Risikobewertung

Ein White Paper zu Definition und praktischer Vorgangsweise

Autor:
Michael Krausz, Auditor
Senior Consultant, X-IT

Version:
1.0, 23.12.2005

INHALT

1. Der Risikobegriff

a. Der klassische Risikobegriff

Der „klassische“ Risikobegriff beruht auf der Annahme, dass ein betriebswirtschaftlich hinreichendes Vorgehen daraus abgeleitet werden kann, wie sich Höhe eines erwarteten Schadens und seine Eintrittswahrscheinlichkeit verhalten. Dies führt zur Formel

$$R = H * E$$

wobei R für das in Geld gemessene Risiko steht, H für die Schadenshöhe und E für die Eintrittswahrscheinlichkeit

Die Ermittlung von Risiken auf dieser Basis bringt mehrere Probleme mit sich, die in der Praxis bereits häufig Niederschlag fanden und teilweise zu grundlegenden Änderungen in der Denkweise der betroffenen Unternehmen geführt haben.

Diese Probleme sind:

- ⇨ seltene Ereignisse mit besonders hohem Schadenswert ergeben laut Formel nur ein mittleres, wenn nicht sogar geringes Risiko. Dies führt zu einer Unterschätzung der tatsächlichen Situation, wobei die Frage des Zeitpunktes, also wann der Schaden genau eintreten wird, vollständig vernachlässigt wird, und in menschlicher Denkweise oft die Tatsache einer Wahrscheinlichkeit von zB 10^{-16} dazu verleitet, zu glauben der Schaden würde erst nach 10^{-16} Zeiteinheiten eintreten.

- ⇨ Der Faktor E liefert keinerlei mathematische Aussage über den Zeitpunkt des Eintretens des Schadens; auch Ereignisse mit besonders niedriger Wahrscheinlichkeit können bereits am nächsten Tag eintreten (aktuelle Beispiele: Bank Software Crash 2003, Tsunami 2004, Erdbeben, Vulkanausbrüche)

- ⇨ Die Formel unterscheidet die beiden Sphären (Bedrohung und Schwachstelle), die zu einem Risiko führen, nicht, daher werden Handlungspotentiale und -spielräume übersehen. Die Formel verleitet daher dazu einerseits zu viel zu tun, andererseits werden manche Risikoräume komplett übersehen bzw. sind lt. Formel nicht bearbeitungswürdig.

- ⇨ Mit dieser Formel lässt sich qualitatives Risiko (zB Rufschaden, Gefahr, Kunden zu verlieren, etc.) nicht berücksichtigen.

b. Der moderne Risikobegriff

Der moderne Risikobegriff ist abgeleitet aus der entsprechenden Literatur im Informationssicherheitsmanagement und geht davon aus, dass sich ein Risiko aus zwei Sphären (Dimensionen) zusammensetzt), die voneinander unabhängig sind und die man daher getrennt oder im Ergebnis behandeln kann.

Ein Risiko tritt dabei erst dann ein, wenn eine (stets vorhandene) Bedrohung auf eine passende Schwachstelle im Unternehmen trifft. Das Risiko kann dabei qualitativer oder quantitativer Natur sein. Erst für das Tupel aus (Schwachstelle, Bedrohung) wird eine Eintrittswahrscheinlichkeit festgelegt.

Beispiele:

Beispiel 1) Für Windows und Unix Server existieren viele bekannte Sicherheitslücken und dazugehörige Schadprogramme (auch „exploits“ genannt). Die Lebensdauer eines nicht gepatchten Windows-Server (d.h. eines neu installierten ohne Sicherheitsupdates) wurde in einer aktuellen Untersuchung mit 45 Minuten angegeben, d.h. nach 45 Minuten war der Server unter der Kontrolle von Hackern. Die erwähnten Schwachstellen sind nun auf Grund Ihrer Natur vom Betriebssystem und der installierten Software abhängig. Es existieren daher einige hundert bekannte Lücken für den Internet Explorer 6.0, die aber für jemanden, der zB Firefox verwendet vollständig irrelevant sind. Dies bedeutet, dass die Bedrohung hoch ist und ständig präsent, die Schwachstelle für den Firefox-User aber nicht existiert, daher ergibt sich im modernen Risikobegriff kein Risiko, da B=hoch, aber S=0.

