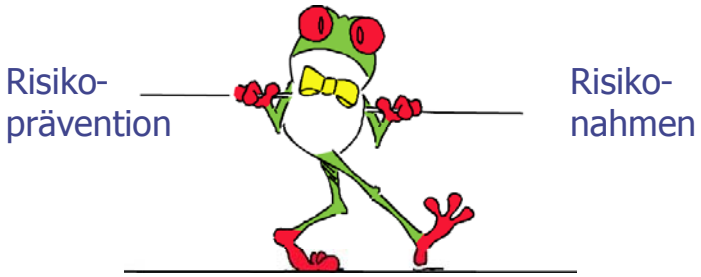
MOTIVATION

Diese Broschüre richtet sich in erster Linie an den Verwaltungsrat und Geschäftsführer, die das IT-Risikomanagement im Unternehmen einführen müssen. Das Gesetz verlangt von der Unternehmensleitung eine angemessene Dokumentation aller Schritte und Massnahmen, die eine nachhaltige Minderung des Unternehmenswertes oder deren Existenz durch Gefahren in der IT beeinflussen könnten. Jeder Geschäftsführer handelt bei mangelhafter physikalischer IT-Sicherheit grob fahrlässig und haftet im Schadensfall persönlich.

Das OR sagt:

> Haftung aus Geschäftsführung, Kontrolle (754) [673/4]
>
> Alle mit der Verwaltung, Geschäftsführung oder Kontrolle betrauten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Geschäftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung der ihnen obliegenden Pflichten verursachen.

Der Inhalt zeigt den Umfang der obliegenden Pflichten in einem modernen IT-Risikomanagement.



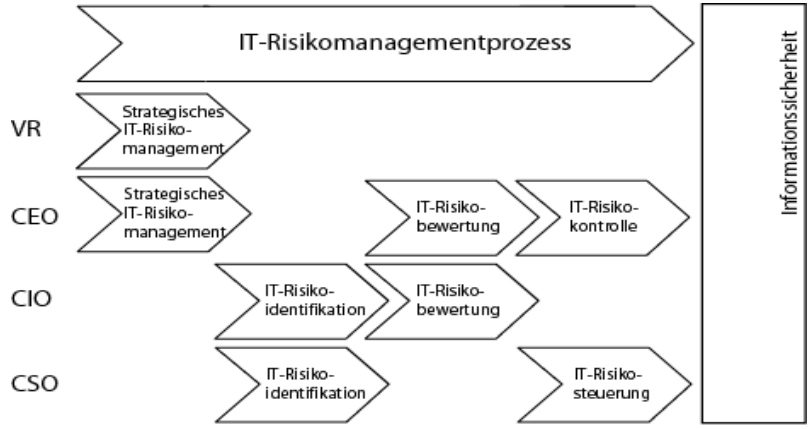
Der Hochseilakt

DER THEORETISCHE ANSATZ

Der theoretische Ansatz des IT-Risikomanagement setzt auf das Wasserfallprinzip, wie Vorgabe erarbeiten, die momentane Situation ausloten, Situation beurteilen und Sicherheitslücken schliessen. Die Erkenntnisse aus diesem Ablauf lieferten in der Praxis nicht die gewünschten Resultate. Viele Verantwortliche sind mit diesem Vorgehen massiv überfordert "Complexity is the worst of security" (Bruce Schneider). Die Verantwortlichen müssen in der Lage sein, die Gefahren und ihre Auswirkungen im Unternehmen zu sehen und verstehen. Aus diesem Grunde ist der theoretische Ansatz wegen der hohen Komplexität sehr schwierig umzusetzen. Ein Aufbrechen in mehreren Zyklen zwischen Strategie und Analyse entspricht dem Vorgehen, das auf dem Prozessansatz des franz. Philosophen und Mathematikers René Descarts aufbaut und die er bereits im 17. Jahrhundert formulierte:

