Governance, Risk und Compliance

Risikoanalysen für kritische IT-Infrastrukturen

Risikoanalysen sind das Fundament für den systematischen Aufbau und die Verbesserung der Informationssicherheit in jeder Institution. Nur die Kenntnis der Risikolage ermöglicht es, gezielte und wirkungsvolle Maßnahmen zur Risikominimierung zu ergreifen.

Illustration: © Kmlmtz66/shutterstock.com

Die Angemessenheit von Maßnahmen ist nur zu bewerten, wenn die Risikolage bekannt ist und Übereinkunft darüber besteht, welche Risikohöhe noch akzeptabel ist. Daher stellen alle gängigen Standards und Normen zu Informationssicherheitsmanagementsystemen (ISMS) die Risikoanalyse und das Risikomanagement in den Vordergrund und verlangen hierfür einen schriftlich niedergelegten Prozess.

Eine Gefährdung für einen konkreten Unternehmenswert – auch Asset, Zielobjekt oder Ressource genannt – besteht, wenn eine Schwachstelle auf eine Bedrohung trifft. Eine Risikoanalyse versucht, die Eintrittswahrscheinlichkeit einer Gefährdung für einen Unternehmenswert zu ermitteln und diese mit der erwarteten Schadenshöhe bei Eintritt der Gefährdung zu assoziieren. Hierfür existieren verschiedene Ansätze.

ISO 27005:2011. So beschreibt der Standard ISO 27005:2011 eine Reihe von Schritten für eine Risikoanalyse. Gemäß dem Standard ist zunächst eine Definition der Rahmenbedingungen für die Risikoanalyse erforderlich. Anschließend sind die Risiken zu identifizieren, wozu der Anhang des Standards zahlreiche Beispiele für Schwachstellen und Bedrohungen einzelner Arten von Unternehmenswerten liefert (IT-Systeme, Gebäude, Personal usw.). Sind diese identifiziert, erfolgt eine Abschätzung der Eintrittswahrscheinlichkeit und eine Priorisierung der Risiken vor dem Hintergrund der Schadenshöhe. Für entsprechend wahrscheinliche und hoch priorisierte Risiken wird dann die Risikobehandlung festgelegt, die (alternativ) in Risikominimierung, Risikovermeidung, Risikoübertragung oder Risikoakzeptanz bestehen kann. Seitens des Risikoeigentümers, also zumeist der Leitungsebene der Institution, ist über die temporäre oder dauerhafte Akzeptanz von Risiken zu entscheiden: Nicht alle beschlossenen Maßnahmen zur Risikominimierung, -vermeidung oder -übertragung sind sofort umsetzbar oder finanzierbar. Diese Entscheidungen werden in einem sogenannten Risikobehandlungsplan dokumentiert. Der Standard sieht außerdem vor, den Interessensträgern die bestehenden Risiken zu kommunizieren und für die identifizierten Risiken und die Wirksamkeit der Maßnahmen eine kontinuierliche Überwachung zu etablieren.

IT-Grundschutz. Auch der klassische IT-Grundschutz sieht – ebenso wie das Standardvorgehen im modernisierten IT-Grundschutz – eine Risikoanalyse vor. Da aber der IT-Grundschutz eine pauschalisierte Sicht auf Gefährdungen verfolgt, ist bei normalem Schutzbedarf (also nicht deutlichen oder gar ruinösen Schadenshöhen) die Risikoanalyse durch den Schritt der Modellierung von Zielobjekten mit Bausteinen der IT-Grundschutzkataloge (oder des IT-Grundschutzkompendiums) abgeschlossen. Die Bausteine enthalten jeweils pauschalisierte Gefährdungen, die Zielobjekt-immanent sind und immer eintreten können. Hier findet keine getrennte Betrachtung von Schwachstellen und Bedrohungen statt. Reichen die Bausteine nicht aus, weil der Schutzbedarf oberhalb von »normal« liegt, kein passender Baustein besteht oder ein Zielobjekt in einer ungewöhnlichen Umgebung eingesetzt wird, so verlangt auch der IT-Grundschutz eine ergänzende Risikoanalyse. Dies geschieht in einem zweistufigen Verfahren. Schritt 1 besteht in der Erstellung einer Übersicht der Sicherheitslage und einer anschließenden Management-Entscheidung zum weiteren Vorgehen. Bei Schritt 2 handelt es sich dann um die eigentliche Risikoanalyse, die entweder auf der Basis von IT-Grundschutz und damit gemäß des BSI Standards 200-3 erfolgen kann oder eine andere Methodik heranzieht. Welche Methodik dies ist, entscheidet eine Institution beim Aufbau des Informationssicherheitsmanagementsystems durch Verabschiedung einer entsprechenden Richtlinie. Für die Dokumentation dieser Schritte sind in der IT-Grundschutzmethodik entsprechende Referenzdokumente vorgesehen, welche auch bei einer Zertifizierung vorzulegen sind.

