (Lebensumstände/ finanzielle Lage/ Strafregisterauszug)?
5_11	Ist ein Testsystem für das Testen neuer Hard- und/ oder Software (z. B. Patches) vorhanden?

5_12	Ist das strategische Wissen der Mitarbeiter (kritische Prozesse/ Root-Passwörter) dem Unternehmen im Notfall zugänglich (z. B. Knowledge Management System, Passwortlisten)?
5_13	Verwendet Ihr Unternehmen unterschiedliche Internetanbieter parallel um den Ausfall der Internetverbindung von einem Anbieter kompensieren zu können?
5_14	Erfolgt die Übertragung vertraulicher Daten über unsichere Verbindungen verschlüsselt?
5_15	Werden Speichermedien für die langfristige Speicherung regelmäßig gewartet?
5_16	Ist die Zuständigkeit für die Wartung der IT-Infrastruktur klar geregelt?
5_17	Sind Firewalls auf den Computern/ Laptops und Servern installiert?
5_18	Ist ein Virenschutzprogramm auf den Computern/ Laptops und Servern vorhanden?
5_19	Ist eine Update-Richtlinie für Software (Betriebssystem, Browser, Office, Virenschutz, usw.) vorhanden?
5_20	Ist die WLAN-Verschlüsselung aktiviert?
5_21	Ist eine Passwort-Richtlinie vorhanden und sind alle Mitarbeiter darüber informiert?
5_22	Wird bei Geräten mit Bluetooth ein Passwort verwendet?
5_23	Wurde von den Mitarbeitern eine Benutzerrichtlinie für den richtigen Umgang mit dem Internet unterschrieben?
5_24	Werden RAID (redundante Anordnung unabhängiger Festplatten) Systeme in PCs eingesetzt?
5_25	Werden RAID-Systeme in Servern eingesetzt?
5_26	Werden Backup-Medien in feuerfesten Stahlschränken bzw. außerhalb des Unternehmens aufbewahrt?
5_27	Sind Backup-Lösungen für PCs, Laptops und Server vorhanden?
5_28	Werden Sicherheitsschulungen (Verfügbarkeit/ Integrität/ Vertraulichkeit/ Social Engineering) für die Mitarbeiter angeboten?
5_29	Sind Backup-Lösungen für mobile Geräte und Datenträger (USB-Sticks/ externe Festplatten) vorhanden?
5_30	Sind auf allen Geräten logische Zugangsbeschränkungen (Passwörter/ Rechtevergabe) vorhanden?
5_31	Werden digitale Unterschriften verwendet um Authentizität zu gewährleisten?
5_32	Werden Festplatten in Laptops und externe Datenträger verschlüsselt?
5_33	Werden sensible Daten verschlüsselt um ihren Inhalt zu schützen?
5_34	Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen IT-Dienstleistern klar geregelt?

Tabelle 8 Tabelle der Sicherheitsvorkehrungen

Jede Sicherheitsmaßnahme muss mit „ja“, „teilweise“, „nein“ oder „keine Angabe“ bewertet werden. „Keine Angabe“ sollte vom Benutzer nur dann ausgewählt werden, wenn er sich nicht sicher ist, ob die entsprechende Vorkehrung umgesetzt wurde. Bei der Auswertung wird dies wie ein „nein“ bewertet. Manche Vorkehrungen, wie die parallele Verwendung alternativer Internetanbieter (5_13), scheint vielleicht für viele Fälle übertrieben zu sein, bei der Auswertung wird diese Vorkehrung jedoch nur dann hoch priorisiert, wenn die Gefahr eines Ausfalls der Internetverbindung (Frage 2_12) als „möglich“ oder „wahrscheinlich“ eingestuft wurde. Diese 34 Fragen sind so gewählt, dass sie von einem Laien relativ einfach beantwortet werden können.

7.3 Auswertung

Nachdem alle Eingabewerte kurz beschrieben wurden, wird im Folgenden erklärt, wie daraus die Einschätzung der Gefährdungslage berechnet wird. Die Auswertung erfolgt in Excel mithilfe von Visual Basic for Applications (VBA). Als Eingangsparameter werden die von den Auswahlboxen zur Verfügung gestellten Werte verwendet. Diese Zahlen werden neben der Auswahlbox ausgegeben, sind jedoch in der Schriftfarbe weiß, damit sie bei normaler Verwendung nicht sichtbar sind. Die Auswertung erfolgt, wenn ein Benutzer im letzten Arbeitsblatt („Sicherheitsvorkehrungen“) auf die Schaltfläche „Zur Auswertung“ klickt. Die Ergebnisse der Einschätzung der Gefährdungslage können sein:

- ausreichend geschützt
- geschützt (möglicherweise nicht ausreichend)
- verbesserungsbedürftig
- nicht geschützt

Ist etwas „ausreichend geschützt“, so heißt das, dass es gegen die meisten einfachen, nicht von langer Hand geplanten Angriffe geschützt ist. Da es immer Wege geben wird Sicherheitsvorkehrungen zu umgehen und eine hundertprozentige Sicherheit unrealistisch ist, wurde dieser Wortlaut gewählt. „Geschützt (möglicherweise nicht ausreichend)“ heißt, dass nicht alle empfohlenen Maßnahmen vollständig umgesetzt sind. Ein Angriff kann deshalb mit höherer Wahrscheinlichkeit erfolgreich sein. „Verbesserungsbedürftig“ bedeutet, dass mehr als eine Vorkehrung nicht vollständig umgesetzt wurde oder für eine der empfohlenen Vorkehrungen „keine Angabe“ gewählt wurde. Bei groben Mängeln ist das Ergebnis „nicht geschützt“. Zumindest die Bereiche, welche mit „verbesserungsbedürftig“ oder „nicht geschützt“ beurteilt wurden, sollten rasch überprüft werden.

7.3.1 Bewertung der Gefährdungslage

Die Bewertung erfolgt nach folgendem Schema:

Zuerst werden den Eintrittswahrscheinlichkeiten numerische Werte zugeordnet. In Excel werden dazu die Werte der Auswahlboxen verwendet.

Eintrittswahrscheinlichkeit der Gefahr:

„sehr unwahrscheinlich“	→	1
„unwahrscheinlich“	→	2
„möglich“	→	3
„wahrscheinlich“	→	4

Im nächsten Schritt werden den Sicherheitsvorkehrungen numerische Werte zugeordnet.

Sicherheitsvorkehrung vorhanden:

„ja“	→	1
„teilweise“	→	2
„nein“	→	3
„keine Angabe“	→	4

Je nachdem wie viele Sicherheitsvorkehrungen für eine Gefahr empfohlen werden, ergeben sich unterschiedliche Ausgabewerte (es können bis zu fünf Vorkehrungen pro Gefahr empfohlen sein):

- Eine Sicherheitsvorkehrung

Eintrittswahrscheinlichkeit	Sicherheitsvorkehrung	Ergebnis
1 oder 2	= 1	ausreichend geschützt
1 oder 2	= 2	geschützt (möglicherweise nicht ausreichend)
1 oder 2	= 3	nicht geschützt
3 oder 4	= 1	ausreichend geschützt
3 oder 4	= 2	verbesserungsbedürftig
3 oder 4	= 3	nicht geschützt
1/ 2/ 3/ 4	= 4	verbesserungsbedürftig

Tabelle 9 Auswertung des Schutzstatus' bei einer Sicherheitsvorkehrung

In Abhängigkeit der Eintrittswahrscheinlichkeit der Gefahr und des Status' der Sicherheitsvorkehrung, werden unterschiedliche Ergebnisse ausgegeben. Ist die

Eintrittswahrscheinlichkeit „sehr unwahrscheinlich“ (1) bzw. „unwahrscheinlich“ (2), ist eine teilweise Implementierung der Sicherheitsvorkehrung (2) ausreichend um das Ergebnis „geschützt (möglicherweise nicht ausreichend)“ zu erhalten. Ist die Eintrittswahrscheinlichkeit „möglich“ (3) bzw. „wahrscheinlich“ (4), ist eine teilweise Implementierung nicht mehr ausreichend um dieses Ergebnis zu erzielen. Wurde beim Status der Sicherheitsvorkehrung „keine Angabe“ (4) gewählt ist das Ergebnis unabhängig von der Eintrittswahrscheinlichkeit „verbesserungsbedürftig“.

- Zwei Sicherheitsvorkehrungen

Wenn für eine Gefahr zwei Sicherheitsvorkehrungen relevant sind, werden beide in die Auswertung einbezogen. Tabelle 10 zeigt die Berechnung des Ergebnisses in Abhängigkeit der Eintrittswahrscheinlichkeit und der Summe der beiden Sicherheitsvorkehrungen.

Eintritts- wahrscheinlichkeit	Sicherheitsvorkehrung	Ergebnis
1 oder 2	Summe der beiden Sicherheitsvorkehrungen = 2	ausreichend geschützt
1 oder 2	Summe der beiden Sicherheitsvorkehrungen < 5	geschützt (möglicherweise nicht ausreichend)
1 oder 2	Summe der beiden Sicherheitsvorkehrungen ≥ 5	nicht geschützt
3 oder 4	Summe der beiden Sicherheitsvorkehrungen = 2	ausreichend geschützt
3 oder 4	Summe der beiden Sicherheitsvorkehrungen ≤ 4	geschützt (möglicherweise nicht ausreichend)
3 oder 4	Summe der beiden Sicherheitsvorkehrungen ≥ 5	nicht geschützt
1/ 2/ 3/ 4	eine Vorkehrung = 4	verbesserungsbedürftig

Tabelle 10 Auswertung des Schutzstatus' bei zwei Sicherheitsvorkehrungen

Die Tabelle zeigt, dass die Kriterien bei hohen Eintrittswahrscheinlichkeiten strenger sind als bei niedrigen. Ist eine der Sicherheitsvorkehrungen mit „keine Angabe“ bewertet folgt automatisch das Ergebnis „verbesserungsbedürftig“.

- Drei Sicherheitsvorkehrungen

Wenn für eine Gefahr drei Sicherheitsvorkehrungen relevant sind, werden alle drei in die Auswertung einbezogen. Tabelle 11 zeigt die Berechnung des Ergebnisses in Abhängigkeit der Eintrittswahrscheinlichkeit und der Summe der drei Sicherheitsvorkehrungen.

Eintrittswahrscheinlichkeit	Sicherheitsvorkehrung	Ergebnis
1 oder 2	Summe der drei Sicherheitsvorkehrungen ≤ 4	ausreichend geschützt
1 oder 2	Summe der drei Sicherheitsvorkehrungen > 4 und ≤ 6	geschützt (möglicherweise nicht ausreichend)
1 oder 2	Summe der drei Sicherheitsvorkehrungen $= 7$	verbesserungsbedürftig
1 oder 2	Summe der drei Sicherheitsvorkehrungen > 7	nicht geschützt
3 oder 4	Summe der drei Sicherheitsvorkehrungen $= 3$	ausreichend geschützt
3 oder 4	Summe der drei Sicherheitsvorkehrungen > 3 und ≤ 5	geschützt (möglicherweise nicht ausreichend)
3 oder 4	Summe der drei Sicherheitsvorkehrungen > 5 und ≤ 7	verbesserungsbedürftig
3 oder 4	Summe der drei Sicherheitsvorkehrungen > 7	nicht geschützt
1/ 2/ 3/ 4	eine Vorkehrung $= 4$	verbesserungsbedürftig

Tabelle 11 Auswertung des Schutzstatus' bei drei Sicherheitsvorkehrungen

Die Tabelle zeigt, dass die Kriterien bei hohen Eintrittswahrscheinlichkeiten strenger sind als bei niedrigen. Ist eine Sicherheitsvorkehrung mit „keine Angabe“ bewertet folgt stets das Ergebnis „verbesserungsbedürftig“.

- 4 Sicherheitsvorkehrungen

Eintrittswahrscheinlichkeit	Sicherheitsvorkehrung	Ergebnis
1 oder 2	Summe der vier Sicherheitsvorkehrungen ≤ 6	ausreichend geschützt
1 oder 2	Summe der vier Sicherheitsvorkehrungen > 6 und ≤ 8	geschützt (möglicherweise nicht ausreichend)
1 oder 2	Summe der vier Sicherheitsvorkehrungen > 8 und ≤ 10	verbesserungsbedürftig
1 oder 2	Summe der vier Sicherheitsvorkehrungen > 10	nicht geschützt
3 oder 4	Summe der vier	ausreichend geschützt

	Sicherheitsvorkehrungen ≤ 5	
3 oder 4	Summe der vier Sicherheitsvorkehrungen > 5 und ≤ 7	geschützt (möglicherweise nicht ausreichend)
3 oder 4	Summe der vier Sicherheitsvorkehrungen > 7 und ≤ 9	verbesserungsbedürftig
3 oder 4	Summe der vier Sicherheitsvorkehrungen > 9	nicht geschützt
1/ 2/ 3/ 4	eine Vorkehrung = 4	verbesserungsbedürftig

Tabelle 12 Auswertung des Schutzstatus' bei vier Sicherheitsvorkehrungen

- 5 Sicherheitsvorkehrungen

Eintritts-wahrscheinlichkeit	Sicherheitsvorkehrung	Ergebnis
1 oder 2	Summe der fünf Sicherheitsvorkehrungen ≤ 7	ausreichend geschützt
1 oder 2	Summe der fünf Sicherheitsvorkehrungen > 7 und ≤ 9	geschützt (möglicherweise nicht ausreichend)
1 oder 2	Summe der fünf Sicherheitsvorkehrungen > 9 und ≤ 11	verbesserungsbedürftig
1 oder 2	Summe der fünf Sicherheitsvorkehrungen > 11	nicht geschützt
3 oder 4	Summe der fünf Sicherheitsvorkehrungen ≤ 6	ausreichend geschützt
3 oder 4	Summe der fünf Sicherheitsvorkehrungen > 6 und ≤ 8	geschützt (möglicherweise nicht ausreichend)
3 oder 4	Summe der fünf Sicherheitsvorkehrungen > 8 und ≤ 10	verbesserungsbedürftig
3 oder 4	Summe der fünf Sicherheitsvorkehrungen > 10	nicht geschützt
1/ 2/ 3/ 4	eine Vorkehrung = 4	verbesserungsbedürftig

Tabelle 13 Auswertung des Schutzstatus' bei fünf Sicherheitsvorkehrungen

Die Ausgabe dieser Auswertung erfolgt in Excel auf dem Auswertungsblatt. Um die Ergebnisse schnell erfassen zu können, werden diese farblich hervorgehoben.

