

Der Weg zur Risikolandkarte

Pragmatische Methodik zur Risikobewertung der Informationssicherheit

Zur Steuerung von Sicherheits-Maßnahmen und IT-Prozessen ist eine fundierte Risikobewertung essenziell. Dieser Beitrag stellt ein praxistaugliches Verfahren vor, das sich an nationale wie internationale Normen anlehnt, aber dennoch eine gewisse „Leichtigkeit“ und damit Effizienz behält.

Von Bernd Ewert, Hamburg

In Zeiten knappen Geldes und nach der meist wenig erfolgreichen Suche nach „Return on Security Investment“ (ROSI) bleibt es dem Verantwortlichen für die Informationssicherheit eines Unternehmens weiterhin oft selbst überlassen, seine Existenzberechtigung nachzuweisen. Dies kann heute im Rahmen eines unternehmensweiten Risikomanagements stattfinden, das auf der Leitungsebene durch Ereignisse wie spektakuläre Datendiebstähle sowie durch gesetzliche Vorgaben inzwischen eine verstärkte Aufmerksamkeit genießt.

Auch einschlägige Normen, sowohl international (ISO/IEC 2700x) als auch national (BSI-Grundschutz), sehen eine Betrachtung der Risiken vor, die sich aus der Gefährdung von Informationen im Unternehmen ergeben können. Es werden auch Beschreibungen mitgeliefert, wie dies erfolgen kann – dabei ist beachtlich, dass die Normen (trotz der Tugend der reinen Lehre) die eine oder andere Vereinfachung in der Betrachtung zulassen. Dieser Artikel beschreibt ein in der Praxis erprobtes Verfahren zur Risikobewertung, das die Anregungen der Normen aufgreift und dabei versucht, allzu große Komplexität zu vermeiden. Es soll nur gerade so umfangreich sein, dass eine fundierte Ableitung und Begründung von Maßnahmen

zur Informationssicherheit möglich wird.

Aufgabenstellung

Vordringliche Aufgabe der Risikobewertung ist es, aus der Vielfalt der vorhandenen Informationen diejenigen herauszufiltern, die schützenswert sind. Diese Aufgabe kann niemals ein einzelner Mitarbeiter alleine erledigen! Es bedarf dazu der Einschätzung all derjenigen, die mit den Informationen täglich umgehen. Eine entsprechende Befragung bietet die Chance, die Mitarbeiter bei ihren eigenen Themen „abzuholen“, sodass für eventuell anstehende Maßnahmen nicht nur das notwendige Verständnis, sondern auch aktive Unterstützung entsteht.

Andererseits sollte die Inanspruchnahme für die Belange der Informationssicherheit so gering wie möglich gehalten werden: Mehr als einen Arbeitstag sollte sich niemand, der nicht direkt mit der Informationssicherheit oder der IKT befasst ist, mit der Risikobewertung beschäftigen müssen. Ein solcher Tag sollte aber für ausgewählte Personen akzeptabel sein – schließlich geht es um eine wichtige Grundlage des Unternehmenserfolgs.

Angesichts der Vielfalt der Informationen bedarf es einer durch-

gängig anwendbaren, für die Beteiligten durchschaubaren Methode zur Risikobewertung. Sie muss gewährleisten, dass beide Seiten von Risiken, sowohl das Schadenspotenzial als auch die Wahrscheinlichkeit des Schadenseintritts, in angemessener Weise erhoben und miteinander in Beziehung gesetzt werden. Ein derart ermitteltes Risiko muss dann anhand einer unternehmensspezifischen Skala dahin gehend bewertet werden, ob es tragbar ist oder nicht – wenn nicht, sind Maßnahmen zu benennen, die das Risiko mindern.

Begrifflichkeiten

Es ist sinnvoll, zwei verschiedene Aspekte von Informationen zu unterscheiden:

_____ Der *Inhalt* einer Information ist die Aussage, die sie enthält: Er ist vollständig immateriell, macht aber ihre Bedeutung aus.

