

Zusammenfassung

Gute Kenntnisse über die Risiken und die Durchführung eines Bewertungsverfahrens der Risiken sind unerlässlich bei der Errichtung einer sicheren EDV-Lösung. Jüngste Untersuchungen haben gezeigt, dass die Mehrheit der EDV-Verantwortlichen nicht angeben kann, in welchem Maß ihre EDV-Lösung [Risiken] ausgesetzt ist, und sie noch weniger in der Lage sind, das

[Risiko], dem sie ausgesetzt sind, finanziell einzuschätzen.

Dieser Abschnitt soll Antworten auf folgende Fragen liefern:

- Was ist ein Risiko im EDV-Bereich?
- Warum sind gute Kenntnisse über die Risiken so wichtig?
- Welche allgemeinen Risiko-Bewertungsverfahren gibt es?

Inhalt

- 1 Der Begriff Risiko in der EDV →
- 2 Die Bedeutung der Messung der Risiken →
- 3 Die Schulen →
- 4 Die Metrik der Risiken →
- 5 Die Pareto-Regel →



1 Der Begriff Risiko in der EDV

Das Risiko kann durch folgende Gleichung beschrieben werden: Risiko = Verwundbarkeit x Bedrohung x Auswirkung. Diese Elemente sind die Grundkomponenten des Risikos (sie werden in anderen Abschnitten ausführlich beschrieben).

- ➔ Die «**Bedrohungen**» bezeichnen alle (im Allgemeinen externe) Elemente, die die EDV-Ressourcen eines Unternehmens angreifen können.
- ➔ Die «**Verwundbarkeit**» bezeichnet alle Sicherheitslücken der EDV-Ressourcen, die von den Bedrohungen genutzt werden können, um die Ressourcen zu gefährden.

- ➔ Die «**Auswirkung**» ist das Ergebnis der Ausnutzung einer Verwundbarkeit durch eine Bedrohung und kann verschiedene Formen annehmen: finanzieller Verlust, Beeinträchtigung des Markenimages, Verlust der Glaubwürdigkeit etc.

> Die Kombination dieser drei Faktoren bildet das "Risiko". Dieser Wert ermöglicht vor allem die Einschätzung der finanziellen Auswirkungen und/oder der Wahrscheinlichkeit des Auftretens eines unerwünschten Ereignisses. Die Berechnung eines Risikos soll die Bewertung bekannter oder unbekannter Ereignisse ermöglichen, die die Integrität der EDV-Ressourcen eines Unternehmens beeinträchtigen können, um in der Folge Gegenmaßnahmen ergreifen zu können.

2 Die Bedeutung der Messung der Risiken

Hinsichtlich der EDV-Systeme ist die Messung der Risiken und deren Bewertung wichtig, da sie folgendes ermöglichen:

- ➔ **Identifizierung der Sicherheitslücken**

Die Sicherheitslücken lassen sich auf der Ebene der EDV-Ressourcen (Infrastruktur, Anwendungen etc.) aber auch auf organisatorischer Ebene (Sicherheitspolitik, Verfahren etc)

erkennen. Manchmal ermöglicht die Bewertung der mit einem Element der EDV-Architektur verbundenen Risiken die Aufdeckung von Sicherheitslücken in der globalen Datenverarbeitung des Unternehmens.

→ Einschätzung des Werts der EDV-Elemente

Um eine Bewertung der Risiken durchführen zu können, ist es erforderlich, den Wert der verschiedenen EDV-Ressourcen zu ermitteln. Alle wichtigen EDV-Ressourcen müssen bewertet werden.

→ Festlegung der Prioritäten der Sicherheitsmaßnahmen

Um die Prioritäten in Bezug auf die Schutzmaßnahmen festlegen zu können, ist es erforderlich, eine Identifizierung, Bewertung und einen Vergleich der Risiken, denen das Unternehmen ausgesetzt ist, durchzuführen.

→ Entwicklung von Know-how

Die Anwendung von Standardverfahren zur Bewertung der Risiken ermöglicht es, von der Erfahrung von EDV-Experten zu profitieren und zu wertvollen Schlussfolgerungen zu gelangen. Dies gilt insbesondere dann, wenn man selbst Laie auf diesem Gebiet ist.

→ Festlegung einer angemessenen Sicherheitspolitik

Nur eine ausführliche Auswertung der Risiken ermöglicht es, eine Vorstellung von den möglichen finanziellen Auswirkungen auf das Unternehmen zu entwickeln und folglich eine Lösung hinsichtlich der Sicherheit der EDV- und Kommunikationssysteme zu implementieren, die eine angemessene Investitionsrentabilität gewährleistet.

3

Die Schulen

Zunächst einmal ist es erforderlich, den Unterschied zwischen einem Audit und einer Bewertung im Bereich der EDV-Sicherheit eindeutig festzulegen:

Die Bewertung oder das "Assessment" ist eine Messung des Zustands der EDV-Sicherheit, die nicht unbedingt einen Vergleich mit Standards oder gesetzlichen Vorschriften umfasst.

Der Audit hat zum Ziel, das Niveau der EDV-Sicherheit in Bezug auf eine Norm oder gesetzliche Vorschriften zu ermitteln. Ein "Assessment" kann eine der Phasen dieses Audits sein.