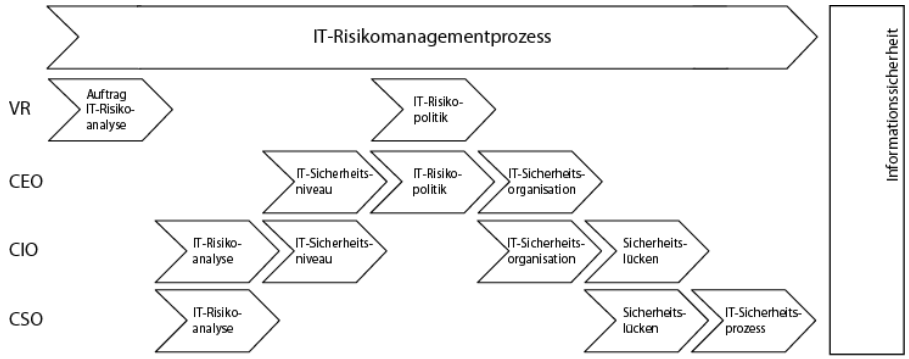
- Formulieren Sie das Problem, das Sie lösen wollen, schriftlich
- Zerlege Sie dieses Problem solange in Einzelprobleme, bis es überschaubar wird und lösbar erscheint
- Achten Sie auf den Gesamtzusammenhang, ordnen und visualisieren Sie die einzelnen Teile so, dass Sie das Ganze überblicken und nichts aus dem Auge verlieren
- Prüfen Sie sodann die Tatsachen und nehmen nichts als gegeben hin
- Lösen Sie sodann konsequent und treffsicher ein Teilproblem nach dem anderen.

Prozesslandschaft und Verantwortung, der theoretische Ansatz



DER PRAGMATISCHE ANSATZ

Prozesslandschaft und Verantwortung, der pragmatische Ansatz



Der pragmatische Ansatz nimmt die Definitionen aus dem theoretischen Vorgehen und teilt den IT-Risikomanagementprozess in mehrere Teilaufgaben und Zyklen (Iteration) zwischen den theoretischen Prozessen. Diese Abweichung bringt das Thema näher zur Praxis im Unternehmen.

IT-Risikomanagementprozess

Am Anfang steht der Auftrag für eine **IT-Risikoanalyse** und stösst den Prozess mit der Risikoidentifikation und Risikobewertung an. Die Unternehmensleitung diskutiert im **IT-Sicherheitsniveauprozess** an den konkreten IT-Risiken im Unternehmen. Die Gefahren und das Ausmass sind nach der Analyse bekannt. Sollte sich herausstellen, dass das Sicherheitsniveau nicht der gewünschten Anforderungen entspricht, kann diese anschliessend noch im IT-Risikopolitikprozess korrigiert werden.

Im **IT-Risikopolitikprozess** bestimmt man nur noch welche Risiken werden wie abgedeckt. Nach diesem Meilenstein steht der Sicherheitsumfang. Auf Grund der Analyseunterlagen und den Sicherheitsvorgaben kann jetzt die gewünschte Organisation aufgebaut werden. Die **IT-Sicherheitsorganisation** lässt die Lücken durch die IT-Abteilung schliessen und etabliert den **IT-Sicherheitsprozess** im Unternehmen. Dieser indirekter Weg bricht die Komplexität in verständlichere Teile und der Überblick bleibt für die Verantwortlichen bestehen. Durch die klaren Input/Output-Definitionen läuft der IT-Risikomanagementprozess zielgerichtet und orientiert sich an den Bedürfnissen des Unternehmens.

Achtung Halbherzigkeit!

Der Erfolg bezüglich IT-Sicherheit hängt sehr stark an der Einstellung der Unternehmensleitung. **Interessen- und Zielkonflikte** sind in diversen Verantwortungsbereichen und Zuständigkeiten unumgänglich. Damit alle Personen im Unternehmen diese Politik leben, legt die Geschäftsleitung diese fest und wird noch vom Verwaltungsrat bestätigt.

Auftrag für IT-Risikoanalyse erstellen

Der Verwaltungsrat und die Geschäftsleitung stehen gegenüber den Aktionären und Geschäftsgläubigern in der Pflicht, alles zu unternehmen, um Schaden der die Unternehmensziele im negativen Sinne massgeblich beeinflusst oder die Existenz des Unternehmens gefährdet, abzuwenden.