_____ Der *Träger* einer Information ist das Material, an dem der Inhalt „anhftet“: Dabei kann es sich um IKT-Equipment, Papier oder andere „Datenträger“ handeln – möglich sind auch, beispielsweise in Datenetzen, relativ abstrakte Gebilde oder Menschen (Fachwissen, Erfahrung usw.). Zusammen mit dem Träger ist immer auch der Raum zu betrachten, in dem er sich befindet.

Mit dieser Betrachtungsweise lässt sich das Risiko, das mit einer Information verbunden ist, besser einordnen: Der *unmittelbare Schaden* aus einer Verletzung der Informationssicherheit ist ein materieller Verlust, der sich auf den Informations-Träger bezieht. Das ist nur dann wirklich schlimm, wenn Menschen dabei zu Schaden kommen. Das meist bedeutendere *Schadenspotenzial* resultiert aus Fol-

geerscheinungen des eigentlichen Schadensereignisses und wird durch den Informations-Inhalt bestimmt.

Andererseits hängt die *Eintrittswahrscheinlichkeit* von Schäden hauptsächlich vom betroffenen Träger ab: Nur bei bewussten, deliktischen Handlungen beeinflusst der Inhalt von Informationen die Wahrscheinlichkeit eines Schadensereignisses (je höher der Wert, desto größer die Bemühungen).

Unter Beachtung dieser Trennung ist es möglich, die Ermittlung des Schadenspotenzials und der Eintrittswahrscheinlichkeit weitgehend zu entkoppeln.

Inhalte und Schadenspotenzial

Schadenspotenzial bezieht sich immer auf Informationsinhalte, deshalb müssen im ersten Schritt die vorhandenen Informationsinhalte erfasst werden. Dies klingt nach extrem hohem Aufwand, der sich aber erheblich reduzieren lässt, wenn man dabei sinnvoll gruppiert. Außerdem besteht die Aufgabe ja nicht darin, alle – auch unwichtigen – Informationen vollständig aufzunehmen. Daher muss bei der Erfassung von vornherein auch das Schadenspotenzial mit betrachtet werden.

Für die Erhebung eignen sich Interviews auf der Ebene von Bereichsleitern, die nicht länger als 1–2 Stunden dauern müssen. Da die Interviewten von der Betrachtung der Träger (z. B. IKT) vollständig abstrahieren dürfen, können sie allein aus der Sicht ihres Fachgebiets auf die benötigten Informationen schauen. So lassen sich die wichtigen Informationsinhalte meist leicht benennen. Beispiele sind: Kostenstellenrechnung, Personalentwicklung, Lieferantenverträge, Ausgangsrechnungen, Produktentwicklung, Werbung oder Anweisungswesen.

Die Betrachtungstiefe sollte variieren, wenn innerhalb von Informationskomplexen starke Unterschiede beim Schadenspotenzial bestehen. Erfahrungsgemäß kommen so durchschnittlich etwa zehn unterschiedliche Informationsinhalte pro Bereich zusammen.

Für jeden der Informationswerte sollte man im Interview auch das Schadenspotenzial in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit erheben. Dabei bleibt es allerdings eine Wunschvorstellung, das Schadenspotenzial immer quantitativ ausdrücken zu können: Zwar gibt es durchaus einzelne Schäden, für die das möglich ist – generell aber kann nur mit einer Skala *qualitativer Werte* gearbeitet werden, in die man dann auch die quantitativen Bewertungen normieren muss. Wie, ist vor Beginn der Interviews abzustimmen.

Es empfiehlt sich, mit einer einheitlichen Skala für alle drei Sicherheitskriterien zu arbeiten, die sich möglichst eng an das unternehmensweite Risikomanagement anlehnen sollte. Dabei ist eine gerade Anzahl von Werten (4 oder 6) sinnvoll, damit nicht bequemerweise einfach die Mitte gewählt werden kann. Die Werte sollten zudem selbsterklärend sein – beispielsweise „unbedeutend“, „spürbar“, „erheblich“ und „existenzbedrohend“.

