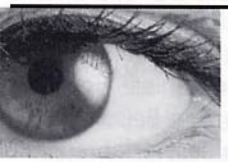
Risikoanalyse



Die Planung und Durchführung von Risikoanalysen führt nur bei einer methodischen Vorgehensweise zum Erfolg.

ALEXANDER GESCHONNECK, BERLIN*

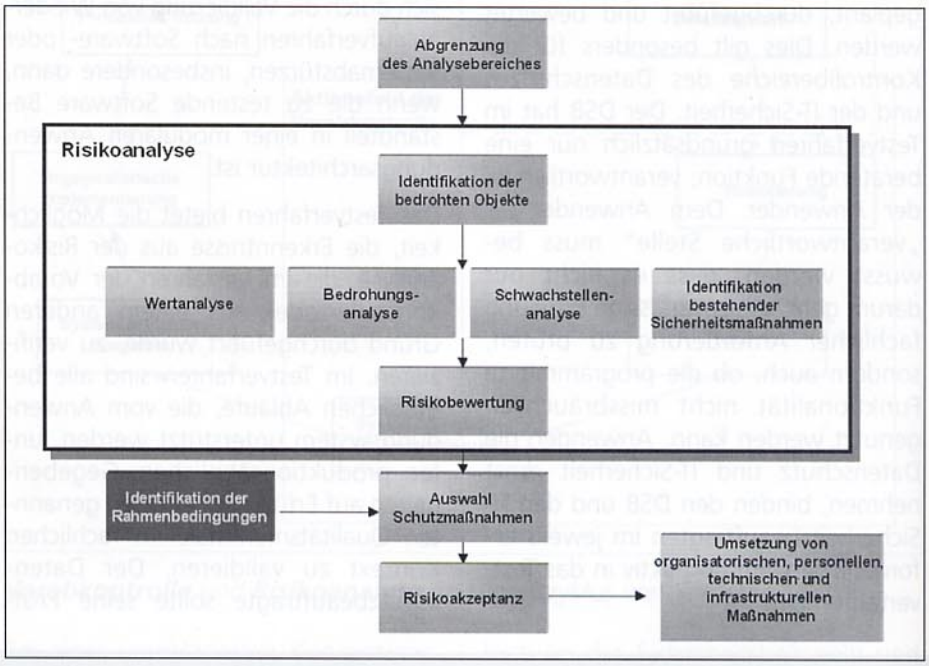
Eine wesentliche Voraussetzung für erfolgreiches IT-Sicherheitsmanagement ist die Einschätzung der bestehenden Sicherheitsrisiken. In einer Sicherheitsanalyse wird versucht, diese Risiken zu erkennen und zu bewerten und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird. Es ist empfehlenswert, eine Strategie zur Sicherheitsanalyse festzulegen. Diese sollte für die gesamte Organisation gültig sein und festlegen, wie die Ziele der Sicherheitsanalyse – Erkennen und Bewerten von Einzelrisiken und Gesamtrisiko – erreicht werden sollen. Der folgende Beitrag beschreibt den idealtypischen Ablauf einer Risikoanalyse. Das Konzept ist praxiserprobt.

Grundprinzipien

Unabhängig von der gewählten Strategie gelten für Risikoanalyseverfahren allgemeine Grundprinzipien:

- ▷ Das gesamte Testverfahren muss transparent gemacht werden.
- ▷ Es dürfen keine versteckten Annahmen gemacht werden, die z.B. dazu führen, dass Bedrohungen unbetrachtet bleiben.
- ▷ Alle Bewertungen müssen begründet werden, um subjektive Einflüsse zu erkennen und so weit wie möglich zu vermeiden.
- ▷ Alle Schritte müssen so dokumentiert werden, dass sie später auch für andere nachvollziehbar sind. Ein derartiges Vorgehen erleichtert auch die Überarbeitung des daraus resultierenden IT-Sicherheitskonzeptes zu einem späteren Zeitpunkt.
- ▷ Der Aufwand für die Durchführung des Verfahrens sollte dem Wert der betrachteten IT-Anwendungen und dem Bedrohungspotenzial der Organisation im Allgemeinen angemessen sein.

