

Praktisches Sicherheitsmanagement

Reiseziele

- Ziel 1.01 Verantwortlichkeiten des Managements
- Ziel 1.02 Risikomanagement
- Ziel 1.03 Bedrohungspotenzial
- Ziel 1.04 Arten von Kontrollmechanismen in der Sicherheit
- Ziel 1.05 Risikoberechnung
- Ziel 1.06 Sicherheitspolitik und unterstützende Dokumente
- Ziel 1.07 Rollen und Verantwortlichkeiten
- Ziel 1.08 Klassifikation der Informationen
- Ziel 1.09 Personalmanagement

Zeitplanung

Neuling	4 Stunden
Etwas Erfahrung	2 Stunden
Experte	1 Stunde

Es gibt mehrere Arten von Bedrohungen, welche die Sicherheit einer Organisation und die zu schützenden Informationswerte beeinflussen können. Das Management muss diese unterschiedlichen Bedrohungen verstehen und sicherstellen, dass angemessene Gegenmaßnahmen implementiert sind. Ein Unternehmen, das sich selbst und seine Informationswerte schützt, muss daher die richtigen Maßnahmen – ein praktisches Sicherheitsmanagement – implementieren. Dieses Kapitel definiert verschiedene Verfahren, gibt Beispiele und zeigt die möglichen Konsequenzen, die entstehen können, wenn solche Sicherheitsmechanismen fehlen.

Ziel 1.01

1.1 Verantwortlichkeiten des Managements

Das Management sollte die Bedeutung der Sicherheit innerhalb der Organisation vorgeben. Dazu gehören der Umfang (Scope), die Ziele (Objectives), die Prioritäten (Priorities) und die Sicherheitsstrategien (Security Strategies) im Rahmen des unternehmensweiten Sicherheitsmanagements (Security Program). Es gehört ebenfalls zur Managementverantwortung, Sicherheit einzuführen, zu unterstützen und die angemessene Wartung zu gewährleisten. Ohne die Unterstützung durch die obere Führung des Unternehmens (senior management) wird ein Sicherheitsmanagement normalerweise nicht die notwendige Aufmerksamkeit, Finanzierung und Ressourcen erhalten. Außerdem nehmen Mitarbeiter Sicherheitsempfehlungen gewöhnlich nicht allzu ernst, wenn nicht das leitende Management dahintersteht und die Empfehlungen durchsetzt. Die obere Führung des Unternehmens hat Einblick in die Geschäftsfelder, Visionen, Ziele und die strategische Richtung. Sie sollte dieses Wissen nutzen, um die Rolle der Sicherheit im Unternehmen festzulegen. Ohne die übergeordnete Führung fehlt normalerweise die allgemeine Richtung, in der sich Computer, Information, physische und personelle Sicherheit bewegen, und alle Bemühungen scheitern schon im Ansatz.

Ein *zentraler Ansatz (top-down approach)* liegt dann vor, wenn die obere Führung des Unternehmens die Sicherheitsziele initiiert und fördert. Der andere, weniger erfolgreiche Ansatz ist *von unten nach oben (bottom-up)*, wenn die IT-Abteilung versucht, ein Sicherheitsmanagement einzurichten, das in den meisten Fällen ohne die notwendige Unterstützung und das erforderliche Budget bleibt. Sicherheit braucht eine ganze Menge Führung, um zu einem Erfolg zu gelangen, da Dinge sich ändern müssen und die Einhaltung der Regeln durchgesetzt werden muss. Es ist nicht fair, von Netzwerkadministratoren zu erwarten, dass sie sich in so wichtigen Angelegenheiten diesen Hut aufsetzen sollen.

Die Unternehmensleitung ist zugleich der endgültige Dateneigentümer; das heißt, sie haben die letztendliche Verantwortung für alle Vermögensgegenstände des Unternehmens inklusive der Daten. Wenn das Management nicht die richtigen Sicherheitsmaßnahmen implementiert, entspricht das nicht der kaufmännischen Sorgfalt. Der Begriff »*kaufmännische Sorgfalt*« (*due care*) bedeutet im juristischen Sinne, dass eine Person oder eine Firma alle zumutbaren Maßnahmen ergreifen muss, um sich und andere zu schützen. Wenn das Management fahrlässig handelt, können Schadensersatzansprüche gestellt werden, die vermeidbar gewesen wären, wenn die richtigen Maßnahmen getroffen worden *wären*. Beispiele für die gebotene Sorgfalt sind die Entwicklung einer Sicherheitspolitik und zugehöriger Verfahren, Schulungen zur Bewusstseinsbildung in der Sicherheit, die Implementierung von Firewalls und Antivirensoftware, Prüfung der Personal- und Rechneraktivität usw. Nahezu alles, was in diesem Buch behandelt wird, hat eine

Verbindung zur Haftung bei Fahrlässigkeit. Das Management hat die Verantwortung dafür, diese Probleme zu verstehen und die Anforderungen der speziellen Unternehmensumgebung zu erkennen.