Fallstricke in den Risikoanalysen. Unabhängig vom gewählten Vorgehen sind Risikoanalysen in der Praxis mit einigen Fallstricken gespickt. Ein häufiges Problem liegt schon darin, die richtigen Skalen für eine Bewertung der Relevanz von Risiken zu finden. Eine Bewertung wird meistens halbquantitativ anhand von Eintrittswahrscheinlichkeiten und Schadenshöhen vorgenommen. Oft erfolgt hier eine Zuordnung numerischer Werte zu den verbalen Bewertungen – aus »niemals« wird »0«, aus »selten« wird »1« usw. Ähnliche Abbildungen werden auch für die Schadenshöhe verwendet. Dadurch lässt sich ein Risikowert gemäß der nachfolgenden Formel bilden:

Risiko = Eintrittswahrscheinlichkeit der Gefährdung x Schadenshöhe bei Eintritt

Allerdings kann dies die tatsächliche Risikolage verzerren. Wird beispielsweise eine Schadenshöhe von 1.000 Euro als »normal« (1) bewertet, 1 Million Euro aber als »hoch« (2), so sind durch die Zuordnung der Werte in der Formel plötzlich 1 Million Euro nur noch doppelt so viel wert wie 1.000 Euro. Hier ist also Vorsicht geboten und die Wahl sinnvoller Wertabstufungen notwendig.

Ein weiteres Problem besteht in einem zu großen Umfang der resultierenden Gefährdungen. Die Anzahl der Gefährdungen ergibt sich bei Anwen-

» **Auch der klassische IT-Grundschutz sieht –** ebenso wie das Standardvorgehen im modernisierten IT-Grundschutz – eine Risikoanalyse vor. «

dung der ISO-27005-Methodik im ungünstigsten Fall (also dem Vorliegen von Schwachstellen für jede betrachtete Bedrohung) aus der Anzahl der Schwachstellen multipliziert mit der Anzahl von Bedrohungen. Haben sich in der Auseinandersetzung mit den Verantwortlichen beispielsweise für ein Zielobjekt nur 5 Arten von Schwachstellen und 10 Arten von Bedrohungen als realistisch erwiesen, so können sich bereits 50 Gefährdungsszenarien ergeben. Sind 10 Zielobjekte zu betrachten, wären im Extremfall sogar 500 Gefährdungsszenarien hinsichtlich der Eintrittswahrscheinlichkeiten in Betracht zu ziehen. Dieses Vorgehen erfordert ein gutes Management der Risikoanalysen, soll das Verfahren nicht unvertretbar viel Zeit verschlingen. Dabei sind die hier gemachten Annahmen sehr tief angesetzt – typische Fachverfahren umfassen gerne 30 Zielobjekte und ein sinnvoll abgegrenzter Geltungsbereich eines ISMS kann leicht 20-30 Verfahren und 10 Standardservices beinhalten. Es ist unnötig zu betonen, dass detaillierte Risikoanalysen mit realistischem Aufwand manuell und ohne Software-Unterstützung hier nicht mehr zu leisten sind.