Beispiel 2) Ebenso würde es sich für ein Unternehmen verhalten, dass zB ein Tandem-System einsetzt. Da es für dieses System keine bekannten exploits (oder zB auch Viren) gibt, mag zwar die Schwachstellenlage <> 0 sein, die Bedrohungslage ist aber = 0. Wiederum führt der moderne Risikobegriff zum korrekten Ergebnis von 0 Risiko. Anmerkung: In diesem Fall ist es fast eine philosophische Frage, ob S=0 oder B=0 angesetzt wird.

Beispiel 3) Angenommen ein Unternehmen setzt Internet Explorer 6.0 ein und verfügt über keine Firewall. Der Internet Explorer 6.0 sei nicht gepatcht. Daraus ergibt sich eine klare Schwachstellenlage, die gemeinsam mit der latenten Bedrohungslage zu einem hohen Risiko führt.

c. Der Risikobegriff im Informationssicherheitsmanagement

Im Informationssicherheitsmanagement geht man grundsätzlich vom modernen Risikobegriff aus (siehe oben 2b) und erweitert diesen auf die Sphären Vertraulichkeit, Verfügbarkeit und Integrität. Diese sind definiert wie folgt:

Vertraulichkeit besteht darin, dass Informationen nur denjenigen zugänglich sind, die dazu auch berechtigt sind. Diese Berechtigung muss daher beim Zugriff geprüft werden. In der Praxis werden dazu Rechtesysteme wie ADS, etc. eingesetzt oder auch besondere Verschlüsselungslösungen (PKI).

Verfügbarkeit besteht darin, dass Informationen, berechtigten Benutzern dann zur Verfügung stehen, wenn diese sie benötigen. Viele Unternehmen sehen im Schutz der Verfügbarkeit ihre höchste Priorität. Verfügbarkeit wird oft auf Hardware-Ebene realisiert.

Integrität besteht darin, dass Informationen gegen Verfälschung und Störeinflüsse geschützt werden, sodass der Inhalt der Information stets authentisch und korrekt bleibt. In der Praxis kann Integrität durch besondere Software, die integritätssichernde Algorithmen implementiert, sichergestellt werden, beispielsweise MD5.

Für die drei Sphären Vertraulichkeit, Verfügbarkeit und Integrität können nun Schwachstellen und Bedrohungen definiert werden, die zunächst zu (B,S)-Tupeln zusammengefasst werden und danach einer qualitativen und quantitativen Bewertung unterzogen werden.

2. Risikoanalyse und –bewertung

a. Risikosphären

Als Risikosphären werden jene Kategorien bezeichnet, in denen das Risiko schlagend wird, diese sind:

- ⇨ Finanzielles Risiko
- ⇨ Rechtliches Risiko (zB Risiko einer Klage, einer Verwaltungsstrafe, etc.)
- ⇨ Rufschaden

Diese Basiskategorien können um weitere für den jeweiligen Anwendungsfall erweitert werden, für IT-Abteilungen wären noch zumindest hinzuziehen:

- ⇨ Vertraulichkeit
- ⇨ Verfügbarkeit
- ⇨ Integrität

Jedes Risiko in jeder der gewählten Sphären wird nun auf die es hervorbringenden Bedrohungen und Schwachstellen untersucht. Sind alle (B,S)-Tupel ermittelt, wird das jeweilige Risiko finanziell bewertet. Daraus kann anschließend eine Prioritätsreihenfolge der Risikominimierung abgeleitet werden.
Die ermittelten (B,S)-Tupel machen es auch einfach, Ansatzpunkte für eine Risikominimierung auf Bedrohungs- oder Schwachstellenseite festzustellen.
Weiters ist es empfehlenswert, in die Risikobewertung, die Kosten der Minimierung einzubeziehen; siehe dazu auch Punkt 3c.)

b. Einfache Risikoanalyse und -bewertung

Im Rahmen einer einfachen Risikobewertung werden die (B,S)-Tupel qualitativ auf der 3-stufigen Skala „niedrig, mittel, hoch“ bewertet, wobei jede Dimension eine eigene Skala hat und daraus das Risiko nach einer eigenen Translationstabelle ermittelt wird, wobei man hier aus Definitionsgründen zwischen vielen Varianten von „lockere Handhabung“ bis „paranoid“ wählen kann. Wichtig ist, dass die Kriterien mit einer Definition unterfüttert werden, d.h. einer Erklärung, warum „niedrig“ eben „niedrig“ ist, etc. In solche Definitionen können finanzielle Parameter oder auch Wahrscheinlichkeiten (wovon eher abzuraten ist) einfließen.