„ausreichend geschützt“ wird grün, „geschützt (möglicherweise nicht ausreichend)“ gelb, „verbesserungsbedürftig“ orange und „nicht geschützt“ rot ausgegeben.

7.3.2 Unternehmen

Wenn es sich beim untersuchten Unternehmen um ein Einpersonenunternehmen handelt, werden die Gefahren 2_6 (Sabotage durch Mitarbeiter), 2_7 (Spionage durch Mitarbeiter), 2_10 (Social Engineering) und 2_11 (Verlust von Schlüsselkräften) mit „irrelevant, weil Einpersonenunternehmen“ bewertet. Da Einpersonenunternehmen keine Mitarbeiter beschäftigen, geht von den oben genannten Gefahren keine Bedrohung aus.

Wird die Frage nach den IT-Dienstleistern mit „nein“ beantwortet, wird die Frage 5_34 (Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen IT-Dienstleistern klar geregelt?) bei der Auswertung zur Gefahr 2_15 (Durch IT-Dienstleister verursachte Probleme) nicht berücksichtigt und als Ergebnis „keine externen IT-Dienstleister vorhanden“ ausgegeben.

7.3.3 Gefahren

Für jede der genannten Gefahren gibt es Vorkehrungen, die diese minimieren können. Die folgende Tabelle zeigt den Zusammenhang zwischen Gefahren und Sicherheitsvorkehrungen. Die Werte in der Spalte „Sicherheitsvorkehrung“ beziehen sich auf Vorkehrungen, welche in Tabelle 8 nachgeschlagen werden können. Aus der nachstehenden Tabelle kann auch abgelesen werden, ob ein, zwei, drei oder vier Sicherheitsvorkehrungen für eine Gefahr vorgeschlagen werden.

Nr.	Gefahr	Sicherheitsvorkehrung
2_1	Feuer	5_1
2_2	Wasser/ Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	5_2 5_3
2_3	Erdbeben	5_4 5_5
2_4	Muren/ Lawinen	5_4 5_5
2_5	Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)	5_6 5_7
2_6	Sabotage (Zerstörung, Manipulation der IT-Infrastruktur) durch Mitarbeiter	5_8 5_10
2_7	Spionage (Datendiebstahl) durch Mitarbeiter	5_8 5_10
2_8	Spionage durch externe Personen	5_8 5_9 5_14

		5_30
2_9	Vandalismus	5_8 5_10
2_10	Social Engineering	5_28
2_11	Verlust von Schlüsselkräften	5_12
2_12	Extern verursachter Ausfall der Internetverbindung	5_13
2_13	Fehler durch HW- oder SW-Updates	5_11
2_14	Datenverlust aufgrund fehlerhafter Speichermedien	5_15 5_16
2_15	Durch IT-Dienstleister verursachte Probleme	5_34

Tabelle 14 Auswertung der möglichen Gefahrenquellen

7.3.4 IT-Infrastruktur

Die Bewertung der Gefahren für die einzelnen verwendeten Geräte ist für die IT-Risikoanalyse besonders wichtig. In der unten angeführten Tabelle sind die Geräte (PCs, Laptops, Server, mobile Geräte und externe Datenträger) horizontal und die Eigenschaften dieser Geräte vertikal aufgelistet. In jeder Zeile werden die für das jeweilige Gerät erforderlichen Sicherheitsvorkehrungen in der Form 5_xx angegeben. Die zugehörigen Sicherheitsvorkehrungen können in Tabelle 8 nachgelesen werden. Ist für einen Gerätetyp eine Sicherheitsvorkehrung nicht sinnvoll (z. B. Internetzugang bei externen Datenträgern) oder sind keine Sicherheitsvorkehrungen erforderlich (weil z. B. kein Internetzugang vorhanden ist), ist diese Zelle mit einem „X“ markiert.

Nr.	Spaltenname	Unterteilung	Beschreibung	PC	Server	Laptop	Mobile Geräte	Externe Datenträger
1	Name		Name des Geräts/ der Gerätegruppe					
2	Netzwerkverbindung		Art der Netzwerkverbindung, falls vorhanden					
21		keine	keine Netzwerkverbindung vorhanden	X	X	X	X	X
22		kabelgebunden	Die Netzwerkverbindung wird über Kabel hergestellt.	5_17 5_18 5_19	5_17 5_18 5_19	5_17 5_18 5_19	X	X
23		kabellos	Es besteht eine kabellose Internetverbindung (WLAN).	5_17 5_18 5_19 5_20 5_21	5_17 5_18 5_19 5_20 5_21	5_17 5_18 5_19 5_20 5_21	5_20 5_21 5_22	X
3	Internetzugang		Ist das Gerät mit dem Internet verbunden?					
31		ja	Das Gerät ist mit dem Internet verbunden.	5_17 5_18 5_19 5_23 5_28	5_17 5_18 5_19 5_23 5_28	5_17 5_18 5_19 5_23 5_28	5_19 5_23	X
32		nein	Das Gerät verfügt über keinen Zugang	X	X	X	X	X

			zum Internet.					
4	Anforderung an die Verfügbarkeit		Wie wichtig ist es, ob Geräte verfügbar sind?					
41		sehr hoch	Die Verzichtbarkeit liegt im Bereich von Minuten.	5_14 5_24 5_26 5_28	5_14 5_25 5_26 5_28	5_14 5_26 5_28	5_28 5_29	5_28 5_29
42		hoch	Die Verzichtbarkeit liegt im Bereich von Stunden.	5_14 5_27 5_28	5_14 5_27 5_28	5_14 5_27 5_28	5_28 5_29	5_28 5_29
43		gering	Die Verzichtbarkeit liegt im Bereich von Tagen.	5_27	5_27	5_27	5_29	5_29
45	Anforderung an die Integrität		Wie wichtig ist es, ob die Daten nicht verändert werden?					
51		sehr hoch	Falsche Daten können die Existenz des Unternehmens bedrohen.	5_8 5_21 5_28 5_30 5_31	5_8 5_21 5_28 5_30 5_31	5_21 5_28 5_30 5_31 5_32	5_21 5_28 5_30 5_31 5_33	5_28 5_31 5_32
52		hoch	Falsche Daten können zu finanziellen Einbußen führen.	5_21 5_28 5_31	5_21 5_28 5_31	5_21 5_28 5_30 5_31	5_21 5_28 5_30 5_31	5_28 5_33
53		gering	Falsche Daten haben nur geringe	5_21 5_30	5_21 5_30	5_21 5_30	5_21 5_30	5_28

			Auswirkungen auf das Unternehmen.					
6	Anforderung an die Vertraulichkeit		Wie wichtig ist es, ob die Daten in die falschen Hände geraten?					
61		sehr hoch	Wenn die Daten in falsche Hände geraten, kann dies die Existenz des Unternehmens gefährden.	5_8 5_14 5_21 5_30 5_33	5_8 5_14 5_21 5_30 5_33	5_14 5_21 5_30 5_33	5_21 5_28 5_30 5_33	5_21 5_28 5_30 5_33
62		hoch	Wenn die Daten in falsche Hände geraten, kann dies zu finanziellen Einbußen führen.	5_14 5_21 5_30 5_33	5_14 5_21 5_30 5_33	5_14 5_21 5_30 5_33	5_21 5_28 5_30 5_33	5_21 5_28 5_30 5_33
63		gering	Wenn die Daten in falsche Hände geraten, kann dies nur zu geringem Schaden führen.	5_21 5_30	5_21 5_30	5_21 5_30	5_21 5_30	5_21 5_30

Tabelle 15 Tabelle der IT-Infrastruktur und der erforderlichen Sicherheitsvorkehrungen

Die Tabelle zeigt, dass „sehr hohe“ und „hohe“ Anforderungen an die Eigenschaften des Schutzbedarfs mit mehr Sicherheitsvorkehrungen verbunden sind als „geringe“ Anforderungen. Aber auch bei geringen Anforderungen sollten einige Vorkehrungen getroffen werden. Beispielsweise sollten bei geringen Anforderungen an die Vertraulichkeit trotzdem logische Zugangskontrollen (5_30) und Passwort-Richtlinien (5_21) vorhanden sein. Um die Gefährdungslage für jedes Gerät zu erhalten, werden ebenfalls die in 7.3.1 beschriebenen Berechnungen vorgenommen. Es können zwischen einem und fünf Eingangsparameter für die Berechnung vorhanden sein.

Das Arbeitsblatt enthält in der Beschreibung Hilfestellungen für die Bewertung des Schutzbedarfs. Dadurch soll es Anwendern erleichtert werden, die Begriffe Verfügbarkeit, Integrität und Vertraulichkeit besser zu verstehen.

7.3.5 Datenschutz

Da alle Datenschutzbestimmungen einzuhalten sind, wird bei der Auswertung nur überprüft, ob alle zwölf Fragen (siehe Tabelle 7) mit „ja“ beantwortet wurden. Ist dies der Fall, erscheint am Auswertungsblatt folgende Anmerkung: „Ihr Unternehmen scheint die Datenschutzbestimmungen in ausreichendem Umfang umgesetzt zu haben.“ Sollte auch nur eine Frage mit „teilweise“ oder „nein“ beantwortet worden sein, erscheint folgende Anmerkung: „Ihr Datenschutz scheint mangelhaft zu sein, eine Überprüfung durch einen Experten wäre vorteilhaft um sicherzustellen, dass keine Bestimmung des Datenschutzgesetzes verletzt wird.“

Sollte ein Unternehmen keine personenbezogenen Daten verarbeiten und die Fragen nicht ausfüllen, erscheint: „Da Sie die Fragen zum Datenschutz nicht ausgefüllt haben, verarbeitet Ihr Unternehmen anscheinend keine personenbezogenen Daten.“

7.3.6 Sicherheitsvorkehrungen

Die folgende Tabelle zeigt die bereits aus Tabelle 8 bekannten Fragen zu den Sicherheitsvorkehrungen und in der Spalte „Zugehörige Gefahr(en)“ die damit assoziierten Gefahren für das Unternehmen. Die in der Form „2_x“ angegebenen Gefahren sind die in Tabelle 5 angeführten Gefahren für das Unternehmen wie beispielsweise Feuer (2_1) oder Vandalismus (2_9). Die restlichen Gefahren sind mit „xx_PC“, „xx_Server“, „xx_Laptop“, „xx_Mob“ und „xx_Datenträger“ gekennzeichnet. Sie beziehen sich auf Gefahren für die IT-Infrastruktur und können in Tabelle 15 nachgeschlagen werden.

Nr.	Frage	Zugehörige Gefahr(en)
5_1	Sind Brandschutzeinrichtungen in den Räumen mit IT-Infrastruktur vorhanden und werden diese ordnungsgemäß gewartet?	2_1

5_2	Ist sichergestellt, dass in Räumen mit IT-Infrastruktur Wasserleitungen weder in der Decke noch in den Wänden verlaufen?	2_2
5_3	Ist sichergestellt, dass sich die IT-Infrastruktur weder im Keller noch direkt unter dem Dach befindet?	2_2
5_4	Sind Notfallpläne für die Bewältigung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	2_3 2_4
5_5	Sind Schutzeinrichtungen zur Verringerung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	2_3 2_4
5_6	Sind die elektrischen Stromkreise durch Sicherungen geschützt und werden diese laufend überprüft?	2_5
5_7	Ist ein Notstromaggregat vorhanden?	2_5
5_8	Ist der Zutritt in das Unternehmen durch physische Zugangskontrollen (Schlüssel/ Chipkarte) gesichert?	2_6 2_7 2_8 2_9 51_PC 51_Server
5_9	Sind Richtlinien für den Umgang mit Besuchern/ Handwerkern vorhanden?	2_7 2_8
5_10	Werden Mitarbeiter vor ihrer Einstellung überprüft (Lebensumstände/ finanzielle Lage/ Strafregisterauszug)?	2_6 2_7 2_9
5_11	Ist ein Testsystem für das Testen neuer Hard- und/ oder Software (z. B. Patches) vorhanden?	2_13
5_12	Ist das strategische Wissen der Mitarbeiter (kritische Prozesse/ Root-Passwörter) dem Unternehmen im Notfall zugänglich (z. B. Knowledge Management System, Passwortlisten)?	2_11
5_13	Verwendet Ihr Unternehmen unterschiedliche Internetanbieter parallel um den Ausfall der Internetverbindung von einem Anbieter kompensieren zu können?	2_12
5_14	Erfolgt die Übertragung vertraulicher Daten über unsichere Verbindungen verschlüsselt?	2_8 61_PC 61_Server 61_Laptop 62_PC 62_Server

		62_Laptop
5_15	Werden Speichermedien für die langfristige Speicherung regelmäßig gewartet?	2_14
5_16	Ist die Zuständigkeit für die Wartung der IT-Infrastruktur klar geregelt?	2_16
5_17	Sind Firewalls auf den Computern/ Laptops und Servern installiert?	22_PC 23_PC 22_Server 23_Server 22_Laptop 23_Laptop 31_PC 31_Server 31_Laptop
5_18	Ist ein Virenschutzprogramm auf den Computern/ Laptops und Server vorhanden?	22_PC 23_PC 22_Server 23_Server 22_Laptop 23_Laptop 31_PC 31_Server 31_Laptop
5_19	Ist eine Update-Richtlinie für Software (Betriebssystem, Browser, Office, Virenschutz, usw.) vorhanden?	22_PC 23_PC 22_Server 23_Server 22_Laptop 23_Laptop 31_PC 31_Server 31_Laptop 31_Mob
5_20	Ist die WLAN-Verschlüsselung aktiviert?	23_PC 23_Server 23_Laptop 23_Mob
5_21	Ist eine Passwort-Richtlinie vorhanden und sind alle Mitarbeiter darüber informiert?	23_PC 23_Server