3.1 Die Sichtweise der Prüfer

Die von den bedeutendsten Prüfungsgesellschaften angewandten Verfahren umfassen eine Vielzahl von "Checklisten", die eine Kontrolle der EDV-Systeme aber auch der globalen Verwaltung des Unternehmens ermöglichen.

Diese Verfahren umfassen häufig einen Vergleich mit Musterverfahren (Best Business Practice). Zu den bekanntesten Verfahren gehören: COBIT (Control Objectives for Information and related Technology), FISCAM (Federal Information System Controls Audit Manual), CISA (Computer Information Systems and Analyses).

3.2 Die Sichtweise der Informatiker

Das in der Informatik angewandte Verfahren lautet TBS (Time Based Security). Im Gegensatz zu traditionellen Audit-Verfahren versucht diese Methode nicht, die folgende Frage zu beantworten: "Wie kann ich ermitteln, wo ich mich im Verhältnis zu den Branchenstandards befindet? TBS hat die Ermittlung der Widerstandsfähigkeit der Lösung gegenüber Attacken zum Ziel. Dieses Verfahren ermöglicht es, die Lebensfähigkeit einer Lösung in Form einer Dauer anzugeben und die potenziellen oder tatsächlichen finanziellen Verluste zu beziffern.

4

Die Metrik der Risiken

4.1 Quantitative Bewertung der Risiken:

Diese Methode hat zum Ziel, das Risiko in Bezug auf die Finanzen und die Frequenz anzugeben.

Wenn man das Risiko auf diese Weise misst, ist es möglich, die finanzielle Bewertung der Risiken, denen das Unternehmen ausgesetzt ist, mit den Kosten für die Durchführung von Schutzmaßnahmen zu vergleichen.

Diese Methode basiert auf der folgenden Formel:

Potenzieller Verlust pro Jahr =
Wert des dem Risiko ausgesetzten Elements x Expositions-
faktor x Einschätzung der Häufigkeit des Auftretens des
Ereignisses pro Jahr.

Man kann also von einer Bewertung der Investitionsrentabilität sprechen (ROI = Return On Investment).

Der "Wert des dem Risiko ausgesetzten Elements" gibt die finanzielle Bewertung des Elements an, das vom Ereignis betroffen sein kann.

Der "Expositionsfaktor" bezeichnet den Teil des Elements, der im Fall einer Katastrophe dem Risiko ausgesetzt ist.

Die **"Einschätzung der Häufigkeit des Auftretens des Ereignisses pro Jahr"** ist eine Einschätzung, wie oft das Ereignis pro Jahr auftreten kann.

Die **"Einschätzung der Häufigkeit des Auftretens des Ereignisses pro Jahr"** ist eine Einschätzung, wie oft das Ereignis pro Jahr auftreten kann.

4.2 Qualitative Bewertung der Risiken

Diese Methode hat die Ermittlung und Bewertung der Risiken untereinander zum Ziel.

Beim «Wert des dem Risiko ausgesetzten Elements» handelt es sich im Bereich der EDV-Risiken um den jeweils zu schützenden Wert.

Der «Verwundbarkeits-Index» gibt den Grad der Verwundbarkeit an, d.h. inwiefern das Element dem Risiko ausgesetzt ist. Falls bereits Sicherheitselemente implementiert worden sind, so ist dieser Index das Abbild der nativen Verwundbarkeit, gewichtet mit den bereits implementierten Sicherheitsmaßnahmen.

«Die Bedrohung» ist eine Einschätzung der Anzahl von Angriffen, denen das Element potenziell ausgesetzt ist.

Zu Beginn dieser Bewertung wird eine Matrix erstellt, welche die verschiedenen Kombinationen (Hoch, Mittel, Gering) der Komponenten sowie das Ergebnis dieser Kombinationen angibt.

Beispiel einer Matrix:

- ➔ HOHER Wert x HOHE Verwundbarkeit x HOHE Bedrohung= HOHES RISIKO
- ➔ HOHER Wert x MITTLERE Verwundbarkeit x HOHE Bedrohung= HOHES RISIKO
- ➔ HOHER Wert x GERINGE Verwundbarkeit x HOHE Bedrohung= MITTLERES RISIKO

4.3 Bewertungsbeispiel

Ausgegangen wird von der Einschätzung des Risikos in Bezug auf folgende Sachlage "Geld auf dem Boden eines öffentlichen Parks liegen lassen". Der Wert des dem Risiko ausgesetzten Elements lässt sich beziffern, da es sich um die im Park auf dem Boden liegende Geldsumme handelt. Die Sicherheitslücke ist hoch, da der Ort für jedermann einsehbar und zugänglich ist. Die Bedrohung ist groß, da sich jede Person im Park des Geldes bemächtigen könnte.

Ergebnis:

- ➔ HOHER Wert x HOHE Verwundbarkeit x HOHE Bedrohung= HOHES RISIKO

5

Die Pareto-Regel

Die 80:20-Regel ist auch auf das Management der Risiken im Zusammenhang mit der elektronischen Datenverarbeitung anwendbar. Sie besagt, dass 80% der Risiken durch 20% der erforderlichen Investitionen abgedeckt werden können. Angesichts der Tatsache, dass die Sicherheit von EDV- und Kommunikationssystemen niemals lückenlos ist, muss dieses Prinzip, das als ein Fürsorgepflicht-Verfahren betrachtet werden kann, unbedingt angewandt werden.