Die primären Ziele des IT-Risikomanagements sind:

a) Sicherung der Existenz des Unternehmens
b) Sicherung des Unternehmenserfolges
c) Einhaltung der gesetzlichen Vorgaben
d) Optimierung der Risikokosten

Damit diese Ziele erreicht werden können, muss das Management das Gefahrenpotenzial kennen, das in der Technologie der Informationsverarbeitung im Unternehmen vorhanden ist. Das Gefahrenpotenzial kann durch eine IT-Risikoanalyse ermittelt werden. Damit eine Bewertung der Gefahren bezüglich Schadensausmass und Eintrittswahrscheinlichkeit vorgenommen werden kann, braucht der Prozess folgende Vorgaben:

1. Schadenssumme
   a) die das Unternehmen in seiner Existenz gefährdet (Verbotsbereich)
   b) die das Unternehmen in seiner Ziele nachhaltig einschränkt (Grenzbereich)
2. Unternehmensinformationen die zu schützen sind
3. relevante Gesetze und Vorgaben

Output:
Auftrag für eine IT-Risikoanalyse

IT-Risikoanalyse durchführen

Input:
Auftrag für eine IT-Risikoanalyse

Die Ist-Aufnahme und die Bewertung wird an Hand der Bausteine aus dem IT-Grundschutzhandbuch von BSI (Bundesamt für Sicherheit in der Informationstechnik Bonn) vorgenommen und beurteilt. Das IT-Grundschutzhandbuch deckt das Spektrum des ISO 17799 Standards ab. Das Resultat dieser Analyse vermittelt der Geschäftsleitung einen Überblick bezüglich den Risiken und deren Tragweite. Die Diskussionsgrundlage sind jetzt für die nächsten Prozesse, *IT-Sicherheitsniveau festlegen*, *IT-Sicherheitspolitik definieren*, vorhanden. Der Vorteil dieses Vorgehens besteht darin, dass an Hand von tatsächlichen IT-Risiken im Unternehmen das Sicherheitsniveau festgelegt werden kann. Das IT-Grundschutzhandbuch umfasst alle Gefahrenkategorien, wie:

- Höhere Gewalt
- Technisches Versagen
- Vorsätzliche Handlung
- Menschliche Fehlhandlungen
- Organisatorische Mängel

Auch die Sicherheitspolitik lässt mit diesen Unterlagen schneller und konkreter definieren.

Output:
IT-Objektübersicht
Welche Ressourcen sind im Unternehmen im Einsatz?
- IT-Systeme, Netze, IT-Anwendungen

IT-Risikobewertung
Welche IT-Anwendungen liegen nicht in der Verfügbarkeitsanforderung?
Welche Schäden an IT-Objekten liegen im Verbotsbereich und Grenzbereich?
Welche Gesetzesvorlagen werden nicht eingehalten?
Welche Unternehmensinformation unterliegen nicht den internen Schutzvorschriften?
- Rating (Eintrittswahrscheinlichkeit/Schadensausmass)
- IT Risikobewertung (Eintrittswahrscheinlichkeit/Schadensausmass)

IT-Objektübersicht personenbezogene Daten
Welche personenbezogene Daten unterliegen den gesetzlichen Auflagen?
IT-Anwendungen & max. Ausfallzeit
Welche Verfügbarkeit erwarten die Anwender?

IT-Sicherheitsniveau festlegen

Input:
IT-Objektübersicht
IT-Risikobewertung
IT-Objektübersicht personenbezogene Daten
IT-Anwendungen & max. Ausfallzeit

Die Unterlagen aus dem Prozess *IT-Risikoanalyse durchführen* zeigen das Sicherheitsniveau des Unternehmens ohne eine gezielte Risikopolitik auf. Es stellt sich nun die Frage, wie kann man das Niveau mit einer geregelten Handlungserwartung und einer instituierten Handlungsfähigkeit verbessern. Die IT-Sicherheitsleitlinie (Information Security Policy) definiert die Handlungserwartung in der Informationsverarbeitung. Die Verfügbarkeit wird unter Berücksichtigung der Chance-/Risikoverhältnisse geregelt. Die Vertraulichkeit und die Integrität der Information und die Rechenschaftspflicht des Einzelnen hinsichtlich der Nutzung von Informationen im Unternehmen werden in diesem Prozess in der IT-Sicherheitsleitlinie fixiert. Der optimale Sicherheitsgrad muss beim festlegen des Sicherheitsniveaus mitberücksichtigt werden.