		23_Laptop 23_Mob 51_PC 52_PC 53_PC 51_Server 52_Server 53_Server 51_Laptop 52_Laptop 53_Laptop 51_Mob 52_Mob 53_Mob 51_Datenträger 52_Datenträger 61_PC 62_PC 63_PC 61_Server 62_Server 63_Server 61_Laptop 62_Laptop 63_Laptop 61_Mob 62_Mob 63_Mob 61_Datenträger 62_Datenträger
5_22	Wird bei Geräten mit Bluetooth ein Passwort verwendet?	23_Mob
5_23	Wurde von den Mitarbeitern eine Benutzerrichtlinie für den richtigen Umgang mit dem Internet unterschrieben?	31_PC 31_Server 31_Laptop 31_Mob 31_Datenträger
5_24	Werden RAID (redundante Anordnung unabhängiger Festplatten) Systeme in PCs eingesetzt?	41_PC 42_PC
5_25	Werden RAID-Systeme in Servern eingesetzt?	41_Server

		42_Server
5_26	Werden Backup-Medien in feuerfesten Stahlschränken bzw. außerhalb des Unternehmens aufbewahrt?	41_PC 41_Server 41_Laptop 41_Mob 41_Datenträger
5_27	Sind Backup-Lösungen für PCs, Laptops und Server vorhanden?	82_PC 83_PC 82_Server 83_Server 82_Laptop 83_Laptop
5_28	Werden Sicherheitsschulungen (Verfügbarkeit/ Integrität/ Vertraulichkeit/ Social Engineering) für die Mitarbeiter angeboten?	2_10 41_PC 41_Server 41_Laptop 41_Mob 41_Datenträger 42_PC 42_Server 42_Laptop 42_Mob 42_Datenträger 51_PC 51_Server 51_Laptop 51_Mob 51_Datenträger 52_PC 52_Server 52_Laptop 52_Mob 52_Datenträger 53_Datenträger 62_PC 62_Server 62_Laptop 62_Mob 62_Datenträger
5_29	Sind Backup-Lösungen für mobile Geräte und	41_Mob

	Datenträger (USB-Sticks/ externe Festplatten) vorhanden?	42_Mob 43_Mob 41_Datenträger 42_Dateträger 43_Datenträger
5_30	Sind auf allen Geräten logische Zugangsbeschränkungen (Passwörter/ Rechtevergabe) vorhanden?	51_PC 51_Server 51_Laptop 51_Mob 51_Datenträger 52_PC 52_Server 52_Laptop 52_Mob 52_Datenträger 53_PC 53_Server 53_Laptop 53_Mob 53_Datenträger 61_PC 61_Server 61_Laptop 61_Mob 61_Datenträger 62_PC 62_Server 62_Laptop 62_Mob 62_Datenträger 63_PC 63_Server 63_Laptop 63_Mob 63_Datenträger
5_31	Werden digitale Unterschriften verwendet um Authentizität zu gewährleisten?	51_PC 51_Server 51_Laptop 51_Mob 51_Datenträger

		52_Laptop 52_Mob
5_32	Werden Festplatten in Laptops und externe Datenträger verschlüsselt?	51_Laptop 51_Datenträger
5_33	Werden sensible Daten verschlüsselt um ihren Inhalt zu schützen?	61_PC 61_Server 61_Laptop 61_Mob 61_Datenträger 62_PC 62_Server 62_Laptop 62_Mob 62_Datenträger
5_34	Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen IT-Dienstleistern klar geregelt?	2_15

Tabelle 16 Sicherheitsvorkehrungen inklusive zugehöriger Gefahr(en)

7.4 Erweiterung der Methode

Da sich die Gefährdungslage in der Informationstechnologie schnell ändert und neue Technologien neuen Gefahren ausgesetzt sind, soll kurz beschrieben werden wie neue Gefahren und Sicherheitsvorkehrungen in die Analyse einbezogen werden können. Als Beispiel wurden die Gefahren, welche von einer Infrarotschnittstelle ausgehen, gewählt. Vor allem Laptops besitzen häufig Infrarotschnittstellen um mit externen Geräten wie Mobiltelefonen oder PDAs zu kommunizieren. Es gibt bei Infrarotschnittstellen keine Authentifizierung und keine Verschlüsselung, was bedeutet, dass jedes sich in Reichweite befindliche Gerät eine Verbindung aufbauen kann, wenn die Schnittstelle aktiviert ist. Am besten wird diese Gefahr gebannt indem die Schnittstelle nach jedem Gebrauch deaktiviert wird.

Die hinzuzufügende Gefahr lautet: „Gefahren durch integrierte Infrarotschnittstellen.“ Die neue Sicherheitsvorkehrung lautet: „Werden Infrarotschnittstellen nach jedem Gebrauch deaktiviert?“

Der erste Schritt ist das Hinzufügen der Gefahr im Arbeitsblatt „Gefahren“.

Durch IT Dienstleister verursachte Probleme		
Gefahren durch integrierte Infrarotschnittstellen	möglich	3

Fertig

Abbildung 25 Hinzufügen einer neuen Gefahr

Wie in Abbildung 25 ersichtlich, wurde die Frage, die Auswahlbox und das Kommentarfenster hinzugefügt. Abbildung 26 zeigt die Einstellungen der Auswahlbox. Der Eingabebereich ist immer gleich, er definiert die im drop-down-Menü verfügbaren Auswahlmöglichkeiten; die Zellverknüpfung entspricht der Zeile in der die Gefahr steht. Durch die Zellverknüpfung wird rechts neben der Auswahlbox die zur Auswahl korrespondierende Nummer ausgegeben (in Abbildung 25 ist dies „3“ für die Auswahl „möglich“). Um die Ausgabe unsichtbar zu machen, kann die Schriftfarbe auf weiß gesetzt werden.

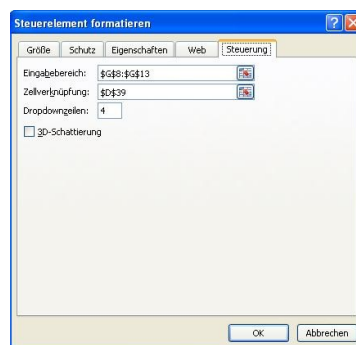


Abbildung 26 Konfiguration der Auswahlbox „Gefahren“

Im nächsten Schritt muss die Sicherheitsvorkehrung im Arbeitsblatt „Sicherheitsvorkehrungen“ angegeben werden (siehe Abbildung 27). Die Konfiguration der Auswahlbox ist in Abbildung 28 zu sehen.

Sind die Verantwortlichkeiten/Zuständigkeiten zwischen Ihnen und Ihren externen IT Dienstleistern klar geregelt?

Werden Infrarotschnittstellen nach jedem Gebrauch deaktiviert?

Zur Auswertung

Abbildung 27 Hinzufügen einer neuen Sicherheitsvorkehrung

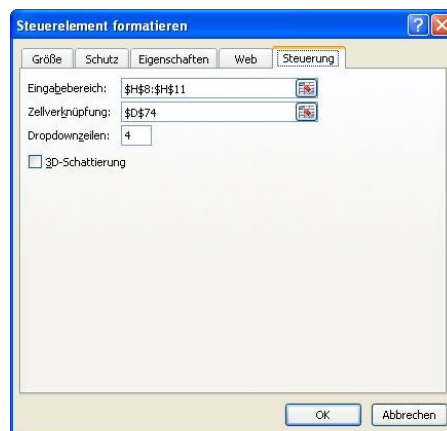


Abbildung 28 Konfiguration der Auswahlbox "Sicherheitsvorkehrung"

Um die neue Gefahr inklusive ihrer Sicherheitsvorkehrung in die Auswertung aufzunehmen, muss der VBA-Code adaptiert werden. Um zum VBA-Code zu gelangen muss man in Excel den Reiter „Entwicklungstools“ wählen und auf „Visual Basic“ klicken. Sollte der Reiter „Entwicklungstools“ nicht vorhanden sein, muss dieser erst aktiviert werden. Um den Reiter zu aktivieren, klicken Sie auf das runde Office-Symbol in der linken oberen Ecke und wählen „Excel-Optionen“. Hier finden Sie den Menüpunkt „Entwicklerregisterkarte in der Multifunktionsleiste anzeigen“. Dieser Menüpunkt muss ausgewählt sein um Visual-Basic öffnen zu können. Im Visual-Basic-Code müssen nun im Modul 3 folgende Zeilen eingefügt werden:

```
'Definition der Variablen
'Gefahr
ginfrarot = Sheets("Gefahren").Range("D39").Value
'Sicherheitsvorkehrung
infrarot = Sheets("Sicherheitsvorkehrungen").Range("d76").Value

'Ausgabe der Gefährdungslage
Sheets("Auswertung").Range("F7") = eine_vorkehrung(ginfrarot, infrarot)
```

Für die Ausgabe der Gefährdungslage stehen folgende Funktionen zur Verfügung:

```
eine_vorkehrung(Gefahr, Sicherheitsvorkehrung)
zwei_vorkehrungen(Gefahr, Sicherheitsvorkehrung1, Sicherheitsvorkehrung2)
drei_vorkehrungen(Gefahr, Sicherheitsvorkehrung1, Sicherheitsvorkehrung2, Sicherheitsvorkehrung3)
vier_vorkehrungen(Gefahr, Sicherheitsvorkehrung1, Sicherheitsvorkehrung2, Sicherheitsvorkehrung3,
    Sicherheitsvorkehrung4)
fuenf_vorkehrungen(Gefahr, Sicherheitsvorkehrung1, Sicherheitsvorkehrung2, Sicherheitsvorkehrung3,
    Sicherheitsvorkehrung4, Sicherheitsvorkehrung5)
```

Es können insgesamt bis zu fünf Sicherheitsvorkehrungen pro Gefahr berücksichtigt werden. Für jede neue Gefahr können auch bereits existierende Sicherheitsvorkehrungen verwendet werden; der entsprechende Name der Vorkehrung ist am Beginn von Modul 3 definiert.

Abschließend muss zum Beispiel in der Zelle „E7“ des Arbeitsblattes „Auswertung“ die Gefahr „Infrarotschnittstelle“ hinzugefügt werden. Es wird empfohlen, neue Gefahren rechts neben den ursprünglichen zu platzieren, da ansonsten alle darunter folgenden Ausgaben neu positioniert werden müssten. Um die Ausgabe farblich hervorzuheben, muss die Zelle „F7“ im Menüpunkt „Bedingte Formatierung“ → „Regeln verwalten“ → „Dieses Arbeitsblatt“ zu den Formatierungen „ausreichend geschützt“, „geschützt (möglicherweise nicht ausreichend)“, „verbesserungsbedürftig“ und „nicht geschützt“ hinzugefügt werden. Das Ergebnis ist in Abbildung 29 zu sehen.

Gefahren			
Feuer	ausreichend geschützt	Info	Infrarotschnittstelle
Wasser/Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	geschützt (möglicherweise nicht ausreichend)	Info	ausreichend geschützt

Abbildung 29 Auswertung inklusive neu hinzugefügter Gefahr

Selbstverständlich können auch nur neue Sicherheitsvorkehrungen oder Gefahren hinzugefügt werden. Dabei müssen die Auswertungen für die dadurch beeinflussten Gefahren wie zuvor beschrieben adaptiert werden.

7.5 Beispielfirmen

Wie im Vergleich der sechs Ansätze festgestellt wurde, ist es sehr viel einfacher eine Methode zu verstehen, wenn zumindest ein durchgängiges Beispiel vorhanden ist. Die Methode wird nun anhand zweier fiktiver Firmen vorgestellt.

7.5.1 Beispiel Einpersonnenunternehmen (EPU)

Neben dem Geschäftsführer beschäftigt das Unternehmen keine Mitarbeiter. Es ist ein Standrechner für die Verrechnung, Kundenverwaltung, Erstellung von Präsentationen und ähnlichem vorhanden. Dieser Rechner besitzt einen

kabelgebundenen Internetanschluss. Einmal wöchentlich wird ein Backup auf einer externen Festplatte erstellt und diese in einem Schrank im Büro verstaut. Außerdem ist ein Laptop für das Arbeiten unterwegs vorhanden und ein Handy. Auf dem Laptop befinden sich keine personenbezogenen Daten und im Büro ist er kabellos mit dem Internet verbunden. Das Büro befindet sich im ersten Stock eines mehrstöckigen Hauses in Wien. Es werden keine externen IT-Dienstleistungen in Anspruch genommen.

Im ersten Schritt werden die zwei Fragen zum Unternehmen beantwortet. In diesem Fall handelt es sich um ein Einpersonnenunternehmen und es werden keine externen IT-Dienstleistungen bezogen.

Unternehmen

Bitte beantworten Sie die beiden Fragen, die Eingaben werden anschließend in der Auswertung berücksichtigt. Bei Einpersonnenunternehmen werden die Fragen, die Mitarbeiter betreffen, nicht berücksichtigt. Die Fragen zu ausgelagerten IT Dienstleistungen werden nicht berücksichtigt, wenn Sie die zweite Frage mit "nein" beantworten. Klicken Sie anschließend bitte auf "Fertig" um zum nächsten Arbeitsblatt zu gelangen.

Handelt es sich bei Ihrem Unternehmen um ein Einpersonnenunternehmen?

Haben Sie IT-Dienstleistungen (z. B. Wartungsverträge, Homepage) an andere Unternehmen ausgelagert (Outsourcing)?

☒ ja ☐ nein

☐ ja ☒ nein

Fertig

Abbildung 30 Angaben zum Unternehmen - Einpersonnenunternehmen

Nun erfolgt die Bewertung der Gefahren, hierzu werden die 15 Gefahren mit ihren Wahrscheinlichkeiten bewertet.