Eine solche Translationstabelle mit gängigen Parametern und Definitionen kann wie folgt lauten. Das resultierende Risiko ist dabei farblich nach Ampelsystem dargestellt:

Bedrohung	Schwachstelle	Risiko
Niedrig	Niedrig	**N**
Niedrig	Mittel	**N**
Niedrig	Hoch	**N**
Mittel	Niedrig	**N**
Mittel	Mittel	**M**
Mittel	Hoch	**M**
Hoch	Niedrig	**N**
Hoch	Mittel	**H**
Hoch	Hoch	**H**

Es sei nochmals darauf hingewiesen, dass eine solche Tabelle den Unternehmensbedürfnissen angepasst werden muss. Eine Bank, Versicherung, Casino, Juwelier, etc. werden eher versuchen, auf der strengeren Seite zu sein, als zB ein Produktionsbetrieb.

c. 3stufige Matrix-Analyse

Bei einer 3stufigen Matrixanalyse werden die Risiken in eine Prioritätenreihung übergeführt, wobei in jeweils einer Matrix die folgenden Problemfelder dargestellt werden:

1. Schritt - Matrix 1: Schwachstellen und Bedrohungen ergeben Risiken
2. Schritt - Matrix 2: Risiken und Schadenspotential ergeben relevante Business-Risiken
3. Schritt - Matrix 3: Business-Risiken und Minimierungskosten ergeben eine Prioritätenreihenfolge

Jeder Matrix liegt eine Definition über den Ergebnisparameter zu Grunde, die zu Beginn festgelegt werden muss und für jede Matrix anders gestaltet sein kann. Im ersten Schritt können auch mehrere Matrizen zu bearbeiten sein, je nachdem wie viele Risikosphären (Vertraulichkeit, Verfügbarkeit, Integrität, Finanzielles Risiko, Rufschaden, Rechtliches Risiko) ausgewählt wurden. Entsprechend müssen auch die Schritte 2 und 3 auf die einzelnen Matrizen angewendet werden. Um Nachvollziehbarkeit gegenüber Auditoren, Wirtschaftsprüfern, etc. zu gewährleisten ist es auch hier notwendig, die entsprechenden Definitionen und Begründungen für eine Einordnung von (B,S)-Tupeln anzugeben.

Im Folgenden wird die Anwendung dieser Methode an einem Beispiel verdeutlicht, Ausgangspunkt ist die typische Risikolage einer Bank hinsichtlich Ihrer IT-Umgebung. In jeder Matrix kommt dabei ein situationsangepasstes Bewertungsschema zur Anwendung.

Matrix 1 – Bedrohungen, Schwachstellen, Risiken

Die Bedrohungen und Schwachstellen sowie die sich daraus ergebenden Risiken sein wie folgt gegeben:

Bedrohung ⇨ ⇩ Schwachstelle	**Bewertung 0**	**Niedrig**	**Mittel**	**Hoch**
Bewertung 0	Brand im Serverraum (1)			Bekannte Viren (2)
Niedrig		Server-Ausfall Zahlungsverkehr (3)	Fehlbedienung Server (4) Denial-of-Service der Internet-Firewall (5)	
Mittel		Eindringen in innere Firewall (6)		Neue Viren (7)
Hoch	Ungepatchtes Tandem-System (8)	Server-Ausfall FileServer Filialen (9)		

Die Eintragungen in die Tabelle werden dabei wie folgt begründet:

(1) Der Serverraum verfügt über eine Sauerstoffabsenkung. Ein Brand kann daher gar nicht mehr entstehen, daher sind B und S gleichermaßen 0.
Risiken der Anlage selbst (zB Fehleranfälligkeit, etc.) müssten zusätzlich getrennt berücksichtigt werden.