Zusammen mit der Einstufung in die Skala sind jeweils mögliche *Schadenskategorien* zu erfassen; auch diese können gegebenenfalls aus dem allgemeinen Risikomanagement entnommen werden. Falls nicht, sind sie zu erstellen. Typischerweise kommen dabei vor:

- _____ physische oder psychische Schädigung von Menschen,
- _____ direkte finanzielle Auswirkung,
- _____ Verstoß gegen Gesetze oder Vorschriften,
- _____ Beeinträchtigung des Geschäftsablaufs,
- _____ negative Außenwirkung,
- _____ Abfluss von Know-how.

Eine Verletzung der Informationssicherheit kann jeweils eine oder mehrere Kategorien von Schäden nach sich ziehen. Es kann dabei hilfreich sein, neben dem Schaden für das eigene Unternehmen auch den Nutzen für einen eventuellen Angreifer zu bedenken, also einmal eine entgegengesetzte Sichtweise einzunehmen. Das Schadenspotenzial ist entsprechend einzustufen.

Da viele Informationsinhalte im Fokus mehrerer Bereiche stehen, werden sie üblicherweise auch mehrfach erfasst. Es bedarf daher am Ende dieser ersten Phase einer Konsolidierung, welche die Anzahl der zu betrachtenden Informati-

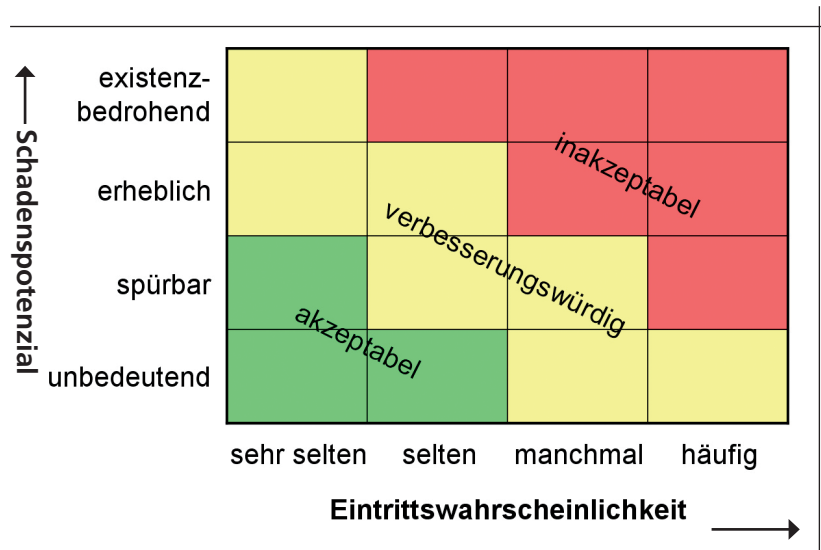


Abbildung 1: Ampelmatrix zur Risikobewertung (Risikolandkarte)

onsinhalte durch eine Zusammenfassung ähnlicher Charakteristiken deutlich verringert. Gibt es aus der Sicht verschiedener Bereiche dabei unterschiedliche Schadenseinschätzungen für ähnliche Inhalte, dann sollten die Ergebnisse gewichtet und zusammengefasst werden. Erfahrungen zeigen, dass eine Liste mit etwa 100 Einträgen auch bei größeren Unternehmen ausreichend ist. Abschließend sollte die Geschäftsleitung das Ergebnis abnehmen.

Das Schadenspotenzial bestimmt direkt den *Schutzbedarf*: Droht hoher Schaden, ist auch der Schutzbedarf hoch. Damit ist eine Vorauswahl für die weitere Betrachtung der identifizierten Risiken möglich. Informationsinhalte, die in allen Sicherheitskategorien niedrige Werte aufweisen, kann man getrost in der Priorität an das Ende der Betrachtung stellen.