Gefahren		
Um eine Risikoanalyse durchführen zu können, müssen die Eintrittswahrscheinlichkeiten von Gefahren eingeschätzt werden. Jede Gefahr kann mit "sehr unwahrscheinlich", "unwahrscheinlich", "möglich" und "wahrscheinlich" bewertet werden. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Bitte denken Sie dabei an Erfahrungen aus der Vergangenheit. Nach der Bewertung aller Gefahren klicken Sie bitte auf "Fertig".		
	Eintrittswahrscheinlichkeit	
Feuer	unwahrscheinlich	
Wasser/Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	unwahrscheinlich	
Erdbeben	sehr unwahrscheinlich	
Muren/Lawinen	sehr unwahrscheinlich	
Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)	unwahrscheinlich	
Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter	sehr unwahrscheinlich	
Spionage (Datendiebstahl) durch Mitarbeiter	sehr unwahrscheinlich	
Spionage durch externe Personen	unwahrscheinlich	
Vandalismus	unwahrscheinlich	
Social Engineering (das Erfragen von Passwörtern z.B.: über das Telefon, meist wird hierfür eine hilfsbereite Person unter Druck gesetzt und eine Notsituation vorgetäuscht)	sehr unwahrscheinlich	
Verlust von Schlüsselkräften	sehr unwahrscheinlich	
Extern verursachter Ausfall der Internetverbindung	unwahrscheinlich	
Fehler durch Hardware oder Software Updates	unwahrscheinlich	
Datenverlust aufgrund fehlerhafter Speichermedien	möglich	
Durch IT Dienstleister verursachte Probleme	sehr unwahrscheinlich	

Abbildung 31 Bewertung der Gefahren - Einpersonnenunternehmen

Im nächsten Schritt werden Daten über die vorhandene IT-Infrastruktur gesammelt. Dabei werden Standrechner, Laptop, Handy und die Backup-Festplatte berücksichtigt.

IT Infrastruktur

		Schutzbedarf													
		Netzwerkverbindung*			Internetzugang*		Verfügbarkeit*			Integrität*			Vertraulichkeit*		
	Name	keine	kabelgebunden	kabellos	ja	nein	sehr hoch	hoch	gering	sehr hoch	hoch	gering	sehr hoch	hoch	gering
Personal Computer (PC)	PC1		X		X			X		X				X	
Laptop	Laptop1			X	X				X			X			X
Server															
Mobile Geräte (Handy, Personal Digital Assistant - PDA)	Handy	X				X		X				X			X
Externe Datenträger (externe Festplatte, CDs, USB-Sticks)	Backup-FP							X		X				X	

* entsprechendes Feld mit einem X markieren

Abbildung 32 Angaben zur IT-Infrastruktur - Einpersonenunternehmen

Wie in Abbildung 32 ersichtlich, ist der Schutzbedarf für den Standrechner und die Backup-Festplatte höher als für den Laptop.

Anschließend müssen die Fragen zum Datenschutz beantwortet werden.

Datenschutz	
Dieser Abschnitt behandelt Vorgaben des Datenschutzgesetzes. Sollte Ihr Unternehmen keine personenbezogenen Daten (z. B. Geburtsdatum, Adresse, Lichtbild) verarbeiten, können Sie diesen Abschnitt überspringen. Das Datenschutzgesetz schreibt Maßnahmen vor, welche sicherstellen, dass "Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind" (§14 DSG 2000). Nichteinhaltung des Datenschutzgesetzes kann zu Verwaltungsstrafen bis €18 890 führen. Wenn Ihr Unternehmen personenbezogene Daten als Auftraggeber oder Dienstleister verarbeitet, beantworten Sie bitte die untenstehenden Fragen und klicken Sie anschließend auf "Fertig".	
1) Ist die Aufgabenverteilung bei der Verwendung personenbezogener Daten zwischen den Mitarbeitern ausdrücklich festgelegt? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".	ja
2) Ist die Verwendung personenbezogener Daten nur aufgrund von Aufträgen der anordnungsbefugten Organisationseinheit erlaubt? (§14(2))	ja
3) Wurde jeder Mitarbeiter über seine Pflichten bezüglich des Datenschutzgesetzes belehrt und kann er die betriebliche Datenschutzvorschrift jederzeit einsehen? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".	ja
4) Ist die Zutrittsberechtigung zu Ihren Räumlichkeiten klar geregelt? (§14(2))	ja
5) Ist die Zutrittsberechtigung zu den Daten und Programmen, welche personenbezogene Daten verarbeiten, klar geregelt? (§14(2))	ja
6) Ist eine Berechtigung zum Betrieb der Datenverarbeitungsgeräte erforderlich und ist jedes Gerät durch Vorkehrungen gegen die unbefugte Inbetriebnahme abgesichert? (§14(2))	ja
7) Sind Protokolle vorhanden, welche die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) nachvollziehbar machen? (§14(2))	nein
Ist eine Dokumentation aller Maßnahmen der Fragen 1 bis 7 vorhanden um die Kontrolle und Beweissicherung zu erleichtern? (§14(2))	nein
Ist Ihr Unternehmen in der Lage, der Auskunft-, Richtigstellungs- und Löschungspflicht nachzukommen? (§26, §27)	ja
Ist Ihnen bekannt, dass auch manuelle Dateien (z. B. Karteien, Listen), die nach mindestens einem Suchkriterium (z. B. Name) zugänglich sind, dem Datenschutzgesetz unterliegen? (§1(3))	nein
Die Übermittlung personenbezogener Daten an Länder außerhalb der EU ist grundsätzlich genehmigungspflichtig. (§12, §13) Wurde diese Genehmigung eingeholt? Sollten Sie keine Daten an Länder außerhalb der EU übermitteln, wählen Sie bitte "ja".	ja
Wurden Ihre meldungspflichtigen Datenanwendungen durch eine Meldung bei der Datenschutzkommission bewilligt? (Nicht meldungspflichtig sind: Rechnungswesen und Logistik, Personalverwaltung, Mitgliederverwaltung, Verwaltung von Benutzerkennzeichen, Kundenbetreuung und Marketing für eigene Zwecke, Patientenverwaltung und Honorarabrechnung, Personentransport und Hotelreservierung, Zutrittskontrollsysteme und KFZ-Zulassung durch beliebige Unternehmen (§17, §19)) Sollten Sie keine meldungspflichtigen Anwendungen verwendet wählen Sie bitte "ja".	ja

Abbildung 33 Angaben zum Datenschutz - Einpersonenunternehmen

Im letzten Schritt werden Angaben zu den vorhandenen Sicherheitsvorkehrungen gemacht.

Sicherheitsvorkehrungen

Bitte füllen Sie auf diesem Blatt aus, in wie weit die angeführten Sicherheitsvorkehrungen bereits umgesetzt wurden. Sie können dazu "ja", "teilweise", "nein" und "keine Angabe" auswählen. Bitte wählen Sie "keine Angabe" nur dann, wenn Sie nicht wissen ob diese Vorkehrung umgesetzt wurde. Bitte beantworten Sie alle Frage. Für die Auswertung werden nur die für ihr Unternehmen relevanten Sicherheitsvorkehrungen herangezogen. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Wenn Sie alle Fragen beantwortet haben, klicken Sie bitte auf die Schaltfläche "Fertig".

		Kommentare
Sind Brandschutzeinrichtungen in den Räumen mit IT-Infrastruktur vorhanden und werden diese ordnungsgemäß gewartet?	ja	Feuerlöscher
Ist sichergestellt, dass in Räumen mit IT-Infrastruktur Wasserleitungen weder in der Decke noch in den Wänden verlaufen?	teilweise	
Ist sichergestellt, dass sich die IT-Infrastruktur weder im Keller noch direkt unter dem Dach befindet?	ja	
Sind Notfallpläne für die Bewältigung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	nein	
Sind Schutzeinrichtungen zur Verringerung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	nein	
Sind die elektrischen Stromkreise durch Sicherungen geschützt und werden diese laufend überprüft?	ja	
Ist ein Notstromaggregat vorhanden?	nein	
Ist der Zutritt in das Unternehmen durch physische Zugangskontrollen (Schlüssel/ Chipkarte) gesichert?	ja	
Sind Richtlinien für den Umgang mit Besuchern/Handwerkern vorhanden?	nein	
Werden Mitarbeiter vor ihrer Einstellung überprüft (Lebensumstände/ finanzielle Lage/ Strafregisterauszug)?	ja	
Ist ein Testsystem für das Testen neuer Hard- und/ oder Software (z. B. Patches) vorhanden?	nein	
Ist das strategische Wissen der Mitarbeiter (kritische Prozesse/ Root-Passwörter) dem Unternehmen im Notfall zugänglich (z. B. Knowledge Management System, Passwortlisten)?	ja	
Verwendet Ihr Unternehmen unterschiedliche Internetanbieter parallel um den Ausfall der Internetverbindung von einem Anbieter kompensieren zu können?	nein	
Erfolgt die Übertragung vertraulicher Daten über unsichere Verbindungen verschlüsselt?	nein	
Werden Speichermedien für die langfristige Speicherung regelmäßig gewartet?	nein	
Ist die Zuständigkeit für die Wartung der IT-Infrastruktur klar geregelt?	ja	
Sind Firewalls auf den Computern/ Laptops und Servern installiert?	ja	
Ist ein Virenschutzprogramm auf den Computern/ Laptops und Servern vorhanden?	ja	

Ist eine Update-Richtlinie für Software (Betriebssystem, Browser, Office, Virenschutz, usw.) vorhanden?	nein	
Ist die WLAN-Verschlüsselung aktiviert?	ja	
Ist eine Passwort-Richtlinie vorhanden und sind alle Mitarbeiter darüber informiert?	ja	
Wird bei Geräten mit Bluetooth ein Passwort verwendet?	ja	
Wurde von den Mitarbeitern eine Benutzerrichtlinie für den richtigen Umgang mit dem Internet unterschrieben?	ja	
Werden RAID (redundante Anordnung unabhängiger Festplatten) Systeme in PCs eingesetzt?	nein	
Werden RAID-Systeme in Servern eingesetzt?	keine Angabe	
Werden Backup-Medien in feuerfesten Stahlschränken bzw. außerhalb des Unternehmens aufbewahrt?	nein	
Sind Backup-Lösungen für PCs, Laptops und Server vorhanden?	ja	
Werden Sicherheitsschulungen (Verfügbarkeit/ Integrität/ Vertraulichkeit/ Social Engineering) für die Mitarbeiter angeboten?	ja	
Sind Backup-Lösungen für mobile Geräte und Datenträger (USB-Sticks/ externe Festplatten) vorhanden?	nein	
Sind auf allen Geräten logische Zugangsbeschränkungen (Passwörter/ Rechtevergabe) vorhanden?	ja	
Werden digitale Unterschriften verwendet um Authentizität zu gewährleisten?	nein	
Werden Festplatten von Laptops und externe Datenträger verschlüsselt?	nein	
Werden sensible Daten verschlüsselt um ihren Inhalt zu schützen?	nein	
Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen IT Dienstleistern klar geregelt?	keine Angabe	

Abbildung 34 Vorhandene Sicherheitsvorkehrungen - Einpersonunternehmen

Die Auswertung dieser Werte ergab folgendes Ergebnis:

Auswertung

Auf diesem Blatt sehen Sie die Auswertung der Risikoanalyse für die von Ihnen eingegebenen Werte. Die Bewertung ist unterteilt in "ausreichend geschützt", "geschützt (möglicherweise nicht ausreichend)", "verbesserungsbedürftig" und "nicht geschützt". Für Gefahren, welche mit "nicht geschützt" bzw. "verbesserungsbedürftig" bewertet sind, sollten auf jeden Fall zusätzliche Sicherheitsvorkehrungen getroffen werden. Für Gefahren, welche mit "geschützt (möglicherweise nicht ausreichend)" bewertet sind liegt es in Ihrem Ermessen zusätzliche Sicherheitsvorkehrungen zu treffen oder das Risiko zu akzeptieren. Auch wenn eine Gefahr mit "ausreichend geschützt" beurteilt wurde, ist kein hundertprozentiger Schutz gewährleistet! Technologien ändern sich sehr schnell und es ist nicht möglich, jede Gefahr in diesem Schnelltest abzufragen. "Ausreichend geschützt" bedeutet, dass ein Unternehmen mit geringem oder mittlerem Schutzbedarf gegen die häufigsten Gefahren geschützt ist.

Gefahren

Feuer	ausreichend geschützt	Info
Wasser/Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	geschützt (möglicherweise nicht ausreichend)	Info
Erdbeben	nicht geschützt	Info
Muren/Lawinen	nicht geschützt	Info
Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)	geschützt (möglicherweise nicht ausreichend)	Info
Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter	irrelevant, weil Einpersonunternehmen	Info
Spionage (Datendiebstahl) durch Mitarbeiter	irrelevant, weil Einpersonunternehmen	Info
Spionage durch externe Personen	geschützt (möglicherweise nicht ausreichend)	Info
Vandalismus	ausreichend geschützt	Info
Social Engineering	irrelevant, weil Einpersonunternehmen	Info
Verlust von Schlüsselkräften	irrelevant, weil Einpersonunternehmen	Info
Extern verursachter Ausfall der Internetverbindung	nicht geschützt	Info
Fehler durch Hardware oder Software Updates	nicht geschützt	Info
Datenverlust aufgrund fehlerhafter Speichermedien	geschützt (möglicherweise nicht ausreichend)	Info
Durch externe IT Dienstleister verursachte Probleme	keine externen Dienstleister vorhanden	Info

Datenschutz

Ihr Datenschutz scheint mangelhaft zu sein, eine Überprüfung durch einen Experten wäre vorteilhaft um sicherzustellen, dass keine Bestimmung des Datenschutzgesetzes verletzt wird.

IT-Infrastruktur		Info - Netzwerkverbindung	Info - Internet	Info Verfügbarkeit	Info - Integrität	Info - Vertraulichkeit
Gerätetyp	Name	Schutz der Netzwerkverbindung	Schutz des Internetzugangs	Schutz der Verfügbarkeit	Schutz der Integrität	Schutz der Vertraulichkeit
PCs	PC1	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	verbesserungsbedürftig
Laptops	Laptop1	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	ausreichend geschützt	ausreichend geschützt	ausreichend geschützt
Server						
Mobile Geräte	Handy	keine Netzwerkverbindung	kein Internetzugang	geschützt (möglicherweise nicht ausreichend)	ausreichend geschützt	ausreichend geschützt
Externe Datenträger	Backup-FP	keine Netzwerkverbindung	kein Internetzugang	geschützt (möglicherweise nicht ausreichend)	verbesserungsbedürftig	geschützt (möglicherweise nicht ausreichend)

Abbildung 35 Auswertung - Einpersonunternehmen

Die Auswertung zeigt, dass das Unternehmen für Lawinen/ Muren und Erdbeben, extern verursachte Ausfälle der Internetverbindung und Fehler durch Hardware- oder Software-Updates anfällig ist. Außerdem gibt es Verbesserungsbedarf bei der Integrität der Backup-Festplatte und Vertraulichkeit des PCs. Ausreichend geschützt ist dieses Unternehmen gegen Feuer und Vandalismus.