Im angelsächsischen Sprachraum kennt das Rechtssystem die Begriffe »due care« und »duty of care«, um die Sorgfaltspflicht der Geschäftsführung bzw. des Vorstands zu beschreiben. Fahrlässigkeit (negligence) führt zu den besonders aus den USA bekannten Schadensersatzforderungen in nahezu unbeschränkter Höhe. In der Prüfung wird stets auf das amerikanische Rechtssystem Bezug genommen.

Sicherheit sollte Teil der Unternehmensziele sein und nicht als eigenständige »Insel« behandelt werden. Je mehr Verständnis dafür besteht, wie die Sicherheit in direkter Weise die geschäftlichen Vorhaben, Produktion, Haftung des Managements und den Umsatz beeinflussen kann, desto mehr wird die Sicherheit im unternehmerischen Handeln und in Projekten verankert sein. Es ist wichtig, Sicherheit im Denken der Entscheider zu integrieren; Sicherheit kann kein nachträglicher Gedanke oder Gegenstand sein, der eigenständig behandelt wird, als hätte er keine drastische Wirkung auf nahezu alle umgebenden Bereiche.

Ziel 1.02

1.2 Risikomanagement

Risikomanagement (risk management) ist der Prozess der Identifikation, Bewertung und Reduktion der Risiken auf ein akzeptables Niveau. Genau genommen geht es hier darum, alle Risiken zu begrenzen und so weit zu reduzieren, bis sie für die Organisation akzeptabel sind. Man kann nicht alle Risiken im Leben vollständig ausschließen. Stattdessen muss man lernen, sie richtig zu identifizieren und mit ihnen umzugehen. *Risikoanalyse (risk analysis)* ist ein Werkzeug, um die Risiken für das Unternehmen zu identifizieren, finanzielle Auswirkungen zu berechnen, Schwachstellen zu identifizieren, Bedrohungen und zugehörige Risiken einzuschätzen und die Wirkung zu bewerten, die eintreten würde, wenn man sich die momentan bestehenden Schwachstellen zunutze machen würde. Die Resultate einer Risikoanalyse sollten durch die Verantwortlichen für das Risikomanagement verwendet werden, um die dringlichsten, realistischen und wirtschaftlichen Verfahren und Gegenmaßnahmen zu implementieren. Es geht bei all dem darum, die notwendigen Hausaufgaben zu machen und Daten zu sammeln, um informierte und logisch begründete Entscheidungen zu treffen.

Lokaler Dialekt

Bedrohungsfaktoren (threat agents) sind Einflüsse, die Schwachstellen ausnutzen, beispielsweise Hacker, Viren, Diebe und Schadsoftware.

1.2.1 Risikoanalyse

Zweck einer Risikoanalyse ist es, die tatsächlichen Werte im Unternehmen zu identifizieren und wie hoch der potenzielle Verlust durch Eintreten jeder der möglichen Bedrohungen sein könnte. Sie ist ein Werkzeug zur Sicherstellung der Kosteneffizienz und Relevanz, damit das Sicherheitsmanagement die *wirklichen* Risiken in angemessener Weise abdeckt. Die vier Hauptziele einer Risikoanalyse sind:

- Identifikation der Vermögensgegenstände (assets) und ihres finanziellen Werts (value)
- Identifikation der Bedrohungen (threats)
- quantitative Bestimmung der Auswirkungen (impact) potenzieller Risiken
- Wirtschaftlichkeit der Gegenmaßnahmen (countermeasures) im Vergleich zu den möglichen Auswirkungen des Risikos

Prüfungstipp

Eine Risikoanalyse muss durch die obere Führung des Unternehmens initiiert, gesteuert und unterstützt werden, um Erfolg zu haben. Die Unternehmensführung muss den Umfang und die Ziele der Analyse definieren, die notwendigen Ressourcen bereitstellen und sich mit den Ergebnissen eingehend befassen.

Das Risikoanalyseteam sollte durch das Management ernannt werden und aus Mitarbeitern aller Abteilungen zusammengesetzt sein, um sicherzustellen, dass alle Risiken in allen Unternehmensbereichen identifiziert und begriffen werden.

Wie zuvor erwähnt, sollte jedem Vermögensgegenstand im Unternehmen ein finanzieller Wert zugewiesen sein, der jedoch nicht nur der Anschaffungs- oder Buchwert sein dürfte. Der tatsächliche Wert ist eine Kombination aus Anschaffungswert, Wartungskosten, internem Personalaufwand für die Entwicklung, Bedeutung des Gegenstands innerhalb der Organisation, Wiederbeschaffungswert, Umsatzverlust und Produktivität bei Ausfall des Vermögensgegenstands, sowie die Summe, die ein Wettbewerber möglicherweise für den Gegenstand zu zahlen bereit wäre. Die Kombination dieser Bewertungsansätze sollte einen klaren Hinweis auf den Folgeschaden bei Beschädigung oder Verlust des betrachteten Vermögensgegenstands geben.