Eine detaillierte Risikoanalyse für ein IT-System umfasst die Identifikation der bestehenden Risiken sowie eine Abschätzung ihrer Größe.



***Ablaufstruktur** Risikoanalyse*

Ablaufstruktur

Durch die Ablaufstruktur wird das Verfahren der Risikoanalyse methodisiert und in einzelne Schritte oder Phasen unterteilt. Jeder Schritt bzw. jede Phase beschreibt ein klar definiertes Arbeitspaket. Das Schritt- oder Phasenmodell zwingt zu einer konsequenten Vorgehensweise mit Prüfung auf Erreichung der schritt- bzw. phasenbezogenen Ziele spätestens am Ende des jeweiligen Arbeitspaketes. Grundsätzlich gilt, dass ein Folgeschritt bzw. eine Folgephase nur begonnen werden darf, wenn die Ziele der vorhergehenden Arbeitspakete erreicht wurden.

INHALT:

- Grundprinzipien
- Ablaufstruktur
- Abgrenzung des Analysebereiches
- Identifikation der bedrohten Objekte
- Wertanalyse
- Bedrohungsanalyse
- Schwachstellenanalyse
- Identifikation bestehender Sicherheitsmaßnahmen
- Risikobewertung

* Alexander Geschonneck ist als Senior Security Consultant bei der HiSolutions AG für eine Vielzahl technischer und organisatorischer Sicherheitsanalysen verantwortlich. Er kann unter geschonneck@hisolutions.com erreicht werden.

Der klassische Ablauf einer detaillierten Risikoanalyse nach CRAMM (CCTA[1] Risk Analysis and Management Method) teilt sich in sieben grobe Schritte.

Abgrenzung des Analysebereiches

Vor Beginn einer Risikoanalyse ist es erforderlich, den zu analysierenden Bereich genau abzugrenzen. Dabei ist anzugeben, ob sich die Analyse auf Hardware, Software und Daten des betrachteten IT-Systems beschränkt oder ob und in welchem Ausmaß andere Werte wie Gebäude und Infrastruktur, Personen, immaterielle Güter, Fähigkeiten und Leistungen einbezogen werden sollen. Es ist hier unbedingt empfehlenswert nicht die IT als Selbstzweck zu betrachten, sondern als geschäftsprozessunterstützende Einheit. Letztendlich ist es für ein Unternehmen nebensächlich, mit welchen Servern und Anwendungen die Leistungserbringung ermöglicht wird, wenn die Kernprozesse des Unternehmens reibungslos und wirtschaftlich funktionieren. Aus diesem Grunde ist es empfehlenswert, bei der Risikoanalyse diese Prozesse nicht aus dem Auge zu verlieren und zum Gegenstand einer Risikoanalyse zu machen.

Identifikation der bedrohten Objekte

In diesem Schritt sind alle bedrohten Objekte, die innerhalb des festgestellten Analysebereiches liegen, zu erfassen. Unter den bedrohten Objekten einer Organisation ist alles zu verstehen, was für diese schutzbedürftig ist, also alle Objekte, von denen der Betrieb des IT-Systems und seine Anwendungen und damit die Funktionsfähigkeit der Organisation abhängen. Beispiele für bedrohte Objekte sind:

- ▷ physische Objekte: Gebäude, Infrastruktur, Hardware, Datenträger, Dokumente, ...
- ▷ logische Objekte: Software, Daten, Information, ...
- ▷ Personen: Know-how-Träger, Führungskräfte, Administrationspersonal, ...
- ▷ Fähigkeiten: Herstellen eines Produktes, Erbringen einer Dienstleistung, ...
- ▷ immaterielle Güter: Image, Vertrauen in die Institution, gute Beziehungen zu anderen Organisationen, ...