7.5.2 Beispiel Kleinstunternehmen

Hierbei handelt es sich um ein Kleinstunternehmen mit fünf Mitarbeitern. Im Büro in Tirol befinden sich drei Rechner mit kabelgebundenem Internetzugang. Zwei Rechner haben die gleiche Hard- und Software, der dritte ist ein älteres Modell und dient ausschließlich der Buchhaltung. Außerdem haben die beiden Außendienstmitarbeiter Laptops, auf denen sich Kundendaten befinden. Es wird täglich ein Backup der Standrechner erstellt und das Backup-Medium in der nahegelegenen Bank aufbewahrt. Es besteht ein Wartungsvertrag für die eingesetzte Hardware mit einer externen Firma.

Im ersten Schritt werden Angaben zum Unternehmen vorgenommen. Bei diesem Unternehmen handelt es sich um kein Einpersonnenunternehmen und es besteht ein Wartungsvertrag mit einem externen Dienstleister.

Unternehmen

Bitte beantworten Sie die beiden Fragen, die Eingaben werden anschließend in der Auswertung berücksichtigt. Bei Einpersonnenunternehmen werden die Fragen, die Mitarbeiter betreffen, nicht berücksichtigt. Die Fragen zu ausgelagerten IT-Dienstleistungen werden nicht berücksichtigt, wenn Sie die zweite Frage mit "nein" beantworten. Klicken Sie anschließend bitte auf "Fertig" um zum nächsten Arbeitsblatt zu gelangen.

Handelt es sich bei Ihrem Unternehmen um ein Einpersonnenunternehmen?

Haben Sie IT-Dienstleistungen (z. B. Wartungsverträge, Homepage) an andere Unternehmen ausgelagert (Outsourcing)?

☐ ja ☒ nein

☒ ja ☐ nein

Fertig

Abbildung 36 Angaben zum Unternehmen - Kleinstunternehmen

Gefahren		
Um eine Risikoanalyse durchführen zu können, müssen die Eintrittswahrscheinlichkeiten von Gefahren eingeschätzt werden. Jede Gefahr kann mit "sehr unwahrscheinlich", "unwahrscheinlich", "möglich" und "wahrscheinlich" bewertet werden. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Bitte denken Sie dabei an Erfahrungen aus der Vergangenheit. Nach der Bewertung aller Gefahren klicken Sie bitte auf "Fertig".		
	Eintrittswahrscheinlichkeit	
Feuer	unwahrscheinlich	
Wasser/Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	unwahrscheinlich	
Erdbeben	unwahrscheinlich	
Muren/Lawinen	möglich	
Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)	unwahrscheinlich	
Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter	unwahrscheinlich	
Spionage (Datendiebstahl) durch Mitarbeiter	möglich	
Spionage durch externe Personen	möglich	
Vandalismus	unwahrscheinlich	
Social Engineering (das Erfragen von Passwörtern z.B.: über das Telefon, meist wird hierfür eine hilfsbereite Person unter Druck gesetzt und eine Notsituation vorgetäuscht)	unwahrscheinlich	
Verlust von Schlüsselkräften	möglich	
Extern verursachter Ausfall der Internetverbindung	unwahrscheinlich	
Fehler durch Hardware oder Software Updates	möglich	
Datenverlust aufgrund fehlerhafter Speichermedien	unwahrscheinlich	
Durch IT Dienstleister verursachte Probleme	möglich	

Abbildung 37 Bewertung der Gefahren - Kleinunternehmen

Nun wird die in der Kurzbeschreibung angegebene IT-Infrastruktur näher beschrieben.

IT-Infrastruktur

							Schutzbedarf								
		Netzwerkverbindung*			Internetzugang*		Verfügbarkeit*			Integrität*			Vertraulichkeit*		
	Name	keine	kabelgebunden	kabellos	ja	nein	sehr hoch	hoch	gering	sehr hoch	hoch	gering	sehr hoch	hoch	gering
Personal Computer (PC)	Rechner 1		X		X			X		X			X		
	Rechner Gruppe1		X		X				X			X			X
Laptop	Gruppe Laptop			X	X			X			X		X		
Server															
Mobile Geräte (Handy, Personal Digital Assistant - PDA)	Gruppe Handy	X				X		X				X			X
Externe Datenträger (externe Festplatte, CDs, USB-Sticks)	Backup						X			X			X		

* entsprechendes Feld mit einem X markieren

Abbildung 38 Angaben zur IT-Infrastruktur - Kleinstunternehmen

Der Schutzbedarf der Integrität und Vertraulichkeit ist bei dem Rechner für die Buchhaltung viel höher als bei den beiden anderen. Der Name (Rechner Gruppe 1) verrät, dass die beiden Rechner zu einer Gruppe zusammengefasst wurden. Der Schutzbedarf des Backup-Mediums ist ebenfalls sehr hoch.

Im nächsten Schritt müssen die zwölf Fragen zum Datenschutz beantwortet werden. Dieses Unternehmen beantwortet alle Fragen mit „ja“, was darauf schließen lässt, dass es die Richtlinien in ausreichendem Umfang umgesetzt hat.

Datenschutz	
Dieser Abschnitt behandelt Vorgaben des Datenschutzgesetzes. Sollte Ihr Unternehmen keine personenbezogenen Daten (z. B. Geburtsdatum, Adresse, Lichtbild) verarbeiten, können Sie diesen Abschnitt überspringen. Das Datenschutzgesetz schreibt Maßnahmen vor, welche sicherstellen, dass "Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind" (§14 DSGVO 2000). Nichteinhaltung des Datenschutzgesetzes kann zu Verwaltungsstrafen bis €18 990 führen. Wenn Ihr Unternehmen personenbezogene Daten als Auftraggeber oder Dienstleister verarbeitet, beantworten Sie bitte die untenstehenden Fragen und klicken Sie anschließend auf "Fertig".	
1) Ist die Aufgabenverteilung bei der Verwendung personenbezogener Daten zwischen den Mitarbeitern ausdrücklich festgelegt? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".	ja
2) Ist die Verwendung personenbezogener Daten nur aufgrund von Aufträgen der anordnungsbefugten Organisationseinheit erlaubt? (§14(2))	ja
3) Wurde jeder Mitarbeiter über seine Pflichten bezüglich des Datenschutzgesetzes belehrt und kann er die betriebliche Datenschutzvorschrift jederzeit einsehen? (§14(2)) Sollte es sich um ein Einpersonenunternehmen handeln, wählen Sie bitte "ja".	ja
4) Ist die Zutrittsberechtigung zu Ihren Räumlichkeiten klar geregelt? (§14(2))	ja
5) Ist die Zutrittsberechtigung zu den Daten und Programmen, welche personenbezogene Daten verarbeiten, klar geregelt? (§14(2))	ja
6) Ist eine Berechtigung zum Betrieb der Datenverarbeitungsgeräte erforderlich und ist jedes Gerät durch Vorkehrungen gegen die unbefugte Inbetriebnahme abgesichert? (§14(2))	ja
7) Sind Protokolle vorhanden, welche die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) nachvollziehbar machen? (§14(2))	ja
Ist eine Dokumentation aller Maßnahmen der Fragen 1 bis 7 vorhanden um die Kontrolle und Beweissicherung zu erleichtern? (§14(2))	ja
Ist Ihr Unternehmen in der Lage, der Auskunft-, Richtigstellungs- und Löschungspflicht nachzukommen? (§26, §27)	ja
Ist Ihnen bekannt, dass auch manuelle Dateien (z. B. Karteien, Listen), die nach mindestens einem Suchkriterium (z. B. Name) zugänglich sind, dem Datenschutzgesetz unterliegen? (§1(3))	ja
Die Übermittlung personenbezogener Daten an Länder außerhalb der EU ist grundsätzlich genehmigungspflichtig. (§12, §13) Wurde diese Genehmigung eingeholt? Sollten Sie keine Daten an Länder außerhalb der EU übermitteln, wählen Sie bitte "ja".	ja
Wurden Ihre meldungspflichtigen Datenanwendungen durch eine Meldung bei der Datenschutzkommission bewilligt? (Nicht meldungspflichtig sind: Rechnungswesen und Logistik, Personalverwaltung, Mitgliederverwaltung, Verwaltung von Benutzerkennzeichen, Kundenbetreuung und Marketing für eigene Zwecke, Patientenverwaltung und Honorarabrechnung, Personentransport und Hotelreservierung, Zutrittskontrollsysteme und KFZ-Zulassung durch beliehene Unternehmen (§17, §19)) Sollten Sie keine meldungspflichtigen Anwendungen verwendet wählen Sie bitte "ja".	ja

Abbildung 39 Angaben zum Datenschutz - Kleinstunternehmen

Nachdem die Fragen zum Datenschutz beantwortet wurden, muss angegeben werden, welche Sicherheitsvorkehrungen aktuell vorhanden sind.

Sicherheitsvorkehrungen

Bitte füllen Sie auf diesem Blatt aus, in wie weit die angeführten Sicherheitsvorkehrungen bereits umgesetzt wurden. Sie können dazu "ja", "teilweise", "nein" und "keine Angabe" auswählen. Bitte wählen Sie "keine Angabe" nur dann, wenn Sie nicht wissen ob diese Vorkehrung umgesetzt wurde. Bitte beantworten Sie alle Frage. Für die Auswertung werden nur die für Ihr Unternehmen relevanten Sicherheitsvorkehrungen herangezogen. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Wenn Sie alle Fragen beantwortet haben, klicken Sie bitte auf die Schaltfläche "Fertig".

		Kommentare
Sind Brandschutzeinrichtungen in den Räumen mit IT-Infrastruktur vorhanden und werden diese ordnungsgemäß gewartet?	ja	
Ist sichergestellt, dass in Räumen mit IT-Infrastruktur Wasserleitungen weder in der Decke noch in den Wänden verlaufen?	teilweise	
Ist sichergestellt, dass sich die IT Infrastruktur weder im Keller noch direkt unter dem Dach befindet?	ja	
Sind Notfallpläne für die Bewältigung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	teilweise	
Sind Schutzeinrichtungen zur Verringerung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?	nein	
Sind die elektrischen Stromkreise durch Sicherungen geschützt und werden diese laufend überprüft?	ja	
Ist ein Notstromaggregat vorhanden?	nein	
Ist der Zutritt in das Unternehmen durch physische Zugangskontrollen (Schlüssel/ Chipkarte) gesichert?	ja	
Sind Richtlinien für den Umgang mit Besuchern/Handwerkern vorhanden?	teilweise	
Werden Mitarbeiter vor ihrer Einstellung überprüft (Lebensumstände/ finanzielle Lage/ Strafregisterauszug)?	teilweise	
Ist ein Testsystem für das Testen neuer Hard- und/ oder Software (z. B. Patches) vorhanden?	teilweise	
Ist das strategische Wissen der Mitarbeiter (kritische Prozesse/ Root-Passwörter) dem Unternehmen im Notfall zugänglich (z. B. Knowledge Management System, Passwortlisten)?	nein	
Verwendet Ihr Unternehmen unterschiedliche Internetanbieter parallel um den Ausfall der Internetverbindung von einem Anbieter kompensieren zu können?	nein	
Erfolgt die Übertragung vertraulicher Daten über unsichere Verbindungen verschlüsselt?	keine Angabe	
Werden Speichermedien für die langfristige Speicherung regelmäßig gewartet?	nein	
Ist die Zuständigkeit für die Wartung der IT-Infrastruktur klar geregelt?	teilweise	
Sind Firewalls auf den Computern/ Laptops und Servern installiert?	ja	
Ist ein Virenschutzprogramm auf den Computern/ Laptops und Servern vorhanden?	ja	

Ist eine Update-Richtlinie für Software (Betriebssystem, Browser, Office, Virenschutz, usw.) vorhanden?	teilweise	
Ist die WLAN-Verschlüsselung aktiviert?	ja	
Ist eine Passwort-Richtlinie vorhanden und sind alle Mitarbeiter darüber informiert?	ja	
Wird bei Geräten mit Bluetooth ein Passwort verwendet?	ja	
Wurde von den Mitarbeitern eine Benutzerrichtlinie für den richtigen Umgang mit dem Internet unterschrieben?	ja	
Werden RAID (redundante Anordnung unabhängiger Festplatten) Systeme in PCs eingesetzt?	nein	
Werden RAID-Systeme in Servern eingesetzt?	nein	
Werden Backup-Medien in feuerfesten Stahlschränken bzw. außerhalb des Unternehmens aufbewahrt?	ja	
Sind Backup-Lösungen für PCs, Laptops und Server vorhanden?	ja	
Werden Sicherheitsschulungen (Verfügbarkeit/ Integrität/ Vertraulichkeit/ Social Engineering) für die Mitarbeiter angeboten?	teilweise	
Sind Backup-Lösungen für mobile Geräte und Datenträger (USB-Sticks/ externe Festplatten) vorhanden?	teilweise	
Sind auf allen Geräten logische Zugangsbeschränkungen (Passwörter/ Rechtevergabe) vorhanden?	ja	
Werden digitale Unterschriften verwendet um Authentizität zu gewährleisten?	nein	
Werden Festplatten von Laptops und externe Datenträger verschlüsselt?	nein	
Werden sensible Daten verschlüsselt um ihren Inhalt zu schützen?	teilweise	
Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen IT Dienstleistern klar geregelt?	ja	

Abbildung 40 Vorhandene Sicherheitsvorkehrungen - Kleinstunternehmen

Die Auswertung ergibt folgende Gefährdungen für dieses Unternehmen:

Auswertung

Auf diesem Blatt sehen Sie die Auswertung der Risikoanalyse für die von Ihnen eingegebenen Werte. Die Bewertung ist unterteilt in "ausreichend geschützt", "geschützt (möglicherweise nicht ausreichend)", "verbesserungsbedürftig" und "nicht geschützt". Für Gefahren, welche mit "nicht geschützt" bzw. "verbesserungsbedürftig" bewertet sind, sollten auf jeden Fall zusätzliche Sicherheitsvorkehrungen getroffen werden. Für Gefahren, welche mit "geschützt (möglicherweise nicht ausreichend)" bewertet sind liegt es in Ihrem Ermessen zusätzliche Sicherheitsvorkehrungen zu treffen oder das Risiko zu akzeptieren. Auch wenn eine Gefahr mit "ausreichend geschützt" beurteilt wurde, ist kein hundertprozentiger Schutz gewährleistet! Technologien ändern sich sehr schnell und es ist nicht möglich, jede Gefahr in diesem Schnelltest abzufragen. "Ausreichend geschützt" bedeutet, dass ein Unternehmen mit geringem oder mittlerem Schutzbedarf gegen die häufigsten Gefahren geschützt ist.