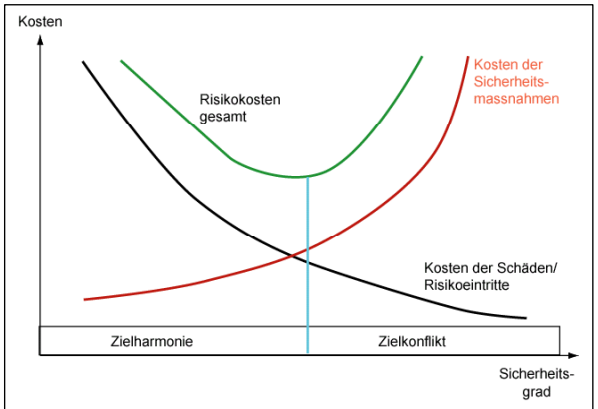


Abbildung 1 Optimaler Sicherheitsgrad

Output:
IT-Sicherheitsleitlinie (Information Security Policy)
Welche Erwartung haben wir in der Informationspolitik?
(Informationsklassifizierung, Systemzugangskontrolle, Verantwortlichkeiten, Informationseigentümer, Durchsetzung, Sicherheitsdokumentation)

IT-Risikopolitik definieren

Input:
IT-Risikobewertung
IT-Objektübersicht personenbezogene Daten
IT-Anwendungen & max. Ausfallzeit

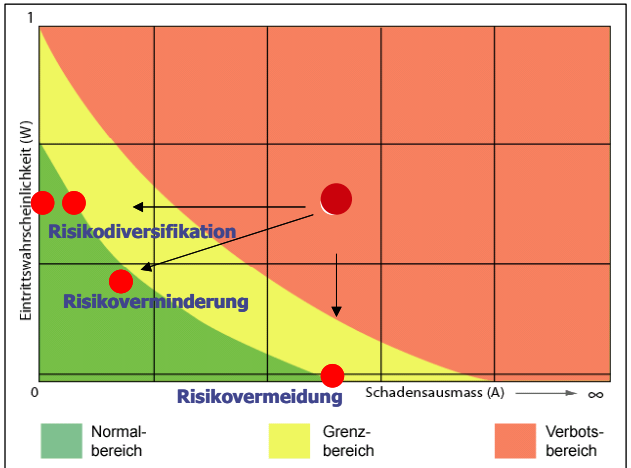


Abbildung 1 Risk Map

Alle Gefahren im Verbotsbereich oder Grenzbereich müssen jetzt mit den geeigneten Massnahmen aus dieser gebracht werden. Auch hier gilt der Spruch *viele Wege führen nach Rom*. Grundsätzlich gibt es drei Arten:

1. Präventive Risikopolitik (Aktive Risikobewältigung)
2. Korrektive Risikopolitik (Passive Risikobewältigung)
3. Keine aktive Risikopolitik (Risiko wird selbst übernommen)

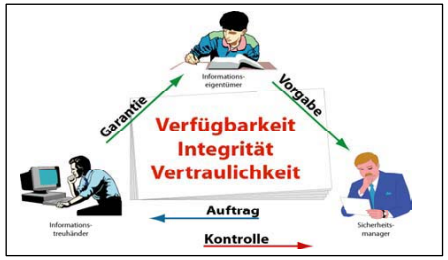
In diesem Prozess wird nicht nur die Frage beantwortet „welche Risiken nehmen wir in kauf und welche wollen wir abdecken“ sondern regelt auch die Grundstrategie wie der Schaden durch die Eintrittswahrscheinlichkeit und/oder der finanzielle Verlust auf ein akzeptables Mass zu reduzieren ist. Das Ziel dieser Tätigkeit ist es nicht, alle Risiken auszuschalten, sondern die Balance zwischen Chance und Risiken zu finden.