Zwischen den bedrohten Objekten bestehen grundsätzlich komplexe Abhängigkeiten. Vertraulichkeit, Integrität oder Verfügbarkeit eines Objektes setzt vielfach die Vertraulichkeit, Integrität oder Verfügbarkeit eines anderen Objektes voraus. Beispiele dafür sind etwa die Erfordernis einer funktionsfähigen Infrastruktur (Stromversorgung, Klimaanlage,...) für den Betrieb eines IT-Systems, die Abhängigkeit der Software von unversehrter und verfügbarer Hardware oder die Voraussetzung korrekter Applikations- und Betriebssystemsoftware für die Integrität der Anwendungsdaten, die Anwesenheit von Systemadministratoren für das Einleiten von Datenwiederherstellungsmaßnahmen.

Die Identifizierung der bedrohten Objekte sowie ihre nachfolgende Bewertung stellen wesentliche Voraussetzungen für ein erfolgreiches IT-Sicherheitsmanagement dar. Dabei ist es den Erfordernissen im Einzelfall anzupassen, in welcher Tiefe und in welchem Detaillierungsgrad die einzelnen Objekte analysiert werden sollen. In vielen Fällen ist eine Zusammenfassung in Gruppen sinnvoll und kann den Analyseaufwand begrenzen.

Wertanalyse

In diesem Schritt wird der Wert der im vorangegangenen Schritt identifizierten Objekte ermittelt. Um eine sinnvolle Bewertung vornehmen zu können, ist es nötig eine sinnvolle Bewertungsbasis zu schaffen. Diese Bewertungsbasis dient der einheitlichen Einschätzung der in den bedrohten Objekten enthaltenen Werten. Mitunter sind hierfür unterschiedliche Verfahren heranzuziehen. In den meisten Fällen werden folgende Aktionen durchgeführt:

- ▷ Festlegung der Bewertungsbasis für Sachwerte und immaterielle Werte,
- ▷ Ermittlung der Abhängigkeiten zwischen den Objekten,
- ▷ Bewertung der bedrohten Objekte.

Bei der Bestimmung der Bewertungsbasis sollte festgelegt werden, ob die Bewertung qualitativ oder quantitativ zu erfolgen hat. So kann eine quantitative Bewertung z.B. auf

- ▷ dem Zeitwert eines Objektes,
- ▷ dem Wiederbeschaffungswert eines Objektes,
- ▷ dem Wert, den das Objekt für einen potenziellen Angreifer hätte, oder
- ▷ dem Schaden, der sich aus dem Verlust oder der Modifikation eines zu schützenden Objektes für die betroffene Organisation ergibt

beruhen.

Bei immateriellen Werten könnte dies der Wert sein, den das Objekt für einen potenziellen Angreifer hätte (z.B. vertrauliche Information). Ein anderer Faktor ist z.B. der Schaden, der sich aus einem Angriff auf das zu schützende Objekt für die betroffene Organisation ergibt. Die Verwendung von quantitativen Bewertungen kann sicherlich weiter sensibilisierend auf das Management wirken, wenn es darum geht, die Ergebnisse der Risikoanalyse mit konkreten risikominimierenden oder – überwälzenden Maßnahmen zu unterlegen. Schwierigkeiten ergeben sich aber regelmäßig, wenn durch die Verwendung von Zahlen eine Scheingenauigkeit vorgegaukelt wird, die so nicht existiert. Aus diesem Grunde ist auch eine qualitative Bewertung der Objektwerte möglich.

Sinnvoll ist hier eine Einteilung in drei bis fünf Klassen:

4 = sehr hoch,
3 = hoch,
2 = mittel,
1 = gering,
0 = unbedeutend

Mit Ausnahme der Festsetzung von Zeit- oder Wiederbeschaffungswert wird die Bewertung von bedrohten Objekten sehr subjektiv sein. Es ist daher notwendig, im Rahmen der Analyse möglichst genaue Bewertungsbasen und Regeln vorzugeben und diese eventuell durch Beispiele zu illustrieren. Weiterhin sollten möglichst viele unterschiedliche Personen (Betroffene

[1] Central Computer and Telecommunications Agency der Britischen Regierung

und Verantwortliche) nach ihrer Einschätzung befragt werden. Dies ermöglicht es, Probleme bei der Selbsteinschätzung der Wichtigkeit zu vermeiden. Die Person, die die Risikoanalyse durchführt, erstellt eine Liste der zu bewertenden Objekte und gibt die Bewertungsbasen mit Beispielen vor. Es ist Aufgabe desjenigen, der die Risikoanalyse durchführt, die einzelnen Bewertungen auf Plausibilität und Konsistenz zu prüfen und ein konsolidiertes Ergebnis zu erarbeiten.