Nachdem das Team aufgestellt ist, werden Vermögensgegenstände identifiziert und der finanzielle Gegenwert festgelegt. Der nächste Schritt ist die Ermittlung der Schwachstellen und der möglichen Bedrohungen, die derzeit vorliegen.

Ziel 1.03

1.3 Bedrohungspotenzial

Um eine Bedrohung richtig zu erkennen, müssen Sie wissen, was genau eine Bedrohung ist. Die folgenden Begriffe haben ähnliche Definitionen, aber sehr unterschiedliche Rollen innerhalb der Sicherheit und bedeutende Abhängigkeiten untereinander, wie Abbildung 1 zeigt.

Eine *Schwachstelle (vulnerability)* ist eine dem Mechanismus innewohnende Schwäche, welche die *Vertraulichkeit (confidentiality)*, *Integrität (integrity)* oder *Verfügbarkeit (availability)* eines Vermögensgegenstands bedroht. Eine Bedrohung ist die Wahrscheinlichkeit, dass jemand die Schwachstelle entdeckt und sie zur Verursachung eines Schadens ausnutzt. Der Faktor, der letzten Endes die Schwachstelle findet und nutzt, ist der *Bedrohungsfaktor (threat agent)*. Das Risiko ist die Wahrscheinlichkeit, dass ein Bedrohungsfaktor die Schwachstelle tatsächlich ausnutzt; die *Kompromittierung (exposure)* ist ein Vorfall, bei dem eine tatsächliche Ausnutzung einer Schwachstelle stattfindet. Um das Risiko zu reduzieren, wird eine *Gegenmaßnahme (countermeasure)* eingeführt, die potenzielle Schäden aus einer identifizierten Bedrohung begrenzt und die Schwachstelle absichert. Beispiele für diese unterschiedlichen Konzepte und ihre Beziehungen sind in Tabelle 1.1 aufgeführt.

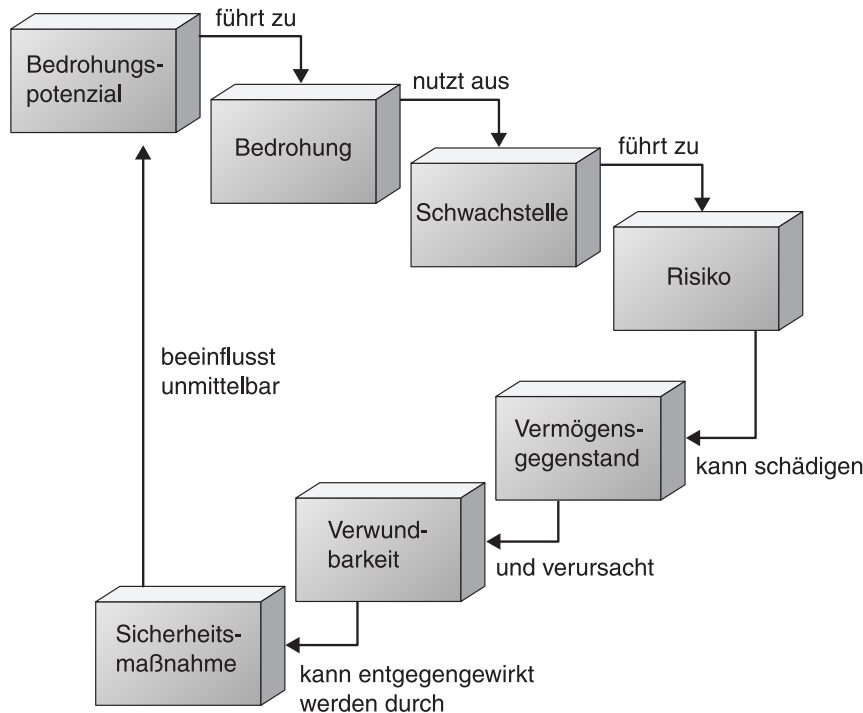


Abb. 1.1: Jeder Begriff hat eine spezielle Rolle in der Sicherheit und eine Beziehung zu einem anderen Begriff