Output:
IT-Sicherheitspolitik

IT-Sicherheitsorganisation aufbauen

Input:
IT-Sicherheitsleitlinie

Die Strategie und die Politik muss in einer handlungsfähigen Organisation umgesetzt werden. Die Stellenbeschreibung beinhaltet die Rechten und Pflichten des IT-Sicherheitsbeauftragten (CSO Chief Security Officer). Der Inhalt des Organisationshandbuches umfasst der strategische sowie der operative Teil des IT-Risikomanagements und wird vom CSO erarbeitet. Der Sicherheitsbeauftragte rapportiert direkt an den CEO oder an den Verwaltungsrat.

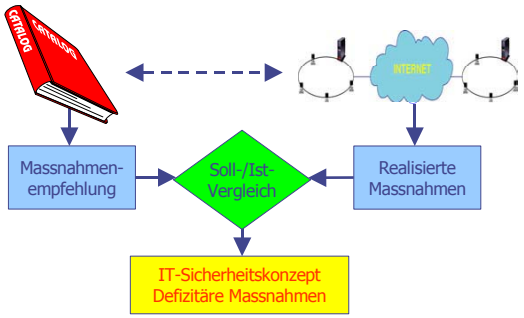


Output:
Stellenbeschreibung CSO
IT-Sicherheitsorganisationshandbuch

IT-Sicherheitslücken schliessen

Input:
IT-Sicherheitspolitik
IT-Risikobewertung
IT-Objektübersicht personenbezogene Daten
IT-Anwendungen & max. Ausfallzeit

Der IT-Sicherheitsbeauftragter erarbeitet einen Massnahmenkatalog und deren Umsetzungsreihenfolge, sowie eine Kosten- und Aufwandschätzung. Die Umsetzung der Massnahmen liegen nicht in der Obhut des IT-Sicherheitsbeauftragten, sondern werden vom CIO ausgeführt. Die Kontrolle über die Qualität, Kosten und Terminplan wird vom CSO gegenüber der Geschäftsleitung wahrgenommen.



Output:
Umsetzungsreihenfolge der Massnahmen
Welche Massnahmen werden wann und wie mit welchen Erwartungen umgesetzt?
Kosten- und Aufwandschätzung
Datensicherungsplan, Notfallplan, Wiederanlaufplan
Welche Vorkehrungen haben wir für den Notfall?

IT-Sicherheitsprozess etablieren

Input:
IT-Auditvorgaben

Der IT-Sicherheitsprozess gilt als etabliert,

- wenn das Ergebnis überprüft und der Geschäftsleitung ein periodischer Feedback in Form eines Auditreports vorliegt
- wenn das Risiko von neuen IT-Objekten in der Geschäftsleitung beurteilt werden
- wenn die Anforderung in der Verfügbarkeit, Integrität und Vertraulichkeit ändert oder sich die Schadenssumme im Grenzbereich oder Verbotsbereich verschieben, wird automatisch eine Risikoanalyse auslösen

Das IT-Risikomanagement ist somit ein kontinuierlicher Prozess im Sinne eines Regelkreises. Alle Prozesse werden von Zeit zu Zeit neu aufgesetzt, damit die technologische Veränderung in der IT Umgeben im Risikokatalog aufgenommen und von der Geschäftsleitung bewertet werden.

Output:
Auditreport (Umsetzungsgrad der Massnahmen, Datenschutzbericht)
IT-Risikobeurteilung

BEGRIFFE DER IT-SICHERHEIT

Sicherheit

Eine Begriffsbildung für die IT-Sicherheit ist der Schutz der IT-Ressourcen, die sich auf Komponenten Verfügbarkeit, Vertraulichkeit und Integrität beziehen.

Ressourcen

Die Ressourcen stellen einen Wert für den Eigentümer dar, den es gegen Bedrohungen zu schützen gilt. (IT-Systeme, Infrastruktur, Netze, IT-Anwendungen und übergreifende Aspekte)

Schutzziele

Das Schutzziel definiert das Ziel bezüglich **Verfügbarkeit**, **Vertraulichkeit** und **Integrität** bezogen auf die IT-Ressourcen.