Bedrohungsanalyse

Nach ISO 13335 ist eine Bedrohung ein möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden für ein System oder die Organisation führen kann.

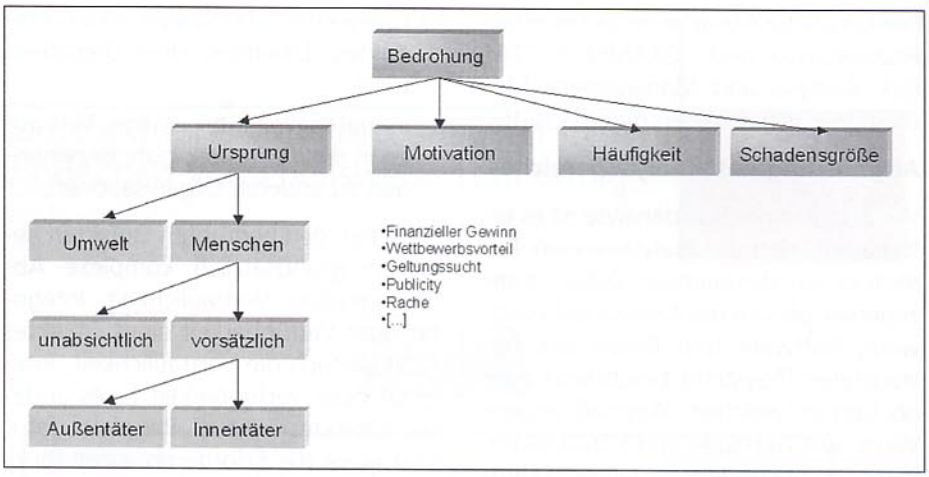
Die zu schützenden Objekte sind vielfältigen Bedrohungen ausgesetzt. Im Rahmen der Risikoanalyse müssen diese nun identifiziert werden; zusätzlich ist ihre Schwere und Eintrittswahrscheinlichkeit abzuschätzen. Daraus ergeben sich dann die beiden Hauptaktionen:

- ▷ die Identifikation möglicher Bedrohungen und
- ▷ die Ermittlung der Eintrittswahrscheinlichkeiten.

Grundsätzlich ist es wichtig sich mit der Charakterisierung von Bedrohungen vertraut zu machen.

Zusätzlich können Bedrohungen unterteilt werden in:

- ▷ höhere Gewalt (etwa Blitzschlag, Feuer, Erdbeben, Personalausfall),
- ▷ organisatorische Mängel (etwa fehlende oder unzureichende Regelungen für Wartung, Dokumentation, Test und Freigabe, fehlende Auswertung von Protokolldaten, mangelhafte Kennzeichnung von Datenträgern),
- ▷ menschliche Fehlhandlungen (etwa fehlerhafte Systemnutzung oder -administration, fahrlässige Zerstörung von Geräten oder Daten, Nichtbeachtung von Sicherheitsmaßnahmen),
- ▷ technisches Versagen (etwa Ausfall von Versorgungs- und Sicherheitseinrichtungen, Softwarefehler, defekte Datenträger),
- ▷ vorsätzliche Handlungen (etwa Manipulation/Zerstörung von Geräten, Manipulation an Daten oder Software, Viren, trojanische Pferde, Abhören, Wiedereinspielen von Nachrichten, Nichtanerkennen einer Nachricht, Maskerade).