Gefahren

Feuer	ausreichend geschützt	Info
Wasser/Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)	geschützt (möglicherweise nicht ausreichend)	Info
Erdbeben	nicht geschützt	Info
Muren/Lawinen	nicht geschützt	Info
Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)	geschützt (möglicherweise nicht ausreichend)	Info
Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter	geschützt (möglicherweise nicht ausreichend)	Info
Spionage (Datendiebstahl) durch Mitarbeiter	geschützt (möglicherweise nicht ausreichend)	Info
Spionage durch externe Personen	verbesserungsbedürftig	Info
Vandalismus	geschützt (möglicherweise nicht ausreichend)	Info
Social Engineering	geschützt (möglicherweise nicht ausreichend)	Info
Verlust von Schlüsselkräften	nicht geschützt	Info
Extern verursachter Ausfall der Internetverbindung	nicht geschützt	Info
Fehler durch Hardware oder Software Updates	verbesserungsbedürftig	Info
Datenverlust aufgrund fehlerhafter Speichermedien	nicht geschützt	Info
Durch externe IT Dienstleister verursachte Probleme	ausreichend geschützt	Info

Datenschutz

Ihr Unternehmen scheint die Datenschutzbestimmungen in ausreichendem Umfang umgesetzt zu haben.

IT-Infrastruktur		Info - Netzwerkverbindung	Info - Internet	Info Verfügbarkeit	Info - Integrität	Info - Vertraulichkeit
Gerätetyp	Name	Schutz der Netzwerkverbindung	Schutz des Internetzugangs	Schutz der Verfügbarkeit	Schutz der Integrität	Schutz der Vertraulichkeit
PCs	Rechner 1	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	verbesserungsbedürftig
	Rechner Gruppe1	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	ausreichend geschützt	ausreichend geschützt	ausreichend geschützt
Laptops	Gruppe Laptop	ausreichend geschützt	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	geschützt (möglicherweise nicht ausreichend)	verbesserungsbedürftig
Server						
Mobile Geräte	Gruppe Handy	keine Netzwerkverbindung	kein Internetzugang	geschützt (möglicherweise nicht ausreichend)	ausreichend geschützt	ausreichend geschützt
Externe Datenträger	Backup	keine Netzwerkverbindung	kein Internetzugang	geschützt (möglicherweise nicht ausreichend)	verbesserungsbedürftig	geschützt (möglicherweise nicht ausreichend)

Abbildung 41 Auswertung - Kleinstunternehmen

Die Auswertung zeigt, dass das Unternehmen anfällig für Erdbeben/ Muren und Lawinen, den Verlust von Schlüsselkräften, extern verursachte Ausfälle der Internetverbindung und Datenverlust aufgrund fehlerhafter Speichermedien ist. Schon kleine Änderungen wie ein alternativer Internetanbieter oder die regelmäßige Wartung der Speichermedien könnte das Gefährdungspotential beträchtlich senken. Außerdem sollte das Unternehmen die Vertraulichkeit der Informationen besser schützen. Dies wäre zum Beispiel durch Verschlüsselung sensibler Daten möglich.

Ausreichend geschützt ist dieses Unternehmen gegen Feuer und Fehler durch externe IT-Dienstleister.

8 Zusammenfassung und Ausblick

Diese Diplomarbeit wollte aufzeigen, weshalb sich die bekannten IT-Risikoanalysen für kleine und mittlere Unternehmen meist nicht eignen. Sie sind mit viel bürokratischem Aufwand, langen Durchlaufzeiten und hohen Kosten verbunden. Oft werden mehrere Mitarbeiter benötigt und die zur Verfügung gestellten Hilfsmittel sind nur schlecht dokumentiert. Computersysteme sind heutzutage aus kaum einem Unternehmen wegzudenken; sie sind der Schlüssel zur Wettbewerbsfähigkeit, Eintrittstor zu Informationen und dienen als Kommunikationsmedium. Die Kehrseite ist, dass ein Unternehmen dadurch stärker angreifbar ist als dies früher der Fall war. Angriffe auf die Informationstechnologie einer Firma können von überall auf der Welt durchgeführt werden und sehr hohen Schaden anrichten. Es ist auch für kleine Firmen wichtig, sich bestmöglich vor diesen Gefahren zu schützen und die Auswirkungen so weit als möglich zu reduzieren. Jedem Unternehmer muss klar sein, welche Gefahren existieren und wie anfällig sein Unternehmen ist. Durch den hier vorgestellten Ansatz der Risikoanalyse soll genau das erreicht werden. Außerdem soll aufgezeigt werden, welche Vorgaben das Datenschutzgesetz macht.

Es wäre sehr hilfreich, wenn die branchenspezifischen Vorgaben einheitlich dokumentiert und zugänglich wären. Dadurch könnte dieser Ansatz einfacher durchgeführt werden. Derzeit muss darauf vertraut werden, dass der Anwender die Spezifika berücksichtigt. Außerdem könnten sowohl die vorhandenen Listen für Gefahren und Sicherheitsvorkehrungen als auch die Fragen zum Datenschutz erweitert werden.

Abkürzungen

BAK	Bundeskanzleramt
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDS	Credit Default Swap
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
Clusif	Club de la Sécurité de l'Information Français
DoS	Denial-of-Service
DSG	Bundesgesetz über den Schutz personenbezogener Daten
EDV	Elektronische Datenverarbeitung
ENISA	European Network and Information Security Agency
EPU	Einpersonenunternehmen
HW	Hardware
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization of Standardization
IT	Informationstechnologie
KMU	Kleine und mittlere Unternehmen
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCG	Österreichische Computergesellschaft
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Analysis
PDA	Personal Digital Assistant
RA	Risikoanalyse
RAF	Royal Air Force
RM	Risikomanagement
SDLC	System Development Life Cycle
SME	Small and medium enterprises
SP	Special Publication
SW	Software
USA	United States of America
VBA	Visual Basic for Applications

Literaturverzeichnis

[Alberts, 2005] Alberts, C., Dorofee, A., *Managing Information Security Risks. The OCTAVESM Approach*, 2005, Addison-Wesley

[Avizienis et. al., 2004] Avizienis, A., Laprie, J-C., Randall, B., Landwehr, K., *Basic Concepts and Taxonomy of Dependable and Secure Computing*, 2004, IEEE Transactions on dependable and secure computing

[BBC, 2009] Bilton, R., *Blackmail fear over lost RAF data*, [Internet], URL: http://news.bbc.co.uk/2/hi/uk_news/8066586.stm [Stand: 11.10.2009]

[BBC, 2009a] Fildes, J., *Phishing attack targets Hotmail*, [Internet], URL: <http://news.bbc.co.uk/2/hi/8291268.stm> [Stand: 11.10.2009]

[BKA, 2007] Bundeskanzleramt Österreich, 2007, *Österreichisches Informationssicherheitshandbuch Version 2.3*, [Internet] URL: www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf [Stand: 24.4.2009]

[BSI, 2004] Bundesamt für Sicherheit in der Informationstechnik, *Ein IT-Grundschutzprofil für den Mittelstand*, [Internet], URL: https://www.bsi.bund.de/cae/servlet/contentblob/474864/publicationFile/31016/profil_mittl_IT_Verbund.pdf.pdf [Stand: 14.10.2009]

[BSI, 2008a] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Profil; Anwendungsbeispiel für eine kleine Institution*, [Internet], URL: https://www.bsi.bund.de/cae/servlet/contentblob/474862/publicationFile/31017/profil_kl_institution.pdf.pdf [Stand: 14.10.2009]

[BSI, 2008b] Bundesamt für Sicherheit in der Informationstechnik, *BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise*, [Internet], URL: https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standa_rd_1002.pdf.pdf [Stand: 19.10.2009]

[BSI, 2008c] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kataloge*, [Internet], URL: https://www.bsi.bund.de/cae/servlet/contentblob/478418/publicationFile/31084/it-grundschutz-kataloge_2008_EL10_de.pdf.pdf [Stand: 19.10.2009]

[BSI, 2009] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz Kataloge*, [Internet], URL: <http://www.bsi.bund.de/gshb/deutsch/index.htm> [Stand: 26.5.2009]

[BSI, 2009a] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz: Ziel, Idee und Konzeption*, [Internet] URL: https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/allgemein/einstieg/01001.html [Stand: 14.10.2009]

[BSI, 2009b] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Standards*, [Internet] URL:

https://www.bsi.bund.de/cln_136/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html [Stand: 14.10.2009]

[BSI, 2009c] Bundesamt für Sicherheit in der Informationstechnik, *Schichtenmodell und Modellierung*, [Internet] URL: https://www.bsi.bund.de/cln_174/sid_D61E67404E62130FFE0BF5A75D9C3521/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Allgemeines/Modellierung/modellierung_node.html [Stand: 14.10.2009]

[Byres, 2004] Byres, E., Lowe, J., *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*, 2004, [Internet], URL: http://www.controlglobal.com/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf [Stand: 21.5.2009]

[Consequa, 2009] Consequa, *Glossar*, [Internet] URL: <http://www.consequa.de/glossar.htm> [Stand: 19.5.2009]

[Dockner, 2007] Dockner, E.J., *Grundzüge der allgemeinen Betriebswirtschaftslehre*, Wien, 2007

[ENISA, 2006] European Network and Information Security Agency, *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, 2006, [Internet], URL: <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools/?searchterm=risk%20management> [Stand: 14.10.2009]

[ENISA, 2006b] European Network and Information Security Agency, *Risk Assessment and Risk Management Methods: Information Package for Small and Medium Sized Enterprises (SME)*, 2006, [Internet], URL: http://www.enisa.europa.eu/doc/pdf/deliverables/WGRARM/ENISA_RM-Deliverable2-Final-version-v1.0-2006-03-30.pdf [Stand: 20.5.2009]

[ENISA, 2007] European Network and Information Security Agency, *Information Package for SMEs*, 2007, [Internet], URL: http://www.enisa.europa.eu/rmra/files/D2_ENISA_Deliverable_Information_Package_for_SMEs.pdf [Stand: 19.5.2009]

[ENISA, 2009] European Network and Information Security Agency, *Risk Management and Information Security Management Systems*, [Internet], URL: <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-isms> [Stand: 13.10.2009]

[ENISA, 2009a] European Network and Information Security Agency, *Critical Success Factors*, [Internet], URL: <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-isms/critical-success-factors> [Stand: 13.10.2009]

[EK, 2006] Europäische Kommission, 2006, *Die neue KMU Definition*, [Internet] URL:

http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide_de.pdf [Stand: 24.4.2009]

[EK, 2008] Europäische Kommission, 2008, *Entscheidung der Kommission zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten*, [Internet], URL: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm [Stand: 10.12.2009]

[Graf, 2004] Graf, W., *Datenschutz im Überblick*, 2004, Facultas Verlags- und Buchhandel

[Hutt, 1995] Hutt, A. E., Seymour, B., Hoyt, D. B., 1995. *Computer Security Handbook*. 3rd Edition. New York: John Wiley & Sons, Inc.

[IEEE Spectrum, 2008] Charette, R., *The Software Issues Behind Heathrow's T5 Meltdown*, [Internet] URL: http://www.spectrum.ieee.org/blog/computing/it/riskfactor/the_software_issues_behind_heathrow [Stand: 12.10.2009]

[InvW, 2009] InvestorWorld.com, *credit default swap*, [Internet], URL: http://www.investorwords.com/5876/credit_default_swap.html [Stand: 25.5.2009]

[ISO, 2009] International Organization for Standardization, *IT Security techniques*, [Internet], URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306 [Stand: 13.10.2009]

[ISO 27005, 2008] International Organization for Standardization, *Information technology - Security techniques - Information security risk management*, 2008

[KMUForschung, 2009] Bronett, W., *KMU in Österreich*, [Internet], URL: <http://www.kmuforschung.ac.at/de/Forschungsberichte/Vorträge/2009/KMU%20in%20Österreich,%20Dr.%20Walter%20Bornett,%20März%202009.pdf> [Stand: 19.10.2009]

[Kluge, 2002] *Ethymologisches Wörterbuch der deutschen Sprache*, 24.Auflage, Berlin/New York, 2002

[Mantl, 2007] Mantl, E., Reimer, S., *Holistische IT Security*, Verlag Mantl, 2007

[Mehari, 2007a], Club de la Sécurité de l'Information Français, *Mehari Überblick*, 2007 [Internet], URL: <http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-Uberblick.pdf> [Stand: 23.9.2009]

[Mehari, 2007b], Club de la Sécurité de l'Information Français, *Mehari Concepts and Mechanisms*, 2007 [Internet], URL: http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-concepts_principles_2007.pdf [Stand: 23.9.2009]

[Mehari, 2007c], Club de la Sécurité de l'Information Français, *Mehari Security Stakes Analysis and Classification Guide*, 2007 [Internet], URL: http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-stakes-analysis_2007.pdf [Stand: 23.9.2009]

[Mehari, 2007d], Club de la Sécurité de l'Information Français, *Mehari Handbuch Risikoanalyse*, 2007 [Internet], URL: <http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-Risikoanalyse.pdf> [Stand: 24.9.2009]

[Mehari, 2009], Club de la Sécurité de l'Information Français, *Methods*, [Internet], URL: <http://www.clusif.fr/en/clusif/present/> [Stand: 23.9.2009]

[Network Computing, 2009] Reder, B., *Chinesische und russische Hacker unterwandern amerikanisches Stromnetz*, [Internet] URL: <http://www.networkcomputing.de/chinesische-und-russische-hacker-unterwandern-amerikanisches-stromnetz/> [Stand: 12.10.2009]