Bedrohungen

Eine Bedrohung tritt dann auf, wenn eine Aktion oder ein Ereignis an einer IT-Ressource einen Schaden anrichten kann (höhere Gewalt, technisches Versagen, organisatorische Mängel, vorsätzliche Handlung und menschliches Fehlverhalten).

Anforderungen

Eine Anforderung beschreibt die Eigenschaft, die von einer Ressource erwartet wird auf Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Wartbarkeit und Portabilität.

Verletzlichkeit

Ein System weist eine Verletzlichkeit auf, wenn eine oder mehrere Schwachstellen die Sicherheit der IT-Ressourcen gefährden.

Massnahmen

Eine Massnahme schützt die IT-Ressource vor der Verletzlichkeit, die einen Schaden an der IT-Ressourcen anrichten könnte.

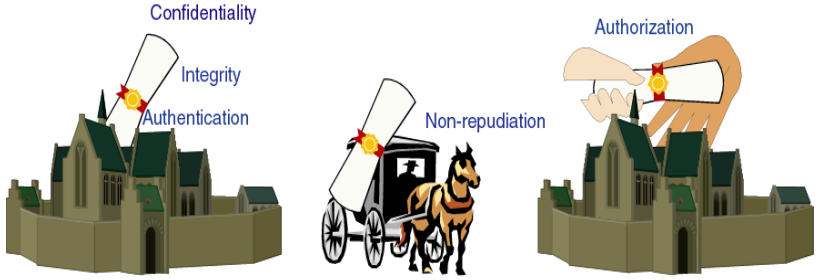
Risiko

Das Risiko ist der zu erwartende Verlust, der sich aus der Wahrscheinlichkeiten für eine bestimmte Bedrohung, der eine bestimmte Verletzlichkeit ausnutzt und zu einem bestimmten Schaden führt.

KOMMUNIKATIONSSICHERHEIT

Die Grafik zeigt die heutige Sicherheitssituation im Internet. Der rechtsfreie Raum wiederspiegelt genau den Zustand aus dem Mittelalter. Jedes Unternehmen ist somit selbst verantwortlich bezüglich Vertraulichkeit (Confidentiality) der Daten & Informationen, Integrität(Integrity), die besagt, dass die Daten & Information unversehrt bleiben gegen vorsätzlich oder unbewusste Veränderungen. Die Authentizität(Authentication) der Daten, dass diese von dem vermeintlichen Kommunikationspartner stammt, dass er derjenige ist, der er vorgibt zu sein. Die „Non – repudiation“ definiert die nicht Abstreitbarkeit oder wie wir diese aus dem Postumfeld als Empfangsbestätigung kennen. Die Authorization(Befugnis) regelt den berechtigten Zugriff auf die Daten.

Avaibility	Verfügbarkeit
Integrity	Unversehrtheit, Vollständigkeit
Authorization	Befugnis, Ermächtigung
Authentication	Beglaubigung
Confidentiality	Vertraulichkeit
Non-repudiation	Nicht-Abstreitbarkeit



Literatur

BERNSTEIN, P.L., Wider die Götter - Die Geschichten von Risiko und Risikomanagement von der Antike bis heute, München 1997

FRANK ROMEIKE/ROBERT B. FINKE (Hrsg.), Erfolgsfaktor Risiko-Management - Vermittelt Methoden und Instrumente für evolutionäre und revolutionäre Wege im Risikomanagement, Wiesbaden 2003

BSI (Bundesamt für Sicherheit in der Informationstechnik), IT-Grundschutzhandbuch, Bonn 2003

MARKUS SCHUMACHER/UTZ RÖDIG/MARIE-LUISE MOSCHGATH, Hacker Contest – Sicherheitsprobleme, Lösungen , Beispiele, Berlin; Heidelberg: Springer 2003

MICHAL WÄCHTER, Datenschutz im Unternehmen – Aktuelles Recht für die Praxis, C.H. Beck München 2003