Informationsträger und Abhängigkeiten

Die Wahrscheinlichkeit für den Eintritt eines Schadens bezieht sich in erster Linie auf die Informationsträger und ihre Standorte: Sie sind es, die möglichen Bedrohungen unterliegen, weshalb sie auch im Zusammenhang betrachtet werden müssen.

Es bedarf grundsätzlich eines umfangreichen Wissens und einer großen Fantasie, um sämtliche mögliche *Bedrohungen* zu erkennen. Eine Hilfestellung bieten vorgefertigte Listen wie in der ISO/IEC 27005, die eine brauchbare Arbeitsgrundlage bilden. Für besonders kritische Bereiche der IKT kann man zusätzlich die sehr umfangreichen Gefährdungskataloge im BSI-Grundschutz heranziehen. Auf jeden Fall ist es erforderlich, sich eine Sammlung zu betrachtender Bedrohungen anzulegen, die insbesondere auch spezifische Bedrohungen für das zu untersuchende Unternehmen enthält.

Als nächstes ist eine Aufstellung der *Informationsträger* und ihrer Aufbewahrungsorte zu erarbeiten, auf welche die Bedrohungen wirken können. Dazu sind drei Vorgehensweisen zu empfehlen:

Die IKT-Umgebung des Unternehmens sollte in geeignete Segmente aufgeteilt werden, die jeweils als Einheit behandelbar sind. Dies kann nach technischen Kriterien geschehen (z. B. verschiedene Netze, Server, Storage, zentrale und verteilte I/O-Geräte, Desktops, Telefone, mobile Endgeräte) oder nach funktionalen Gesichtspunkten (z. B. Internet-Auftritt, Mail-Infrastruktur,

File-Services). Wichtig ist, dass die Modellierung danach erfolgt, dass Bedrohungen für ein Segment sinnvoll diskutierbar sind und man dabei möglichst wenig Redundanz erzeugt.

Andere Arten von Informationsträgern sind zu typisieren, sodass auch sie gemeinsam betrachtet werden können: Übliche Typen sind unter anderem Papierdokumente, das gesprochene Wort, Mitarbeiter und Dienstleister.

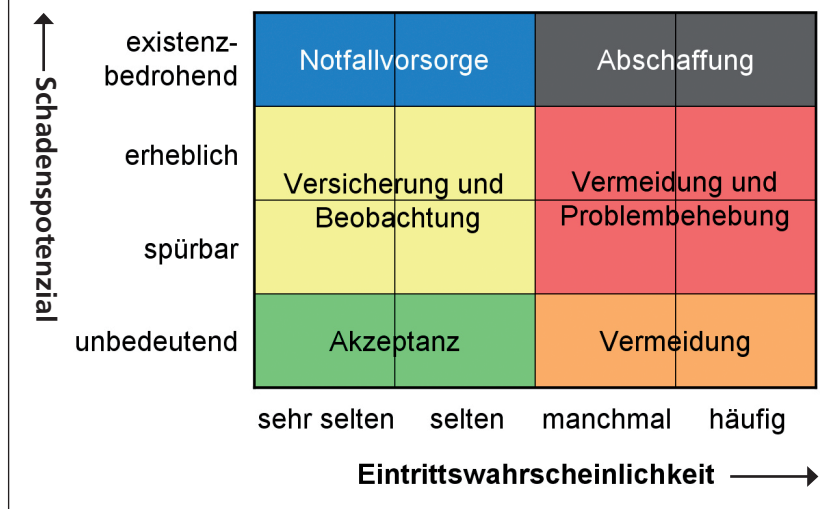
Die Orte, an denen sich Informationsträger befinden können, sind zu benennen: Hierzu gehören Rechenzentren, Tresore, Archive und Büroräume, aber auch Transportwege. Der Einfachheit halber kann man diese Orte mit zu den Informationsträgern zählen.