[Network Computing, 2009a] Reder, B., *Mehrere Terabyte Daten über neuen US-Kampffjet gestohlen*, [Internet] URL: <http://www.networkcomputing.de/mehrere-terabyte-daten-ueber-neuen-us-kampffjet-gestohlen/> [Stand: 12.11.2009]

[NIST 2002] Stoneburner, G., Goguen, A., Feringa, A., *Risk Management Guide for Information Technology Systems*, [Internet], URL: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> [Stand: 23.9.2009]

[NVD 2009], National Institute of Standards and Technology, *National Vulnerability Database*, [Internet], URL: <http://nvd.nist.gov/> [Stand: 23.9.2009]

[OCTAVE-S V1, 2005] CERT, *Volume1: Introduction to OCTAVE-S*, [Internet], URL: <http://www.cert.org/octave/download/index4.html> [Stand: 11.10.2009]

[OCTAVE-S V3, 2005] CERT, *Volume3: Method Guidelines*, [Internet], URL: <http://www.cert.org/octave/download/index4.html> [Stand: 11.10.2009]

[ÖNORM 27001, 2008] ON Österreichisches Normungsinstitut, *Informationstechnologie - Sicherheitstechnik - Informationssicherheits-Managementsysteme – Anforderungen*, 2008

[ÖNORM 27002, 2008] ON Österreichisches Normungsinstitut, *Informationstechnologie - Sicherheitstechnik – Leitfaden für das Management der Informationssicherheit*, 2008

[Peltier, 2005] Peltier, T., R., *Information Security Risk Analysis*, 2nd Edition, 2005, Auerbach Publications

[Port, 2009] Portfolio.com, *The Formula That Killed Wall Street*, 2009, [Internet], URL: <http://www.portfolio.com/business-news/2009/03/03/Formula-That-Killed-Wall-Street?page=1#page=1> [Stand: 20.5.2009]

[RIS, 2009a] Rechtsinformationssystem, *Recht auf Richtigstellung und Löschung*, [Internet], URL: <http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12017627&ResultFunctionToken=0b2cc733-916c-4982-9e46-6707cf65c583&Kundmachungsorgan=&Index=&Titel=&Gesetzesnummer=&VonArtikel=&BisArtikel=&VonParagraf=&BisParagraf=&VonAnlage=&BisAnlage=&Typ=&Kundmachungsnummer=&Unterzeichnungsdatum=&FassungVom=29.12.2009&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=datenschutzgesetz> [Stand: 29.12.2009]

[RIS, 2009b] Rechtsinformationssystem, *Auskunftsrecht*, [Internet], URL: <http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40023950&ResultFunctionToken=0b2cc733-916c-4982-9e46-6707cf65c583&Kundmachungsorgan=&Index=&Titel=&Gesetzesnummer=&VonArtikel=&BisArtikel=&VonParagraf=&BisParagraf=&VonAnlage=&BisAnlage=&Typ=&Kundmachungsnummer=&Unterzeichnungsdatum=&FassungVom=29.12.2009&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=datenschutzgesetz> [Stand: 29.12.2009]

[Rothman, 2008] Rothman, M., *Is Insider activity or outsider activity a bigger enterprise threat?*, 2008, [Internet], URL: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1334510,00.html [Stand: 21.5.2009]

[Schaumann, 2008] Schaumann, P., *Informationssicherheit und Risikomanagement*, 2008, [Internet], URL: http://sicherheitskultur.at/Eisberg_risk.htm [Stand: 20.5.2009]

[Spiegel, 2007] Spiegel Online, *Cyber-Angriffe auf Estland alarmieren EU und Nato*, [Internet], URL: <http://www.spiegel.de/netzwelt/web/0,1518,483416,00.html> [Stand: 12.10.2009]

[Stärker, 2008] Stärker, L., *Datenschutzgesetz*, 2008, Verlag Österreich

[StatA, 2009a] Statistik Austria, *Unternehmen mit Internetzugang im Jänner 2008*, 2009, [Internet], URL: http://www.statistik.at/web_de/static/unternehmen_mit_internetzugang_im_jaenner_2008_022196.pdf [Stand: 20.5.2009]

[StatA, 2009b] Statistik Austria, *Unternehmen mit Website im Jänner 2008*, 2009, [Internet], URL: http://www.statistik.at/web_de/static/unternehmen_mit_website_im_jaenner_2008_022198.pdf [Stand: 20.5.2009]

[StatA, 2009c] Statistik Austria, *Unternehmen mit Einkäufen über elektronische Netzwerke im Jahr 2007*, 2009, [Internet], URL: http://www.statistik.at/web_de/static/unternehmen_mit_einkaeufen_ueber_elektronische_netzwerke_im_jahr_2007_022200.pdf [Stand: 20.5.2009]

[Stumwöhrer, 2009] Stumwöhrer, K., *Austrian Standards plus*, Mündlich am 16.12.2009

[Verizon, 2008] Verizon, *2008 Data Breach Investigation Report*, 2008, [Internet], URL: <http://www.verizonbusiness.com/resources/security/databreachreport.pdf> [Stand: 21.5.2009]

[Welt, 2002] Welt Online, *Herabfallende Kokosnüsse sind gefährlicher als Haifische*, 2002, [Internet], URL: http://www.welt.de/print-welt/article397374/Herabfallende_Kokosnuesse_sind_gefaehrlicher_als_Haifische.html [Stand: 24.5.2009]

[WKO, 2008a] Wirtschaftskammer Österreich, *Klein- und Mittelbetriebe in Österreich*, [Internet] URL: <http://wko.at/Statistik/kmu/erläuterungen.pdf> [Stand: 14.5.2009]

[WKO, 2008b] Wirtschaftskammer Österreich, *Arbeitgeberbetriebe nach Branchen und Beschäftigtengrößengruppen*, [Internet] URL: <http://wko.at/Statistik/kmu/KmuBetBggBran.pdf> [Stand: 19.5.2009]

[WKO, 2009] Wirtschaftskammer Österreich, *Betriebe und Beschäftigte nach Größenstufen*, [Internet] URL: <http://wko.at/statistik/jahrbuch/am-beschBGr.pdf> [Stand: 14.5.2009]

[ZDNet, 2009] ZDNet UK, *Wigan loses unencrypted data on 43.000 children*, [Internet], URL: <http://news.zdnet.co.uk/security/0,1000000189,39742409,00.htm> [Stand: 11.10.2009]

Anhang I – Abstract

Corporate IT systems can be exposed to a large number of risks from internal and external environments. Many large companies have developed their own dedicated and costly IT departments, equipped with specialists to fight these potential risks. However, despite the availability of IT risk analysis the task of performing them is often too complex and expensive for small to medium sized enterprises (SME's). Due to a lack of time and resources SME's are also often at greater risk of attack against their standard software packages such as operating systems and word processing software. Within the Austrian economy over 80% of all companies are SME's illustrating their significance.

This dissertation compares six IT analysis methodologies (Austrian Information Security Handbook, ISO/IEC 27005, OCTAVE, Grundsatzansatz of the German Federal Office for Information Security, Mehari and NIST SP800-30) and explores their strengths and weaknesses and their feasibility for SMEs. Following this a new, basic methodology is introduced which aims to help SME's improve their IT security measures whilst attaining compliance with the Austrian Data Protection Act. The risk analysis is designed to be achievable in approximately half a day by one person and is supported by an easy to use Excel file. It is therefore thought to be effective for SME companies' who have limited resources for IT security. Although less detailed than other methodologies it does aim to disclose many shortcomings of IT systems whilst being cost effective.

Anhang II – Kurzfassung

Die IT-Infrastruktur von Unternehmen ist vielfältigen Risiken ausgesetzt. Diese Risiken können von internen oder externen Gefahren ausgehen. Großbetriebe investieren viel Geld in eine IT-Abteilung um sich gegen diese Gefahren zu schützen. Eine IT-Risikoanalyse zeigt die Schwachstellen einer IT-Infrastruktur zu einem bestimmten Zeitpunkt auf. Es existieren viele unterschiedliche IT-Risikoanalysen, die meisten davon sind für kleine und mittlere Unternehmen jedoch zu teuer in der Umsetzung oder es ist das notwendige Fachwissen für die Umsetzung im Unternehmen nicht vorhanden. Kleine Unternehmen sind anfälliger für Angriffe gegen Standardsoftware wie das Betriebssystem oder die Office-Anwendungen, weil sie keine Experten haben, welche sie gegen diese Gefahren in ausreichendem Maße schützen. Kleine und mittlere Unternehmen haben einen Anteil von über 80% an der österreichischen Wirtschaft und sind deshalb für den Wirtschaftsstandort von außerordentlicher Bedeutung.

Diese Masterarbeit vergleicht sechs IT-Risikoanalysen (Österreichisches Informationssicherheitshandbuch, ISO/IEC 27005, OCTAVE, Grundschutzansatz, Mehari und NIST SP800-30), zeigt ihre Stärken und Schwächen auf und erörtert die Möglichkeit der Durchführung in kleinen Unternehmen. Anschließend wird ein neuer Ansatz vorgestellt, der speziell auf die Bedürfnisse kleiner Unternehmen ausgerichtet ist. Der Ansatz ist innerhalb eines halben Tages von einer Person durchführbar und die Umsetzung wird durch eine Excel-Datei unterstützt. Das Ziel dieses Ansatzes ist es, Sicherheitslücken in der IT-Infrastruktur kleiner Unternehmen aufzudecken und dadurch einen positiven Beitrag zum erfolgreichen Weiterbestehen des Unternehmens zu leisten. Die Methode ist nicht so detailliert wie andere, dafür aber kostengünstig, leicht verständlich und rasch umsetzbar.

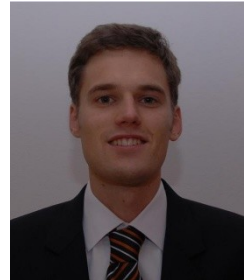
Anhang III – Lebenslauf

Robert KOPKA

Othelloogasse 1/9/23
1230 Wien

E-mail: robert_kopka@gmx.at

Geboren am 9. Februar 1984 in Wien



AUSBILDUNG

Oktober 2007 – Februar 2010

Masterstudium

„Wirtschaftsinformatik“,
Universität Wien, Dr.-Karl-Lueger-Ring 1,
1010 Wien

Oktober 2008 – März 2009

Erasmus-Semester

School of Engineering and Applied Science,
Aston University, Aston Triangle, Birmingham,
B4 7ET, England

2005 – 2007

Bachelorstudium

„Informations- und Kommunikationssysteme“,
FH Technikum, Wien Höchstädtplatz 5, 1200
Wien

BERUFSERFAHRUNG

Oktober 2005 – April 2008

Bundesministerium für Landesverteidigung (BMLV)

EDV-Abteilung

IT Risikoanalyse für kleine Unternehmen

Herzlich Willkommen bei der IT Risikoanalyse für kleine Unternehmen. Diese Risikoanalyse ist speziell auf die Bedürfnisse von Kleinst- und Kleinunternehmen ausgelegt. Das Ziel ist es, die Gefährdung von kritischen IT-Komponenten zu identifizieren und die Anfälligkeit für ausgewählte umweltbezogene, menschliche und technische Gefahren aufzuzeigen. Außerdem wird die Einhaltung grundlegender Vorschriften des österreichischen Datenschutzgesetzes abgefragt. Dieser Schnelltest erhebt keinen Anspruch auf Vollständigkeit. Sollten bei der Auswertung Schwachstellen identifiziert werden, wird empfohlen, die Beiziehung eines Fachexperten zu überlegen. Um diese Risikoanalyse durchführen zu können müssen Sie Makros zulassen. Die Arbeitsblätter wurden unter Windows XP und MS Office 2007 Professional erstellt.

Dieser Schnelltest wurde im Rahmen einer Masterarbeit von Robert Kopka (robert_kopka@gmx.at) an der Universität Wien entwickelt.

Diese Risikoanalyse besteht aus fünf Schritten:

- Unternehmen: Zwei Fragen zum Unternehmen
- Gefahren: Ein Gefahrenkatalog bestehend aus 15 Gefahren
- IT Infrastruktur: Angaben zur IT Infrastruktur des Unternehmens
- Datenschutz: Fragen zur Einhaltung des österreichischen Datenschutzgesetzes
- Sicherheitsvorkehrungen: Katalog bestehend aus 34 Sicherheitsvorkehrungen

Vorgangsweise:

Klicken Sie bitte auf die Schaltfläche "Start" um die Risikoanalyse durchzuführen. Sie werden automatisch von einem Arbeitsblatt zum nächsten weitergeleitet. Verwenden Sie bitte immer die vorhandenen Schaltflächen (klicken Sie NICHT auf die Reiter in der Leiste am unteren Ende des Fensters), da diese oft mit einer Überprüfung der eingegeben Daten verknüpft sind. Nachdem Sie alle Fragen auf allen Arbeitsblättern ausgefüllt haben, werden Ihre Eingaben ausgewertet und die Ergebnisse ausgegeben. Jeder Abschnitt enthält eine kurze Anleitung.

Sie können den aktuellen Stand der Risikoanalyse jederzeit speichern und später an dieser Stelle weiterarbeiten.

Durch betätigen der Schaltfläche "Zurücksetzen" können Sie alle Arbeitsblätter in den Ursprungszustand versetzen.

Unternehmen

Bitte beantworten Sie die beiden Fragen, die Eingaben werden anschließend in der Auswertung berücksichtigt. Bei Einpersonenenunternehmen werden die Fragen, die Mitarbeiter betreffen, nicht berücksichtigt. Die Fragen zu ausgelagerten IT Dienstleistungen werden nicht berücksichtigt, wenn Sie die zweite Frage mit "nein" beantworten. Klicken Sie anschließend bitte auf "Fertig" um zum nächsten Arbeitsblatt zu gelangen.

Handelt es sich bei Ihrem Unternehmen um ein Einpersonenenunternehmen?

☐ ja ☐ nein

Haben Sie IT-Dienstleistungen (z. B. Wartungsverträge, Homepage) an andere Unternehmen ausgelagert (Outsourcing)?

☐ ja ☐ nein

Gefahren

Um eine Risikoanalyse durchführen zu können, müssen die Eintrittswahrscheinlichkeiten von Gefahren eingeschätzt werden. Jede Gefahr kann mit "sehr unwahrscheinlich", "unwahrscheinlich", "möglich" und "wahrscheinlich" bewertet werden. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Bitte denken Sie dabei an Erfahrungen aus der Vergangenheit. Nach der Bewertung aller Gefahren klicken Sie bitte auf "Fertig".