Begriff	Definition	Beispiel
Schwachstelle	Schwäche in einem Mechanismus	Buffer Overflow
Bedrohung	Die Gefahr, dass jemand die Schwachstelle entdeckt und ausnutzt	Hacker nutzt ein Tool, um den Buffer Overflow zu nutzen und sich privilegierten Zugang zum System zu verschaffen
Risiko	Die Wahrscheinlichkeit, dass ein Bedrohungsfaktor eine Schwachstelle ausnutzt (Risiko ist höher, wenn keine Gegenmaßnahmen vorhanden sind)	Wenn der Programmcode schlecht geschrieben ist und keine Firewall für die Zugriffsbeschränkung auf das System mit dem Buffer Overflow vorhanden ist, besteht ein hohes Risiko, dass versucht werden wird, den Buffer Overflow auszunutzen
Gegenmaßnahme	Absicherung, die das Risiko begrenzt	Neuschreiben des Programms oder Ersetzen durch eine Anwendung mit höherer Sicherheit. Firewall und Intrusion Detection System können hier ebenfalls als Gegenmaßnahmen eingesetzt werden

Tabelle 1.1: Definition von Sicherheitsbegriffen und Beispiele

Die Anwendung der richtigen Gegenmaßnahmen kann die Schwachstelle eliminieren und das Risiko reduzieren. Das Unternehmen kann den Bedrohungsfaktor nicht ausschließen, kann sich aber dagegen schützen, dass die Bedrohung zur Ausnutzung von Schwachstellen in der IT-Umgebung führt.

Da wir nun die Definition einer Bedrohung kennen, betrachten wir als nächstes verschiedene Bedrohungen, welche die Vertraulichkeit, Integrität oder Verfügbarkeit eines Vermögensgegenstands negativ beeinflussen können. Diese sind in Tabelle 1.2 dargestellt.

Zugrunde liegendes Prinzip der Sicherheit	Bedrohung	Erläuterungen
Vertraulichkeit	Abschauen (Shoulder Surfing)	Einer Person über die Schulter schauen, um die Eingabe von Kennwörtern oder sensiblen Daten zu verfolgen
	Social Engineering	Vorgeben, jemand anders zu sein, um eine andere Person zur Preisgabe vertraulicher Informationen zu bewegen

Tabelle 1.2: Verschiedene Arten von Bedrohungen und Beispiele

Zugrunde liegendes Prinzip der Sicherheit	Bedrohung	Erläuterungen
Vertraulichkeit	Abfangen von Nachrichten (Message Interception)	Erlangen von Daten, die gerade übertragen werden
	Stöbern (Browsing)	Nach Informationen suchen, ohne notwendigerweise deren Format zu kennen
	Eingabemitschnitt (Keyboard Logger)	Software oder Hardware wird heimlich installiert und protokolliert sämtliche Tastatureingaben des Anwenders
	Netzwerkschnüffeln (Network Sniffing)	Nutzung von Hardware oder Software, um den Datenverkehr im Netzwerk mitzulesen
Integrität		
	Nachrichtenfälschung	Abfangen und Verändern einer Nachricht, dann Weiterversand
	Änderungen der Konfiguration	Änderung kritischer Dateien auf einem Rechner, um dessen Funktionalität zu verändern
	Änderung der Protokolldateien	Veränderung der Protokolldateien, gewöhnlich, um Spuren einer unerlaubten Handlung zu verwischen
	Data Diddling	Veränderung von Daten, bevor sie in den Rechner eingegeben werden, oder direkt bei der Datenausgabe
Verfügbarkeit		
	Natürliche oder von Menschen verursachte Katastrophen	Tornado, Brand, Vandalismus, Erdbeben, terroristische Angriffe etc.
	Denial of Service	Angriff, bei dem so viele Ressourcen des Zielsystems gebunden werden, dass es nicht länger ordnungsmäßig funktioniert
	Versagen einer Komponente	Technischer Fehler, der andere Komponenten oder Geräte beeinträchtigt
	Zerstörung von Daten	Veränderung von Daten bis zu einem Punkt, an dem sie für andere nicht mehr nutzbar sind

Tabelle 1.2: Verschiedene Arten von Bedrohungen und Beispiele (Forts.)

Prüfungstipp

Das Abschauen über die Schulter (shoulder surfing) kann durch Verwendung einer Videokamera erreicht werden, wenn eingegebene Daten an anderer Stelle auf einem Bildschirm gezeigt werden.

Nachdem die Schwachstellen und Bedrohungen erkannt worden sind, sollte das Sicherheitsteam unterschiedliche Gegenmaßnahmen identifizieren, die dem Unternehmen beim Selbstschutz dienlich sind.

Ziel 1.04

1.4 Arten von Kontrollmechanismen in der Sicherheit

Sicherheitskontrollen (security controls) und -mechanismen werden implementiert, um die Vertraulichkeit, Integrität und Verfügbarkeit der Ressourcen zu schützen. Dies sind die drei Hauptprinzipien der Sicherheit, die auch als »CIA-Triade« (von Confidentiality, Integrity, Availability) bekannt sind. Die *Vertraulichkeit* verhindert unberechtigte Offenlegung sensibler Informationen; die *Integrität* verhindert unberechtigte Änderungen an Systemen und Daten; die *Verfügbarkeit* verhindert die Unterbrechung der Dienste und der Produktion.