Die Zusammenstellung sollte unter Beteiligung der für IKT, Archive und Haustechnik Zuständigen erfolgen. Darüber hinaus ist zu ermitteln, welche Inhalte mit welchen Trägern verbunden sind: Da auch Standorte berücksichtigt werden, geht es jedoch nicht nur um die reine Trägereigenschaft – besser ist es, hier von *Abhängigkeiten* zu sprechen. Dabei sind auch Wege von Informationsinhalten über mehrere Träger hinweg zu verfolgen; gerade Übergänge und Schnittstellen bilden oft besonders gefährdete Bereiche.

Die Abhängigkeiten lassen sich am besten unter Mithilfe von Mitarbeitern zusammenstellen, die für die Schnittstelle zwischen der IKT und den Anwendern verantwortlich sind. Sie haben oft auch ein profundes Wissen über Prozesse, die über die IKT hinaus gehen, wie zum Beispiel Formularwesen und Archivierung. So lässt sich recht schnell ein Bild der vorliegenden Abhängigkeiten aufbauen.

Die geeignete Modellierung der IKT-Umgebung ist wohl die größte Herausforderung in einer Risikobewertung: Sie sollte nicht zu

Abbildung 2: Schutzstrategie zum Umgang mit identifizierten Risikoklassen



grob erfolgen, um keine relevanten Bedrohungen zu übersehen, aber auch nicht zu fein, um den Aufwand zu begrenzen. Auch hier sollte eine Liste mit nicht mehr als etwa 100 Einträgen das Ziel sein, selbst bei großer Komplexität der IKT-Umgebung.

Eintrittswahrscheinlichkeiten und Risiken

Für die dritte Phase ist wesentlich, dass die Wahrscheinlichkeit für den Eintritt eines Schadens von der Bedrohungslage sowie den vorhandenen Schwachstellen und Schutzmaßnahmen, also den Informationsträgern, abhängt. Jeder der Informationsträger (und Orte) auf der erstellten Liste wird daher im Hinblick auf die für ihn relevanten Bedrohungen untersucht; dafür werden erneut die Träger-Verantwortlichen herangezogen.

Für jeden Informationsträger wird dabei pro Bedrohung die Wahrscheinlichkeit ermittelt, mit der diese Bedrohung angesichts der vorhandenen *Schwachstellen*, aber auch im Lichte schon getroffener *Schutzmaßnahmen* auf den Informationsträger wirken wird. Mangels vorliegender Statistiken sind meist Annahmen erforderlich: Daher ist auch hier eine qualitative Skala mit vier bis sechs Stufen vollkommen ausreichend – z. B.: „sehr selten“, „selten“, „manchmal“, „häufig“. Diese Begriffe sollten zum Verständnis mit Erläuterungen wie „seltener als alle x und häufiger als alle y Wochen“ versehen werden. Jede Einstufung ist zusammen mit ihrer Begründung zu dokumentieren.

Danach kann man die bisherigen Betrachtungen zusammenführen: Für jedes Paar aus Inhalt und Träger müssen die Untersuchungsergebnisse über das Schadenspotenzial und die Eintrittswahrscheinlichkeit kombiniert werden. Dabei sind noch Anpassungen möglich, falls die Trennung von Inhalt und Träger zu einem unrealistischen Bild führt:

_____ Befindet sich ein Inhalt auf einem besonders wertvollen Träger, kann bei Bedarf das Schadenspotenzial erhöht werden.

_____ Wird ein Inhalt als bevorzugtes Angriffsziel, der Nutzen für einen Angreifer also als besonders hoch angesehen, dann kann an dieser Stelle die Eintrittswahrscheinlichkeit für menschliche Bedrohungen erhöht werden.