*Charakterisierung von **Bedrohungen***

Es ist wichtig, alle wesentlichen Bedrohungen zu erfassen, da andernfalls Sicherheitslücken bestehen bleiben können. Bei der Identifikation von möglichen Bedrohungen können Bedrohungskataloge hilfreich sein, die den Charakter von Checklisten haben. Es ist jedoch zu betonen, dass keine derartige Liste vollständig sein kann, und darüber hinaus auch Bedrohungen einem ständigen Wandel und einer ständigen Weiterentwicklung unterworfen sind. Es ist daher immer notwendig, über Bedrohungskataloge hinaus auch die Möglichkeit weiterer Bedrohungen in Betracht zu ziehen. In diesem Schritt der Risikoanalyse ist auch zu überlegen, von wem eine Bedrohung jeweils ausgehen kann (etwa Mitarbeiter, Leasingpersonal, Externe). Der Schutz gegen Innentäter ist mit technischen Maßnahmen oft nur unzureichend oder mit sehr hohem Aufwand zu bewerkstelligen, hier wird in verstärktem Maß auf personelle und organisatorische Maßnahmen zurückzugreifen sein.

Im weiteren Verlauf ist zu bestimmen, mit welcher Wahrscheinlichkeit eine Bedrohung im betrachteten Umfeld eintreten wird. Diese ist abhängig von:

- ▷ der Häufigkeit der Bedrohung (Wahrscheinlichkeit des Auftretens anhand von Erfahrungen, Statistiken, ...),
- ▷ der Motivation und den vorausgesetzten Fähigkeiten und Ressourcen eines potenziellen Angreifers,
- ▷ Einschätzung der Attraktivität und Verwundbarkeit des IT-Systems bzw. seiner Komponenten,
- ▷ Umweltfaktoren und organisationsspezifischen Einflüssen.

Eintrittswahrscheinlichkeiten können ebenfalls qualitativ und quantitativ beschrieben werden. Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuschen könnte, die durch die ungenaue Methode der Schätzung nicht zu rechtfertigen ist, ist eine qualitative Bewertung empfehlenswert: 4 = sehr häufig, 3 = häufig, 2 = mittel, 1 = selten, 0 = sehr selten.

Die allgemeinen Bedeutungen der Skalenwerte können für spezifische Anwendungsbereiche konkretisiert werden. Im Allgemeinen werden sie dann in „Anzahl pro Zeiteinheit" angegeben. Sie sollten dann so festgelegt werden, dass die Bedeutung der Ziffern von 0 bis 4 gleichmäßig zunimmt: 4: einmal pro Minute 3: einmal pro Stunde 2: einmal pro Tag 1: einmal pro Monat 0: einmal im Jahr.

Es kann durchaus sinnvoll oder sogar erforderlich sein, für verschiedene Anwendungsbereiche unterschiedliche Auslegungen der Werteskala zu definieren. Auch hier sei nochmals erwähnt, dass der Anschein einer Schein-

genauigkeit vermieden werden sollte. Denkbar wäre hier auch der Ansatz mit pauschalisierten Eintrittswahrscheinlichkeiten zu arbeiten.

Schwachstellenanalyse

Unter einer Schwachstelle (Vulnerability) versteht man eine Sicherheitsschwäche eines oder mehrerer Objekte, die durch eine Bedrohung ausgenutzt werden kann. Schwachstellen können etwa bei Gebäuden, Hardware, Software, in der Organisation und Verwaltung sowie beim Personal auftreten. Typische Beispiele für Schwachstellen sind etwa:

- ▷ mangelnder baulicher Schutz von Räumen mit IT-Einrichtungen,
- ▷ nachlässige Handhabung von Zutrittskontrollen,
- ▷ Spannungs- oder Temperaturschwankungen,
- ▷ kompromittierende Abstrahlung,
- ▷ Spezifikations- und Implementierungsfehler,
- ▷ schwache Passwortmechanismen,
- ▷ unzureichende Dokumentation und Prozessbeschreibungen,
- ▷ unzureichende Ausbildung, mangelndes Sicherheitsbewusstsein.