(2) Ein 4stufiges Vienschutzkonzept (File-Server, Clients, Mail,. http) ist in Kraft, die Scanner verwenden tägliche Updates. Daher können bekannte Viren nicht mehr in das System eindringen. Das grundsätzliche Bedrohungspotential ist HOCH, da zu jedem Zeitpunkt unzählige Viren kursieren, es existiert jedoch keine Schwachstelle auf Grund des installierten Virenschutzes.

(3) Ein Ausfall der Server für den Zahlungsverkehr wird auf Grund der Verwendung eines Clusters sowie des guten Wartungs- und Pflegeszustandes sowie der klimatischen Bedingungen (gute Lüftung und Kühlung) mit niedriger Schwachstelle und niedriger Bedrohung angenommen.

(4) Würden die Server falscher Bedienung unterworfen, so wird hier mittlere Bedrohungslage angenommen jedoch abgefedert durch gute Ausbildung der Mitarbeiter, woraus eine niedrige Schwachstellenlage folgt.

(5) Da nicht ausgeschlossen werden kann, dass die Firewall zum Internet einer DoS-Attacke unterzogen wird, wird mittlere Bedrohung angenommen. Jedoch ist die Firewall mit einem Traffic-Shaper ausgestattet, sodass eine Gegenmaßnahme existiert und daher nur niedriges Schwachstellenniveau angenommen werden muss.

(6) Dass in die innere Firewall eingedrungen wird, ist zwar auf Grund der inneren Lage erschwert, wodurch von nur niedriger Bedrohungslage auszugehen ist, die Firewall wurde aber seit 6 Monaten nicht mehr gepatcht, sodass eine mittlere Schwachstellenlage existiert.

(7) Da gegen neue Viren keine a priori Schutzmaßnahmen greifen, jedoch das Unternehmen über Support-Verträge gut vorgesorgt hat, ist die Bedrohungslage hoch, die Schwachstellenlage aber nur mittel.

(8) Da das zentrale Tandem-System nicht gepatcht wurde, dafür aber keine Bedrohungen bekannt sind, ist die Schwachstellenlage zwar hoch, die Bedrohungslage aber 0.

(9) Da die Server für die Filialen nicht öffentlich zugänglich und in gutem Wartungszustand sind, jedoch keinerlei Ausfallsicherheit unterliegen, ist das Bedrohungspotential niedrig, das Schwachstellenpotential jedoch hoch.

Auswertung der Matrix

Aus der in der Matrix per definitionem getroffenen Risikoeinteilung ergeben sich nun folgende Risiken:

Niedriges Risiko für die Tupel: (1), (2), (3), (8)
Mittleres Risiko für die Tupel: (4), (5), (6)
Hohes Risiko für die Tupel: (7), (9)

Zu beachten ist, dass die Matrixeinteilung „vorsichtig“ vorgenommen wurde, sodass zB (B,S) = (hoch, mittel) und (B,S)=(niedrig, mittel) bereits als hohes Risiko eingestuft wurde.

Die Ergebnisse dieser Matrix bilden nun den Ausgangspunkt für Matrix 2, die als Ergebnis die relevanten Business-Risiken ergibt.

Matrix 2 – Risiken und Schadenspotential

In Matrix 2 werden nun die ermittelten Risiken, den für das jeweilige Risiko anzunehmenden Schadenspotential gegenübergestellt. Das Schadenspotential sollte dabei nicht bloß „angenommen" werden, sodern, wo möglich, mit präzisen Berechnungen untermauert werden. Folgende Größen können dabei berücksichtigt werden:

- ⇨ Kosten von Überstunden zur Behebung des Schadens
- ⇨ Hardwarekosten (Wiederbeschaffung, temporäre Miete, etc.)
- ⇨ sonstiger Sachschaden
- ⇨ Personenschäden und Ersatzleistungen
- ⇨ Verfahrenskosten bei gerichtlichen Verfahren
- ⇨ potentielle Strafen

Die in Matrix 1 ermittelten Risiken wurden nun wie folgt bewertet:

Risiko ⇨ ⇩Schadenspotential pro Jahr	**Bewertung 0**	**Niedrig**	**Mittel**	**Hoch**
0 – € 10.000			(4) Fehlbedienung (5) Internet Firewall	
€ 10.001 - € 100.000	(2) Viren (3) Server Ausfall (8) Tandem		(6) Eindringen in Firewall	(7) Neue Viren
€ 100.001 - € 500.000				(9) Server-Ausfall
> € 500.000	(1) Brand			