_____ Schadenspotenzial und Eintrittswahrscheinlichkeit müssen zueinander passen: Beispielsweise kann man bei einer Bedrohung, die sich auf einzelne Datensätze bezieht, nicht von einem Schaden für eine ganze Datenbank ausgehen. Hier sind eventuell Entscheidungen für bestimmte Szenarien und in der Folge Anpassungen zur einen oder anderen Seite erforderlich.

Nun lässt sich das *Risiko* für das jeweils betrachtete Paar aus Inhalt und Träger im Hinblick auf die untersuchten Bedrohungen errechnen. Spätestens hier ist ein technisches Hilfsmittel geboten, da mehrdimensionale Ergebnisse entstehen. Die erzielten Ergebnisse lassen sich anschließend weiter auswerten:

_____ Alle Paare zu einem bestimmten Inhalt lassen sich zu einer Gesamtansicht auf das Risiko zusammenstellen, das mit diesem Informationsinhalt verbunden ist. Diese Ansicht sollte dem Verantwortlichen für den Inhalt vermittelt werden, um das Risikobewusstsein im jeweiligen Geschäftsbereich zu schärfen.

_____ Alle Paare zu einem bestimmten Träger ergeben das Gesamtrisiko für diesen Informationsträger: So ist eine differenziertere Ansicht als etwa bei Nutzung von Vererbung des Schutzbedarfs nach dem Maximumsprinzip möglich. Die Verantwortlichen für den Träger können damit feststellen, an welchen Stellen Risiken besonders hoch und welche Inhalte die Treiber dafür sind.

Bewertung und Maßnahmen

Auf diese Weise ist bereits eine Transparenz entstanden, die alle weiteren Tätigkeiten zur Informationssicherheit unterstützt. Zwar ist nun bekannt, welche Risiken für die Informationen bestehen, doch es ist noch nicht klar, wie das Unternehmen darauf reagieren soll. Um dies zu bestimmen, müssen Maßstäbe für den Umgang mit Risiken vom unternehmensweiten Risikomanagement übernommen oder – in Abstimmung damit – neu geschaffen werden. Entsprechende Festlegungen lassen sich zum Beispiel in einer Matrix mit den Dimensionen Eintrittswahrscheinlichkeit und Schadenspotenzial darstellen, in der man für jede Kombination aus den genutzten Klassifizierungen definiert, wie ein solches Risiko zu bewerten ist; dafür wird oft ein Ampelsystem verwendet, wie es auch Abbildung 1 zeigt.

In eine solche Matrix werden nun jeweils für ein Paar aus Informationsinhalt und -träger die Schnittpunkte aus Eintrittswahrscheinlichkeit und Schadenspotenzial eingetragen, die sich pro Bedrohung ergeben. Das Resultat ist eine *Risikolandkarte*, mit der sich das Gesamtrisiko anschaulich darstellen lässt.

Die Lage eines Risikos in der Risikolandkarte kann auch zur Priorisierung dienen: Diejenigen Risiken, die im roten Bereich liegen, sind mit höchster Priorität anzugehen, diejenigen im gelben Bereich nachrangig. Will man hier weiter differenzieren, können natürlich auch mehr Farbbereiche zum Einsatz kommen.

Nach der Risikobewertung folgt die Konzeption des Umgangs mit den vorhandenen Risiken: Zunächst sollte man dazu eine allgemeine *Schutzstrategie* festlegen, welche die grobe Richtung von Maßnahmen für abgegrenzte Risikogruppen enthält. Hierfür ist unbedingt die Unterstützung des Managements notwendig!