Wenn ein Kontrollmechanismus in der Sicherheit Vertraulichkeit bietet, gewährleistet er das notwendige Niveau der Geheimhaltung an allen Stellen der Datenverarbeitung und vereitelt alle Versuche der unberechtigten Offenlegung. Ein auf Integrität angelegter Kontrollmechanismus bietet Sicherheit im Hinblick auf die Richtigkeit und Verlässlichkeit der Daten und Systeme; unberechtigte Änderungen werden verhindert. Ein Kontrollmechanismus für die Verfügbarkeit gewährleistet, dass Systeme oder Daten jederzeit in angemessener Form bereitstehen und dass die Ausführung von Anwendungen in vorhersagbarer Form und mit ausreichender Leistung geschieht. Jeder der in diesem Buch angesprochenen Sicherheitsmechanismen zielt in irgendeiner Form auf eines der drei Hauptprinzipien.

Es gibt drei Haupttypen von Kontrollmechanismen zur Wahrung der drei Sicherheitsprinzipien: administrative, technische und physische Kontrollen. *Administrative Kontrollen (administrative controls)* sind gewöhnlich Verantwortlichkeiten des Managements, beispielsweise durch Entwicklung einer Sicherheitspolitik (security policy), Verfahren (procedures) und Normen (standards). Administrative Kontrollmechanismen umfassen außerdem Personenüberprüfungen (personnel screening), Durchführung von Sicherheitsschulungen (security awareness training), Einrichten einer Datenklassifikation (classifying data), Durchsetzung der Regeln (rules are enforced) und Einführung einer Änderungskontrolle (change control).

Technische Kontrollen sind logische Mechanismen, die Ressourcen und Informationen schützen, beispielsweise durch Verschlüsselung (encryption), Firewalls,

Intrusion-Detection-Systeme und Software für den Zugriffsschutz (access control). Solche technischen Mechanismen sind oft durch Software oder Hardware realisiert, die den Zugriff der Anwender (subjects) auf Ressourcen (objects) einschränkt.

Physische Kontrollen schützen Computersysteme, Abteilungen, Personen und die Anlage insgesamt. Beispiele für physische Kontrollmechanismen sind Wachpersonal, Zuanlagen, Schlösser und Beschläge, das physische Entfernen eines Datenträgers und Bewegungsmelder.

Die Geheimhaltung einer Kontrolle sollte nicht als gegeben hingenommen werden und sollte nicht das schützende Element sein. Beispielsweise sollte sich eine Firma nicht darauf verlassen, dass niemand von der Einrichtung eines Intrusion-Detection-Systems weiß und dass daher niemand dieses System umgehen kann. Schon morgen könnte jemand von der Existenz dieser Kontrolle erfahren. Sich auf die Geheimhaltung von Schutzmechanismen zu verlassen, wird als »*security through obscurity*« (in etwa: *Sicherheit durch Verbergen*) bezeichnet und ist nicht immer der beste Ansatz zum Schutz. Ein Unternehmen sollte sicherstellen, dass die implementierten Kontrollen das gewünschte Schutzniveau in einheitlicher Form gewährleisten und sich der Tatsache bewusst sein, dass viele von der Existenz dieser Gegenmaßnahmen wissen und gegebenenfalls die Kontrollen umgehen könnten. Deswegen ist die *Rundumverteidigung (defense in depth)* wichtig, bei der verschiedene Schichten der Sicherheit angelegt werden, statt sich nur auf ein oder zwei Kontrollen oder Absicherungen zu verlassen.

Lokaler Dialekt

Die Begriffe *Kontrolle (control)*, *Absicherung (safeguard)* und *Gegenmaßnahme (countermeasure)* werden in diesem Buch synonym verwendet und beziehen sich auf eine Art von Schutzmechanismus.

In den meisten Unternehmen kommunizieren die Abteilungen für physische Sicherheit und die für Netzwerksicherheit nicht miteinander und wissen nicht einmal, was der jeweils andere Bereich eigentlich macht. Beide Abteilungen haben vermutlich keine sehr gute Vorstellung davon, was das Management für die Sicherheit tut oder unterlässt. Schade, denn beide haben im Grunde das gleiche Ziel – die Firma zu schützen – und nur eine etwas andere Perspektive und andere Schwerpunkte. Gäbe es mehr Dialog und Synergien zwischen diesen unterschiedlichen Kontrollen und Tätigkeiten, könnten Sicherheitslöcher leichter erkannt und verstanden werden. Doppelte Arbeit könnte reduziert werden und damit Zeit und Geld sparen.