Auswertung

Aus Matrix 2 ergibt sich nun die folgende Relevanzreihung der ermittelten Risiken:

1. Keine Risiken hoher Relevanz
2. 3 Risiken mittlerer Relevanz: (6), (7), (9)
3. 7 Risiken niedriger Relevanz: (1) bis (6) und (8)

Die Begründungen dazu ergeben sich wie folgt:

(1), (2), (3), (8): Da diese bereits als 0-Risiko bewertet wurden, ergibt sich auch im Falles des Brandes mit hohem Schadenspotential kein relevantes Risiko. 0-Risiken sollten nicht einfach aus der Behandlung in Matrix 2 gestrichen werden, da auch das Festlegen eines Schadenspotentials wichtige operative Einsichten bringen kann. Außerdem kann je nach Festlegen der Definitionsskala auch bereits mittlere Relevanz vorliegen.

(4), (5): In diesem Fällen ist die Schadenshöhe so gering, dass keine höhere Risikostufe gerechtfertigt erscheint.

(6): Ein Eindringen in die interne Firewall könnte andere betriebskritische Systeme kompromittieren und Kosten durch Neuinstallation auslösen.

(7): Da ein neuer Viren hohe Auswirkungen auf Systeme haben kann, aber typischerweise rasch in den Griff zu bekommen ist wurde nur eine mittlere Schadensstufe angenommen.

(9): Ein Server-Ausfall für die Filialsysteme wurde in eine hohe Schadensklasse eingereiht, da ein potentieller Stillstand aller Filialsysteme angenommen wurde.

Mit den Ergebnissen aus Matrix 2 kann nun eine Prioritätsreihenfolge in Matrix 3 erarbeitet werden, dabei kann man wahlweise nach Zeit oder finanziellem Aufwand vorgehen; eine Vorgangsweise nach finanziellem Aufwand ist oft praktischer.

Matrix 3 – Business-Risiken und Minimierungskosten

Relevanzklasse ⇨ ⇩Minimierungseinsatz	**Niedrig**	**Mittel**	**Hoch**
0 – € 10.000	(1), (2), (3) (4), (5), (6) (8)	(7) Neue Viren	
€ 10.001 - € 100.000			
€ 100.001 - € 500.000		(9) Server-Ausfall	
> € 500.000			

<u>Auswertung der Matrix</u>

Die Auswertung ergibt nun als erstes Ergebnis:
Es liegen nur mittlere und niedrige Minimierungskosten vor.

Das zweite Ergebnis ist eine *Priorisierungsreihenfolge*, die wie folgt lautet.
1. Behebungspriorität: (9) durch Aufbau redundanter Systeme
2. Behebungspriorität: (6) und (8) durch Installieren von Patches
3. Behebungspriorität: (1) bis (5) und (7); es werden keine Kosten anfallen, da eine Minimierung nicht notwendig/möglich ist.

Die Begründungen lauten im Einzelnen wie folgt:
(9) Einem Serverausfall der Filialsysteme kann durch Redundanz hinsichtlich Verfügbarkeit vorgebeugt werden, woraus sich Kosten für Hardware, Software und Arbeitszeit ergeben.
(8) Patches zu installieren ist ein einfacher und kostengünstiger Weg, das Risiko weiter zu verringern.
(6) Ein Installieren von Patches auf der inneren Firewall ist kostengünstig möglich.
(2) bis (5): Die Risiken sind bereits minimal und können nicht weiter minimiert werden.
(1) und (7): Bei diesen Risiken kann ein Mitteleinsatz nicht sinnvoll erfolgen bzw. würde, selbst wenn er stattfindet, keine weitere Minimierung bringen.

3. Normen und Best Practices

Die folgenden Normen und Best Practices können als Ausgangspunkte und Arbeitshilfen betrachtet werden:

1.) ISO 17799 / ISO 27001 (Norm)
2.) ISO 15504 (Norm)
3.) CoBIT / COSO (Best Practice)
4.) Grundschutzhandbuch, Risikoliste (Best Practice)
5.) Österreichische Sicherheitshandbücher (Best Practice)
6.) ÖNORM A7799 (Norm)
7.) ÖNORM A 17700 (Norm)