Eine Schutzstrategie muss passend zu Eintrittswahrscheinlichkeit und Schadenspotenzial jeweils unterschiedliche Kategorien von Maßnahmen vorsehen (vgl. Abb. 2):

—— Bei eher hoher Eintrittswahrscheinlichkeit gilt es vor allem, den Eintritt eines Schadensereignisses zu vermeiden: Selbst geringe Schäden sind, wenn sie oft vorkommen, zumindest sehr lästig. Durch die (teilweise) Verhinderung des Schadens-

eintritts wandert das Risiko in der Tabelle „nach links“ – trotzdem wird meist eine Restwahrscheinlichkeit bleiben. Bei einem mittleren Schadenspotenzial sollte daher zusätzlich durch angemessene Vorbereitung auf das Ereignis (etabliertes Incident- und Problem-Management) auch das Schadens-Ausmaß verringert werden. Existenzbedrohende Schäden mit hoher Eintrittswahrscheinlichkeit sind generell nicht hinnehmbar – hier ist die gesamte Situation neu zu gestalten.

—— Eine eher niedrige Eintrittswahrscheinlichkeit lässt präventive Maßnahmen nur selten wirtschaftlich erscheinen. Deshalb geht es hier vor allem darum, die Situation zu beobachten, damit man auf eventuelle Lageänderungen angemessen reagieren kann. Für Schäden mittleren Ausmaßes sind oft Versicherungsprämien günstiger als eigene Maßnahmen, eine Abwälzung der Schäden also ein sinnvoller Weg. Für existenzbedrohende Schäden allerdings reicht das nicht: Zwar kön-

Tools zur Risikobewertung

Die Bedingungen, unter denen Unternehmen ihre Tätigkeit ausüben, wandeln sich permanent. Es reicht daher nicht, Risiken nur einmalig festzustellen und entsprechende Maßnahmen umzusetzen – vielmehr müssen Risiken immer wieder neu identifiziert und überprüft werden. Gerade eine stets wiederkehrende Risikobewertung sollte natürlich so effizient wie möglich erfolgen. Dabei muss es auch möglich sein, frühere Ergebnisse für Wiederholungen zu nutzen und die Entwicklung zu verfolgen.

Bei der Risikobewertung entstehen zahlreiche Dokumente, die sämtlich einander zugeordnet sind und aufbewahrt werden müssen. Schon zur Wahrung des Überblicks ist daher ein Hilfsmittel sinnvoll, das diese Aufgabenstellung unterstützt. Es sollte mindestens folgende Bestandteile umfassen:

—— Fragebögen: sollten aus dem Tool heraus auch mit Einbeziehung früherer Angaben generierbar sein, um den Befragten die Antworten zu erleichtern.

—— Datenbank für Assets: Das Tool sollte als Register fungieren,

das sowohl die Informationsinhalte als auch die Informationsträger enthält.

—— Integrierte Risikobewertung: Assets und die zu ihnen passenden Bedrohungen sollten gemeinsam zu verwalten sein.

Der Markt für solche Tools entwickelt sich derzeit noch. Dabei ergibt sich zum einen die Schwierigkeit, dass mehrere Standards existieren, die unterschiedliche Methoden vorsehen. Der Grundschatz des deutschen BSI wird durch das parallel entwickelte BSI-Grundschatz-Tool abgedeckt, eine formale Betrachtung der Eintrittswahrscheinlichkeit unterbleibt dabei jedoch. Zudem ist die internationale Norm zur Risikobewertung im Rahmen der Informationssicherheit (ISO/IEC 27005), die selbst mehrere Verfahren vorschlägt, erst Mitte 2008 erschienen – es ist zu erwarten, dass künftig noch weitere Software-Hersteller „in den Ring steigen“ werden. Doch auch ein anderer Aspekt sorgt noch für Irritationen: Wie bei allen Tools ist eine Integration in das Umfeld sinnvoll. Jedoch in welches?

Manche Hersteller setzen dabei auf die Integration in das Systemmanagement, womit grundsätzlich die Orientierung an der technischen

Umgebung erleichtert wird. Jedoch muss dann auch die Zuordnung der vielen Einzelkomponenten zu den für die Risikobewertung genutzten Segmenten der IKT darstellbar sein. Die Nutzung solcher Tools verführt zudem leicht dazu, sich auf die IKT zu konzentrieren – Informationssicherheit sollte jedoch nicht nur als IKT-Sicherheit wahrgenommen werden!