Die unterschiedlichen Arten von Kontrollmechanismen (administrativ, technisch, physisch) müssen integriert werden, um einen schichtweisen Ansatz wie in Abbildung 1.2 zu verfolgen. Sie müssen im Einklang arbeiten, um die notwendigen Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität für alle organisatorischen Ressourcen zu erfüllen.

Prüfungstipp

Kontrollen sollten zur Abschreckung deutlich sichtbar sein, aber ihre innere Funktion sollte nicht auf den ersten Blick erkennbar sein, damit Einzelpersonen sie nicht ohne größeren Aufwand umgehen können.

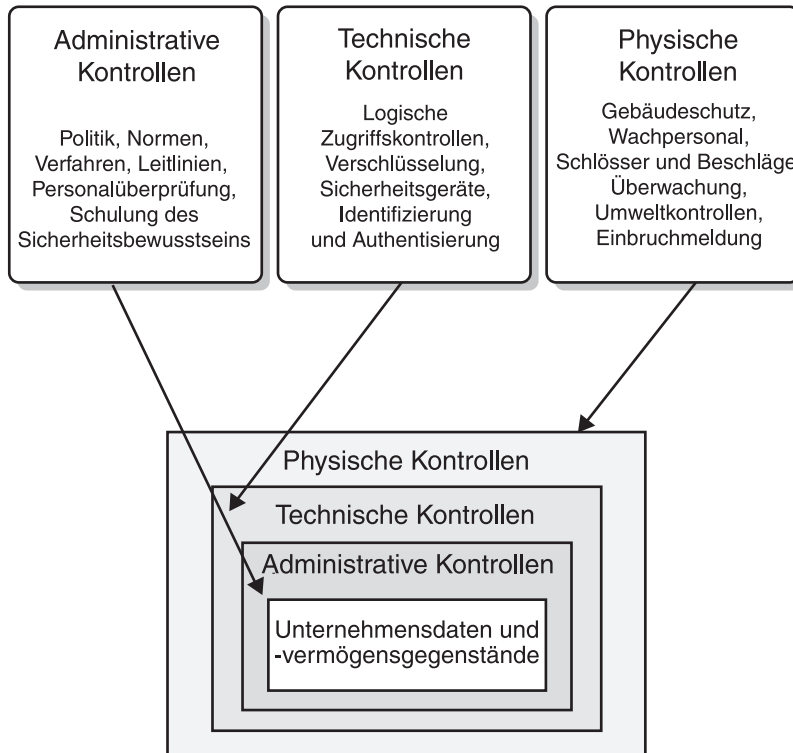


Abb. 1.2: Unterschiedliche Kontrollmechanismen sollten schichtweise arbeiten, um Vermögensgegenstände zu schützen.

Ziel 1.05

1.5 Risikoberechnung

Im Rahmen der Risikoanalyse wird ein *Wirtschaftlichkeitsvergleich* (*cost/benefit comparison*) durchgeführt, um die jährlichen Kosten einer Gegenmaßnahme mit dem geschätzten Schadenspotenzial jedes Risikos zu vergleichen. In den meisten Fällen sollte eine Gegenmaßnahme nur dann implementiert werden, wenn die jährliche Schadenssumme (annualized cost of loss) höher ist als die Kosten der Gegenmaßnahme selbst. Wenn also ein Server 5.000 € wert ist, sollte eine 7000 € teure Schutzmaßnahme für den Server nicht verwendet werden.

Das Sicherheitsteam muss das Risiko des tatsächlichen Eintretens der Bedrohungen kalkulieren und die Auswirkungen berücksichtigen. Dazu gehört die Abschätzung des *potenziellen Schadens* (*potential loss*) und der *Spätfolgen* (*delayed loss*). Spätfolgen sind Schäden, die nicht sofort sichtbar sind, sondern später eintreten – beispielsweise Verlust von Kunden, Nichteinhaltung vertraglicher Verpflichtungen, Rufschädigung, Umsatzrückgang und Pönalen der Kreditoren. Eine Firma, die per eBusiness Produkte verkauft und deren Datenbank mit Kreditkartennummern der Kunden kompromittiert wird, könnte zum Beispiel direkte Schäden und Spätfolgen erleiden. Wenn ein Angriff die Firma zwingt, für einige Stunden offline zu gehen, entsteht ein Umsatzverlust. Die Kosten für beigezogene Experten und Berater für die Ermittlung des Hergangs, aber auch die Kosten des Wiederanlaufs aller Systeme müssten in diesem Beispiel ebenfalls berücksichtigt werden. Das sind die direkten Schäden. Wenn sich der Vorfall bei Kunden und in den Medien herumspricht, wird die Firma wahrscheinlich Kunden verlieren, einen schlechten Ruf haben und für Monate oder Jahre finanziell beeinträchtigt sein (dies sind Beispiele für Spätfolgen).