Eintrittswahrscheinlichkeit

Feuer		
Wasser/ Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)		
Erdbeben		
Muren/ Lawinen		
Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)		
Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter		
Spionage (Datendiebstahl) durch Mitarbeiter		
Spionage durch externe Personen		
Vandalismus		
Social Engineering (das Erfragen von Passwörtern z. B. über das Telefon, meist wird hierfür eine hilfsbereite Person unter Druck gesetzt und eine Notsituation vorgetäuscht)		
Verlust von Schlüsselkräften		
Extern verursachter Ausfall der Internetverbindung		
Fehler durch Hardware- oder Software-Updates		
Datenverlust aufgrund fehlerhafter Speichermedien		

Durch IT-Dienstleister verursachte Probleme

IT-Infrastruktur

Dieser Abschnitt ist Ihrer IT-Infrastruktur gewidmet. Dabei werden PCs, Laptops, Server, mobile Geräte und externe Datenträger unterschieden. Gleichartige Geräte (gleiche Hardware, Software, Konfiguration, Aufgabenbereiche) können dabei zu Gruppen zusammengefasst werden. Bitte füllen Sie für jedes Gerät/ jede Gerätegruppe die gesamte Zeile aus. Ist ein Feld aus mehreren zu wählen (Netzwerkverbindung, Internetzugang, Verfügbarkeit, Integrität, Vertraulichkeit), ist das entsprechende Feld mit einem X zu markieren. Bitte markieren sie nur EIN Feld pro Kategorie (= farblicher Markierung). Wenn Sie ein weiteres Gerät (z. B. einen weiteren PC) hinzufügen wollen, klicken Sie bitte links auf die Zahl der nächsten Zeile mit der rechten Maustaste und wählen "Zellen einfügen". Die Zeile wird oberhalb der markierten Zeile eingefügt. Zum Löschen klicken Sie mit der rechten Maustaste auf die zu löschende Zeile und wählen "Zellen löschen". Bitte löschen Sie die Zeilen, in denen sich die Kategorienamen (Personal Computer, Laptop, Server, mobile Geräte, externe Datenträger) befinden NICHT, auch dann nicht, wenn Sie über kein Gerät dieser Kategorie verfügen.

Hilfestellung für die Bewertung des Schutzbedarfs

Verfügbarkeit sehr hoch → Verzichtbarkeit des Geräts liegt im Bereich von Minuten

Verfügbarkeit hoch → Verzichtbarkeit des Geräts liegt im Bereich von Stunden

Verfügbarkeit gering → Verzichtbarkeit des Geräts liegt im Bereich von Tagen

Integrität sehr hoch → unrichtige Daten können für das Unternehmen lebensbedrohend sein

Integrität hoch → unrichtige Daten können hohen Schaden (finanzieller Schaden, Verlust von Reputation,...) anrichten

Integrität gering → unrichtige Daten können nur geringen Schaden anrichten

Vertraulichkeit sehr hoch → gelangen Daten in die falschen Hände, kann dies für das Unternehmen lebensbedrohend sein

Vertraulichkeit hoch → gelangen Daten in die falschen Hände, kann hoher Schaden entstehen

Vertraulichkeit gering → gelangen Daten in die falschen Hände, kann nur geringer Schaden entstehen

	Name	Netzwerkverbindung*			Internetzugang*		Verfügbarkeit*			Schutzbedarf			Vertraulichkeit*		
										Integrität*					
		keine	kabelgebunden	kabellos	ja	nein	sehr hoch	hoch	gering	sehr hoch	hoch	gering	sehr hoch	hoch	gering
Personal Computer (PC)															
Laptop															
Server															
Mobile Geräte (Handy, Personal Digital Assistant - PDA)															
Externe Datenträger (externe Festplatte, CDs, USB-Sticks)															

* entsprechendes Feld mit einem X markieren

Datenschutz

Dieser Abschnitt behandelt Vorgaben des Datenschutzgesetzes. Sollte Ihr Unternehmen keine personenbezogenen Daten (z. B. Geburtsdatum, Adresse, Lichtbild) verarbeiten, können Sie diesen Abschnitt überspringen. Das Datenschutzgesetz schreibt Maßnahmen vor, welche sicherstellen, dass "Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind" (§14 DSG 2000). Nichteinhaltung des Datenschutzgesetzes kann zu Verwaltungsstrafen bis €18 890 führen. Wenn Ihr Unternehmen personenbezogene Daten als Auftraggeber oder Dienstleister verarbeitet, beantworten Sie bitte die untenstehenden Fragen und klicken Sie anschließend auf "Fertig".

1) Ist die Aufgabenverteilung bei der Verwendung personenbezogener Daten zwischen den Mitarbeitern ausdrücklich festgelegt? (§14(2)) Sollte es sich um ein Einpersonunternehmen handeln, wählen Sie bitte "ja".

2) Ist die Verwendung personenbezogener Daten nur aufgrund von Aufträgen der anordnungsbefugten Organisationseinheit erlaubt? (§14(2))

3) Wurde jeder Mitarbeiter über seine Pflichten bezüglich des Datenschutzgesetzes belehrt und kann er die betriebliche Datenschutzvorschrift jederzeit einsehen? (§14(2)) Sollte es sich um ein Einpersonunternehmen handeln, wählen Sie bitte "ja".

4) Ist die Zutrittsberechtigung zu Ihren Räumlichkeiten klar geregelt? (§14(2))

5) Ist die Zutrittsberechtigung zu den Daten und Programmen, welche personenbezogene Daten verarbeiten, klar geregelt? (§14(2))

6) Ist eine Berechtigung zum Betrieb der Datenverarbeitungsgeräte erforderlich und ist jedes Gerät durch Vorkehrungen gegen die unbefugte Inbetriebnahme abgesichert? (§14(2))

7) Sind Protokolle vorhanden, welche die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) nachvollziehbar machen? (§14(2))

Ist eine Dokumentation aller Maßnahmen der Fragen 1 bis 7 vorhanden um die Kontrolle und Beweissicherung zu erleichtern? (§14(2))

Ist Ihr Unternehmen in der Lage, der Auskunft-, Richtigstellungs- und Löschungspflicht nachzukommen? (§26, §27)

Ist Ihnen bekannt, dass auch manuelle Dateien (z. B. Karteien, Listen), die nach mindestens einem Suchkriterium (z. B. Name) zugänglich sind, dem Datenschutzgesetz unterliegen? (§1(3))

Die Übermittlung personenbezogener Daten an Länder außerhalb der EU ist grundsätzlich genehmigungspflichtig. (§12, §13) Wurde diese Genehmigung eingeholt? Sollten Sie keine Daten an Länder außerhalb der EU übermitteln, wählen Sie bitte "ja".

Wurden Ihre meldungspflichtigen Datenanwendungen durch eine Meldung bei der Datenschutzkommission bewilligt? (Nicht meldungspflichtig sind: Rechnungswesen und Logistik, Personalverwaltung, Mitgliederverwaltung, Verwaltung von Benutzerkennzeichen, Kundenbetreuung und Marketing für eigene Zwecke, Patientenverwaltung und Honorarabrechnung, Personentransport und Hotelreservierung, Zutrittskontrollsysteme und KFZ-Zulassung durch beliehene Unternehmen (§17, §19)) Sollten Sie keine meldungspflichtigen Anwendungen verwendet wählen Sie bitte "ja".

Sicherheitsvorkehrungen

Bitte füllen Sie auf diesem Blatt aus, in wie weit die angeführten Sicherheitsvorkehrungen bereits umgesetzt wurden. Sie können dazu "ja", "teilweise", "nein" und "keine Angabe" auswählen. Bitte wählen Sie "keine Angabe" nur dann, wenn Sie nicht wissen ob diese Vorkehrung umgesetzt wurde. Bitte beantworten Sie alle Frage. Für die Auswertung werden nur die für Ihr Unternehmen relevanten Sicherheitsvorkehrungen herangezogen. Das Feld "Kommentare" dient dazu, Notizen zu machen um die Auswahl zu begründen bzw. nachvollziehbar zu machen. Wenn Sie alle Fragen beantwortet haben, klicken Sie bitte auf die Schaltfläche "Fertig".

		Kommentare
Sind Brandschutzeinrichtungen in den Räumen mit IT-Infrastruktur vorhanden und werden diese ordnungsgemäß gewartet?		
Ist sichergestellt, dass in Räumen mit IT-Infrastruktur Wasserleitungen weder in der Decke noch in den Wänden verlaufen?		
Ist sichergestellt, dass sich die IT Infrastruktur weder im Keller noch direkt unter dem Dach befindet?		
Sind Notfallpläne für die Bewältigung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?		
Sind Schutzeinrichtungen zur Verringerung der Auswirkungen von Erdbeben/ Muren/ Lawinen vorhanden?		
Sind die elektrischen Stromkreise durch Sicherungen geschützt und werden diese laufend überprüft?		
Ist ein Notstromaggregat vorhanden?		
Ist der Zutritt in das Unternehmen durch physische Zugangskontrollen (Schlüssel/ Chipkarte) gesichert?		
Sind Richtlinien für den Umgang mit Besuchern/Handwerkern vorhanden?		
Werden Mitarbeiter vor ihrer Einstellung überprüft (Lebensumstände/ finanzielle Lage/ Strafregisterauszug)?		
Ist ein Testsystem für das Testen neuer Hard- und/ oder Software (z. B. Patches) vorhanden?		
Ist das strategische Wissen der Mitarbeiter (kritische Prozesse/ Root-Passwörter) dem Unternehmen im Notfall zugänglich (z. B. Knowledge Management System, Passwortlisten)?		
Verwendet Ihr Unternehmen unterschiedliche Internetanbieter parallel um den Ausfall der Internetverbindung von einem Anbieter kompensieren zu können?		
Erfolgt die Übertragung vertraulicher Daten über unsichere Verbindungen verschlüsselt?		
Werden Speichermedien für die langfristige Speicherung regelmäßig gewartet?		
Ist die Zuständigkeit für die Wartung der IT-Infrastruktur klar geregelt?		
Sind Firewalls auf den Computern/ Laptops und Servern installiert?		
Ist ein Virenschutzprogramm auf den Computern/ Laptops und Server vorhanden?		
Ist eine Update-Richtlinie für Software (Betriebssystem, Browser, Office, Virenschutz, usw.) vorhanden?		
Ist die WLAN-Verschlüsselung aktiviert?		
Ist eine Passwort-Richtlinie vorhanden und sind alle Mitarbeiter darüber informiert?		
Wird bei Geräten mit Bluetooth ein Passwort verwendet?		
Wurde von den Mitarbeitern eine Benutzerrichtlinie für den richtigen Umgang mit dem Internet unterschrieben?		
Werden RAID (redundante Anordnung unabhängiger Festplatten) Systeme in PCs eingesetzt?		
Werden RAID-Systeme in Servern eingesetzt?		
Werden Backup-Medien in feuerfesten Stahlschränken bzw. außerhalb des Unternehmens aufbewahrt?		
Sind Backup-Lösungen für PCs, Laptops und Server vorhanden?		
Werden Sicherheitsschulungen (Verfügbarkeit/ Integrität/ Vertraulichkeit/ Social Engineering) für die Mitarbeiter angeboten?		
Sind Backup-Lösungen für mobile Geräte und Datenträger (USB-Sticks/ externe Festplatten) vorhanden?		

Sind auf allen Geräten logische Zugangsbeschränkungen (Passwörter/
Rechtevergabe) vorhanden?

Werden digitale Unterschriften verwendet um Authentizität zu gewährleisten?

Werden Festplatten von Laptops und externe Datenträger verschlüsselt?

Werden sensible Daten verschlüsselt um ihren Inhalt zu schützen?

Sind die Verantwortlichkeiten/ Zuständigkeiten zwischen Ihnen und Ihren externen
IT Dienstleistern klar geregelt?

Auswertung

Auf diesem Blatt sehen Sie die Auswertung der Risikoanalyse für die von Ihnen eingegebenen Werte. Die Bewertung ist unterteilt in "ausreichend geschützt", "geschützt (möglicherweise nicht ausreichend)", "verbesserungsbedürftig" und "nicht geschützt". Für Gefahren, welche mit "nicht geschützt" bzw. "verbesserungsbedürftig" bewertet sind, sollten auf jeden Fall zusätzliche Sicherheitsvorkehrungen getroffen werden. Für Gefahren, welche mit "geschützt (möglicherweise nicht ausreichend)" bewertet sind liegt es in Ihrem Ermessen zusätzliche Sicherheitsvorkehrungen zu treffen oder das Risiko zu akzeptieren. Auch wenn eine Gefahr mit "ausreichend geschützt" beurteilt wurde, ist kein hundertprozentiger Schutz gewährleistet! Technologien ändern sich sehr schnell und es ist nicht möglich, jede Gefahr in diesem Schnelltest abzufragen. "Ausreichend geschützt" bedeutet, dass ein Unternehmen mit geringem oder mittlerem Schutzbedarf gegen die häufigsten Gefahren geschützt ist.

Gefahren

- Feuer
- Wasser/ Flüssigkeiten (Regen, Überschwemmung, Wasserrohrbruch)
- Erdbeben
- Muren/ Lawinen
- Unterbrechung der Stromversorgung (Blitzschlag, Kurzschluss)
- Sabotage (Zerstörung, Manipulation der IT Infrastruktur) durch Mitarbeiter
- Spionage (Datendiebstahl) durch Mitarbeiter
- Spionage durch externe Personen
- Vandalismus
- Social Engineering
- Verlust von Schlüsselkräften
- Extern verursachter Ausfall der Internetverbindung
- Fehler durch Hardware oder Software Updates
- Datenverlust aufgrund fehlerhafter Speichermedien
- Durch externe IT Dienstleister verursachte Probleme

Datenschutz

IT-Infrastruktur

Gerätetyp	Name	Schutz der Netzwerkverbindung	Schutz des Internetzugangs	Schutz der Verfügbarkeit	Schutz der Integrität	Schutz der Vertraulichkeit
-----------	------	-------------------------------	----------------------------	--------------------------	-----------------------	----------------------------