Lösungsansätze. Einen Ausweg aus dem Dilemma bieten eine konsequente Reduzierung der betrachteten Bedrohungen und Schwachstellen sowie eine sinnvolle Gruppierung von Zielobjekten bei der Risikoanalyse. Für diese Gruppierung liefert der IT-Grundschutz nutzbare Regeln (vgl. BSI Standard 100-2 beziehungsweise 200-2). Für eine übersichtliche Zahl an Bedrohungs- und Schwachstellenszenarien liefert hingegen das BSI an ganz anderer Stelle einen praxisgerechten Ansatz, der aus dem Umfeld des IT-Sicherheitsgesetzes (BSIG) stammt. Das BSIG sieht für betroffene Institutionen eine Verpflichtung der Umsetzung von IT-Sicherheitsmaßnahmen auf dem Stand der Technik und eines ISMS auf Basis eines eingeführten Standards vor. Dies ist nicht mit einer Umsetzung von IT-Grundschutz oder ISO 27001:2013 gleichzusetzen. Vielmehr wird einzelnen KRITIS-Sektoren erlaubt, einen branchenspezifischen Sicherheitsstandard (B3S) zu formulieren. In diesem Fall prüft das BSI den vorgelegten B3S und gibt diesen frei, sofern der B3S den gestellten Anforderungen genügt. Die Umsetzung des B3S ist dann ausreichend, um die Gesetzesvorgabe zu erfüllen. Die Formulierung eines B3S wird durch Branchenarbeitskreise vorgenommen. Zur Unterstützung dieser hat das BSI eine Orientierungshilfe herausgegeben, die alle Anforderungen an einen B3S festschreibt (»Orientierungshilfe zu Inhalten und Anforde-

Schwachstellen- und Bedrohungskategorien gemäß Orientierungshilfe des BSI zu B3S

Schwachstellenkategorien		Bedrohungskategorien	
A.2.1	Organisatorische Mängel	A 1.1	Hacking und Manipulation
A.2.2	Technische Schwachstellen	A 1.2	Terroristische Akte
A.2.3	Technisches Versagen	A 1.3	Naturgefahren
A.2.4	Menschliche Fehlhandlungen	A 1.4	Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)
A.2.5	Infrastrukturmängel	A 1.5	Missbrauch (Innentäter)
A.2.6	Netzseitige Mängel	A 1.6	Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)
A.2.7	Verkopplung von Diensten	A 1.7	Unbefugter Zugriff
		A 1.8	Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen
		A 1.9	Schadprogramme
		A 1.10	Social Engineering
		A 1.11	Gezielte Störung / Verhinderung von Diensten (DDoS, gezielte Systemabstürze, ...)
		A 1.12	Advanced Persistent Threat (APT)
		A 1.13	Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systemen

rungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG«, unter www.bsi.bund.de zum freien Download erhältlich). Hierbei ist der Anhang besonders interessant, denn er formuliert für Gefahrenanalysen 13 übersichtliche Bedrohungskategorien und 7 Schwachstellenkategorien (siehe Tabelle). Mit der Verwendung dieser Kategorien bei Risikoanalysen hat Controlware auch außerhalb kritischer Infrastrukturen gute Erfahrungen gemacht.

Wie kann die Anwendung dieser Kategorien bei Risikoanalysen in der Praxis erfolgen? Controlware beginnt in der Regel mit der Definition und sinnvollen Abgrenzung des Betrachtungsgegenstandes. Oft sind hier funktionelle Eingrenzungen naheliegend, also die Bezugnahme auf ein bestimmtes Fachverfahren (etwa Lohnbuchhaltung) oder auf einen Service (etwa E-Mail). Wichtig ist jedoch, dass eine derartige Abgrenzung auch physikalisch nachvollzogen wurde. Ansonsten besteht die Gefahr, potenzielle Risiken zu übersehen und Maßnahmen von geringer Wirkung zu formulieren. Schließlich kümmern sich Schadsoftware und Hacker nicht um Linien in Netzplänen, sondern lassen sich nur durch technische Maßnahmen wie Sicherheitsgateways aufhalten. Ist die Abgrenzung erfolgt, sind 5 Schritte erforderlich, die hier nur grob umrissen werden können:

Schritt 1: Identifizieren der Zielobjekte

Zunächst erfolgt die Identifizierung aller Anwendungen, IT-Systeme, Netzkomponenten sowie Räume, Gebäude, Personal und Kommunikationsverbindungen. Gleichartige Objekte werden dabei in Gruppen zusammengefasst. Ihre Bezeichnungen und die Kerneigenschaften werden tabellarisch dargestellt und eindeutig nummeriert. Dieser Schritt entspricht dem der sogenannten IT-Strukturanalyse des IT-Grundschutzes (BSI Standard 100-2).