Zur korrekten Berechnung dieser Auswirkungen muss die Eintrittswahrscheinlichkeit (*likelihood*) mit dem zugehörigen Folgeschaden festgestellt werden. Dafür gibt es zwei grundsätzliche Vorgehensweisen: quantitative und qualitative Risikoanalyse.

1.5.1 Quantitative und qualitative Ansätze

Eine *quantitative* Risikoanalyse versucht, allen Risiken und Folgeschäden exakte Werte zuzuweisen. Dies ist gewöhnlich die bessere Methode, da die Führung die finanziellen Schätzungen recht leicht auf die Gewinn- und Verlustrechnung und die Bilanzsumme abbilden kann. Ein *qualitativer* Ansatz weist jedem Risiko und jeder Gegenmaßnahme eine Punktbewertung (*rating*) zu, das gewöhnlich durch »Bauchgefühl« (*good feeling*) oder auf der Grundlage von Meinungen der Mitarbeiter zustande kommt, die innerhalb des Unternehmens als »Experten« angesehen werden.

Die *qualitative* Analyse verwendet Szenarien, die alle möglichen Bedrohungen und Entwicklungen der Lage darstellen, sodass verschiedene Personen die Hypothesen konzeptionell nachvollziehen und ihre Meinung dazu abgeben können. Nachdem ein Szenario für eine bestimmte Bedrohung geprüft worden ist, werden Einzelpersonen gefragt, ob und in welchem Ausmaß sie diesen speziellen Punkt als echte Bedrohung für das Unternehmen sehen. Die Punktbewertung erfolgt normalerweise auf einer Skala von 1 bis 5 oder nach den Kriterien »niedrig, mittel, hoch«. Danach werden die verschiedenen Gegenmaßnahmen erklärt, und die gleiche Gruppe von Personen bewertet die einzelnen Maßnahmen. Das Endergebnis zielt darauf ab, die Meinungen derjenigen einzuholen, die den potenziellen Bedrohungen am nächsten sind und offenkundig die meiste Erfahrung auf den betroffenen Gebieten haben.

Die Schritte einer qualitativen Analyse:

1. Entwicklung der Risikoszenarien
2. Zusammenkunft der unternehmensinternen »Experten«
3. Durcharbeiten der Szenarien, um identifizierte Bedrohungen zu verstehen
4. Rangfolge der Bedrohung nach Ausmaß, Abschätzung der Eintrittswahrscheinlichkeiten
5. Abstufung der Gegenmaßnahmen nach ihrer Wirkung

Prüfungstipp

Die Delphi-Methode kann genutzt werden, um Einzelpersonen die anonyme Äußerung ihrer Meinung zu ermöglichen. Dadurch wird eine Atmosphäre geschaffen, in welcher der einzelne eher eine ehrliche Meinung äußert und nicht durch andere beeinflusst oder eingeschüchtert wird.

Quantitative Risikoanalyse Da quantitative Bewertungen sich mit Zahlen und finanziellen Werten befassen, sind einige Formeln unvermeidlich. Die zwei wichtigsten Formeln sind der Erwartungswert des *Einzelschadens* (*single loss expectancy, SLE*), der auf den *mittleren jährlichen Schaden* (*annual loss expectancy, ALE*) umgerechnet wird. Ziel des SLE ist die Feststellung des möglichen Gesamtschadens, der durch Beschädigung eines Vermögensgegenstands durch eine spezifische Bedrohung entsteht. Der ALE wird benutzt, um den logisch sich ergebenden Maximalaufwand für die Absicherung des Vermögensgegenstands zu ermitteln.

(1) SLE = Gesamtrisikofaktor x Wert des Vermögensgegenstands

oder auf Englisch:

Single loss expectancy = exposure factor (EF) x asset value

(2) ALE = SLE x jährliche Häufigkeit des Ereignisses

Englisch:

ALE = SLE x annualized rate of occurrence (ARO)

Der *Gesamtrisikofaktor* (*exposure factor, EF*) ist die geschätzte Prozentzahl des vermutlich stattfindenden Schadens. Die *jährliche Häufigkeit des Ereignisses* (*annualized rate of occurrence, ARO*) ist die geschätzte mittlere Häufigkeit, mit der das Ereignis eintritt. Da der ARO-Wert auf das Jahr umgerechnet wird, kann er maximal 1,0 sein. Wenn das Ereignis einmal in zehn Jahren eintritt, ist der ARO bei 0,1 und für ein Ereignis in 100 Jahren bei 0,01.