Eine Schwachstelle selbst verursacht noch keinen Schaden, sie ist aber die Voraussetzung, die es einer Bedrohung ermöglicht, wirksam zu werden und damit ein IT-System zu beeinträchtigen. Auf Schwachstellen, für die eine korrespondierende Bedrohung existiert, sollte sofort reagiert werden.

Eine Schwachstellenanalyse ist die Überprüfung von Sicherheitsschwächen, die durch festgestellte Bedrohungen ausgenutzt werden können. Diese Analyse muss sowohl das Umfeld als auch bereits vorhandene Schutzmaßnahmen miteinbeziehen. Es ist wichtig, jede Schwachstelle daraufhin zu bewerten, wie leicht es ist, sie auszunutzen.

Identifikation bestehender Sicherheitsmaßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die eine oder mehrere der nachfolgenden Funktionen erfüllen (sinnvoll in Kombination):

- ▷ Vermeidung von Risiken,
- ▷ Verkleinerung von Bedrohungen oder Schwachstellen,
- ▷ Entdeckung unerwünschter Ereignisse,
- ▷ Eingrenzung der Auswirkungen eines unerwünschten Ereignisses,
- ▷ Überwälzung von Risiken oder
- ▷ Wiederherstellung eines früheren Zustandes.

Im Rahmen dieses Schrittes sollte auch geprüft werden, ob die bereits existierenden oder geplanten Sicherheitsmaßnahmen korrekt zum Einsatz kommen. Falsch oder unvollständig eingesetzte Sicherheitsmaßnahmen stellen eine zusätzliche potenzielle Schwachstelle eines Systems dar.

Risikobewertung

Nach dem Durchdenken der bisher beschriebenen Schritte ergibt sich automatisch, dass Risiken eigentlich eine Funktion folgender Parameter darstellen:

- ▷ Eintrittswahrscheinlichkeit einer Bedrohung,
- ▷ bereits existierende oder geplante Sicherheitsmaßnahmen, die dieses Risiko reduzieren könnten.

Wie diese Größen miteinander verknüpft werden, um die Höhe der Einzelrisiken und des Gesamtrisikos zu bestimmen, ist abhängig von der gewählten Risikoanalysemethode (quantitativ und/oder qualitativ). Ziel der Risikobewertung ist es, die Risiken, denen die bedrohten Objekte ausgesetzt sind, zu erkennen und zu bewerten, um auf dieser Basis geeignete und angemessene Sicherheitsmaßnahmen auswählen zu können. Der adäquaten Aufbereitung, Auswertung und Interpretation der Ergebnisse einer Risikoanalyse kommen wachsende Bedeutung zu. Da die Risikoanalyse auch als Grundlage für weitreichende weiterführende Entscheidungen dient, ist auf eine klare Darstellung der Situation sowie eine umfassende Ergebnisdarstellung zu achten. □

Ergebnisse der Analyseschritte / Analysephasen (siehe Abbildung):

Ergebnis der Wertanalyse:

Aufstellung der bedrohten Objekte und ihres Wertes für die Organisation.

Ergebnis der Bedrohungsanalyse:

Liste von Bedrohungen, der von ihnen bedrohten Objekte, und ihrer Eintrittswahrscheinlichkeiten.

Ergebnis der Schwachstellenanalyse:

Liste von potenziellen Schwachstellen mit Angaben darüber, wie leicht diese für einen Angriff ausgenutzt werden können.

Ergebnis der Identifikation der bestehenden Sicherheitsmaßnahmen:

Aufstellung aller bereits existierenden oder geplanten Sicherheitsmaßnahmen mit Angaben über ihren Implementierungsstatus und ihren Einsatz.

Ergebnis der Risikobewertung:

Quantitative oder qualitative Bewertung von Einzelrisiken und Gesamtrisiko für den betrachteten Analysebereich.

*Ergebnisse der detaillierten **Risikoanalyse***

- ▷ Wert der bedrohten Objekte (Schadensausmaß),
- ▷ Möglichkeit, eine Schwachstelle durch eine Bedrohung auszunutzen,