Schritt 2: Schwachstellenanalyse

Bei der Schwachstellenanalyse wird nun eine Zuordnung der Schwachstellen gemäß Anhang der B3S-Orientierungshilfe zu den Zielobjekten vorgenommen. Dabei spielt die Frage noch keine Rolle, ob tatsächlich eine Bedrohung vorliegt. Für jede Schwachstelle erfolgt außerdem eine Bewertung der Wahrscheinlichkeit des Vorliegens der Schwachstelle in einem einfachen Schema, etwa »theoretisch«, »möglich« und »bekannt«.

Schritt 3: Bedrohungsanalyse

Auch bei der Bedrohungsanalyse wird mit der Zuordnung der Bedrohungen gemäß Anhang der B3S-Orientierungshilfe ähnlich verfahren. Analog zu Schritt 2 wird ebenfalls nicht gefragt, ob bei den Zielobjekten eine Schwachstelle vorliegt. Auch hier erfolgt eine Bewertung der Eintrittswahrscheinlichkeit.

Schritt 4: Formulieren von Gefährdungen

Für jedes Zielobjekt wird nun eine Gefährdung formuliert, wenn einer Bedrohung tatsächlich eine Schwachstelle gegenübersteht. Eine Gefährdung könnte etwa lauten: »Hacking und Manipulation infolge organisatorischer Schwachstellen bei Server S1«. Die Wahrscheinlichkeit des Eintretens der Gefährdung ergibt sich aus den bereits bestimmten Einzelwahrscheinlichkeiten von Bedrohung und Schwachstelle. Eine Konsolidierung der zu betrachtenden Gefährdungen ist dabei sinnvoll. Hierzu hat es sich bewährt, gleiche Gefährdungen unterschiedlicher Zielobjekte zusammenzufassen und nur einmal zu betrachten, wenn diese auf mehrere Zielobjekte des Betrachtungsgegenstandes wirken.

Schritt 5: Risikoanalyse

Die Risikoanalyse besteht aus der Verknüpfung von Eintrittswahrscheinlichkeiten der Gefährdungen und der Schadenshöhe der einzelnen Zielobjekte. Die Kenntnis der Schadenshöhe setzt entweder eine Schutzbedarfsanalyse gemäß IT-Grundschutz voraus oder eine geschäftsprozessbezogene Betrachtung.

Es ist wichtig hervorzuheben, dass der Anhang der B3S-Orientierungshilfe jeweils nur Kategorien für Schwachstellen und Bedrohungen liefert. Bei der Formulierung von Gefährdungen ist es sinnvoll, diese für den Einzelfall zu konkretisieren. Möglich ist dies durch Bezug auf Gefährdungen der IT-Grundschutzkataloge oder des IT-Grundschutzkompendiums, aber auch durch Heranziehen spezifischer Quellen zu »best practises« bestimmter Technologien, aktueller Sicherheitshinweise oder Informationen von Sicherheitsanalysten. Die Einordnung in die Kategorien schafft damit Übersichtlichkeit, reduziert das Mengenproblem und macht Analysen unterschiedlicher Betrachtungsgegenstände untereinander vergleichbar.

Abschließend lässt sich feststellen, dass Controlware mit diesem Vorgehen gute Projekterfahrungen gemacht hat. Zwar senkt die beschriebene Konsolidierung der Gefährdungsszenarien den Detaillierungsgrad der Analyse nur ein wenig, reduziert dafür aber den Aufwand deutlich. Dies ist ein wichtiger Aspekt, denn eine Gefährdungsanalyse nimmt Controlware stets im Dialog mit dem Kunden in Form von Workshops vor. Bei zu umfangreichen Gefährdungslisten sind die Teilnehmer rasch überfordert und es kommt zu Fehleinschätzungen der Risikolage. Hier erleichtert die vorgestellte Methode die Arbeit deutlich, was letztlich dem Sicherheitsniveau der Institution zugutekommt. *Georg Basse*

Georg Basse,
Senior Consultant IT-Security
Controlware GmbH

www.controlware.de