Andere Hersteller kommen von der Seite des unternehmensweiten Risikomanagements: Dort wird jedoch oft mit statistischen Verfahren gearbeitet, für welche die Informationssicherheit einen geeigneten Input schuldig bleibt. Selbst Vorfalldatenbanken bieten hier angesichts permanenter Veränderungen nur eine eingeschränkte Hilfe.

Ein Tool muss letztlich zur eigenen Methode und Organisation passen – eine persönliche umfassende Betrachtung der angebotenen Tools lohnt daher. Wer die Entwicklung noch abwarten, aber trotzdem schon Risikobewertungen vornehmen will, der kann auch „auf kleiner Basis“ erst einmal mit „hausgemachten“ Mitteln beginnen (kleine Datenbank, Tabellenkalkulation). Die dabei gemachten Erfahrungen sind später für die Auswahl des optimalen Tools durchaus hilfreich.

nen Teilaspekte versichert werden, die Zielrichtung muss hier aber eine effektive Notfallvorsorge sein. Solche Maßnahmen verschieben das Risiko in der Tabelle „nach unten“.

Auf der Basis der Schutzstrategie kann dann eine fokussierte Diskussion von *Maßnahmen* zu einzelnen Risiken erfolgen. Dabei wird es zu individuellen Entscheidungen kommen, die vor allem spezifisch auf den durch ein Risiko betroffenen Informationsträger ausgerichtet sind. Hat man die Maßnahmen festgelegt, sollte man jedes Risiko erneut bewerten: Dabei geht es um die Einschätzung der voraussichtlichen Veränderung durch die ergriffenen Maßnahmen, die sowohl die Eintrittswahrscheinlichkeit als auch das Schadenspotenzial verringern können. Dieses Ergebnis lässt sich später, nachdem die Maßnahmen wirksam geworden sind, auch zur Erfolgskontrolle heranziehen.

Fazit

Eine Risikobewertung wird zur Übersicht im Dickicht der Informationsgefährdungen immer wichtiger, um die richtigen „Schutzschneisen“ anlegen zu können. Auf diesem sich permanent wandelnden Terrain müssen alle Bewertungen möglichst aktuell sein, also regelmäßig und bei besonderen Anlässen überprüft und gegebenenfalls neu vorgenommen werden. Es bedarf dazu einer effektiven und effizienten Methode!

Der Vorteil der beschriebenen Herangehensweise liegt darin, dass die aufwändigen Einzelbetrachtungen zu Schadenspotenzial und Eintrittswahrscheinlichkeit getrennt und damit jeweils „nur“ etwa 100-mal durchzuführen sind. Die nachfolgende Zusammenführung, die theoretisch bis zu 100x100 Ergebnisse liefert, kann dagegen weitgehend automatisiert erfolgen und er-

fordert dann nur eine verhältnismäßig geringe manuelle Überarbeitung.

Entscheidend bei der Risikobewertung im Rahmen der Informationssicherheit bleibt es, die kritischen Punkte zu finden! Dies wird mit der beschriebenen Methode erreicht. Orientiert man sich dagegen an etablierten Verfahren zum unternehmensweiten Risikomanagement, stellt man in einigen Branchen fest, dass dort zwar sehr elaborierte Berechnungsverfahren existieren (z. B. bei Banken). Wie wir alle wissen, hat eine solche „Scheingenauigkeit“ jedoch nicht dabei geholfen, die wirklichen großen Risiken zu finden. Lassen Sie sich also nicht entmutigen oder ins Bockshorn jagen – es gilt weiterhin: Lieber einfach und ungefähr richtig als aufwändig und genau falsch! ■

Bernd Ewert ist Geschäftsführer der consequa GmbH.