Wenn das Analyseteam beispielsweise einen Tornado als Risiko für das Unternehmen ermittelt, könnte dies zu folgenden Berechnungen führen: Ein Tornado wird vermutlich etwa 50 % des Unternehmens beschädigen, und die Gesamtanlagen

sind 200.000 € wert. Daher ist der SLE-Wert 100.000 €. Wenn nur alle zehn Jahre ein Tornado vorkommt, liegt der ALE-Wert bei 100.000 €:

$$(3) 200.000 \text{ €} \times 0,5 = 100.000 \text{ € (SLE)}$$

$$(4) 100.000 \text{ €} \times 0,1 = 10.000 \text{ € (ALE)}$$

Für das Analyseteam und die Führung des Unternehmens bedeutet dieser Wert, dass jährlich bis zu 10.000 € für den Schutz vor Tornados ausgegeben werden können. Ausgaben von mehr als 10.000 € wären übertrieben und wirtschaftlich nicht sinnvoll.

Diese Informationen werden für alle Vermögensgegenstände und alle Bedrohungslagen erhoben und dann an das Management übergeben, um in Bezug auf die Sicherheit gut informierte und logisch richtige Entscheidungen zu treffen. Die Analyseergebnisse helfen dem Management dabei, Prioritäten für unterschiedliche Risiken zu setzen, das tatsächliche Gesamtrisiko für das Unternehmen zu erkennen und ein entsprechendes Sicherheitsbudget aufzusetzen.

Orientierungshilfe

Bei der Durchführung einer Risikoanalyse werden viele zusätzliche Formeln und Berechnungen benötigt; SLE und ALE sind nur zwei davon. Für Prüfungszwecke sind dies die zwei Formeln, die Sie kennen und verstehen sollten.

Eine rein quantitative Risikoanalyse ist unmöglich, da viele der betrachteten Ereignisse nur geschätzt werden können und daher qualitativer Natur sind. Die Schätzung, dass ein Tornado nur 50 % der unternehmenseigenen Anlagen beschädigt, ist eine qualitative Annahme, weil niemand wirklich wissen kann, ob 10 % oder 100 % des Schadens sich tatsächlich ereignen werden. Das Ziel der Risikoanalyse ist also, auf Basis der vorhandenen Informationen sinnvolle Abschätzungen zu treffen.

Die Schritte der quantitativen Risikoanalyse in der Übersicht:

1. Verständnis der Ziele und des Umfangs der Analyse
2. Schätzung und Zuweisung finanzieller Werte zu den Vermögensgegenständen, die geschützt werden sollen
3. Identifikation der Schwachstellen und der Bedrohungsfaktoren
4. Abschätzung des potenziellen Gesamtschadens für jedes Risiko
5. Abschätzung der Eintrittswahrscheinlichkeit und der erwarteten Häufigkeit des Eintretens der Ereignisse
6. Vorschläge für kostenoptimale Absicherung und Bewältigungsmaßnahmen, die zur Begrenzung des Risikos implementiert werden können
7. Nach Ende der Risikoanalyse: Dokumentation der Informationen und Präsentation gegenüber dem Management

1.5.2 Umgang mit Risiken

Der Zweck der Risikoanalyse und des Risikomanagements ist es, Wege zur Begrenzung des Risikos zu finden. Es gibt keine hundertprozentig sicheren Systeme oder Anlagen und man kann nicht alle Risiken beseitigen. Folglich müssen Risiken identifiziert, verstanden und angemessen behandelt werden. In den meisten Fällen muss ein Restrisiko hingenommen werden. Das *Gesamtrisiko (total risk)* besteht vor Implementierung der Gegenmaßnahmen; das *Restrisiko (residual risk)* danach. Im Folgenden werden konzeptionelle Formeln gezeigt, die zum Verständnis dieser Risikotypen beitragen:

$$(5) \text{ Bedrohungen} \times \text{Schwachstellen} \times \text{Wert der Vermögensgegenstände} \\ = \text{Gesamtrisiko}$$

Englisch:

$$\text{Threats} \times \text{vulnerability} \times \text{asset value} = \text{Total risk}$$

$$(6) \text{ Gesamtrisiko} \times \text{Gegenmaßnahme} = \text{Restrisiko}$$

Englisch:

$$\text{Total risk} \times \text{countermeasure} = \text{Residual risk}$$

Das Management hat mehrere Möglichkeiten, mit Risiken umzugehen:

- **Transfer des Risikos** Abschluss einer Versicherung
- **Reduzierung des Risikos** Implementierung einer Gegenmaßnahme
- **Akzeptanz des Risikos** keine Aktion, Hinnahme des Risikos, wie es ist
- **Zurückweisung des Risikos** Risiko ignorieren und so tun, als ob es nicht da wäre

Wenn eine Gegenmaßnahme mehr kosten würde als der erwartete potenzielle Schaden, kann sich das Management dafür entscheiden, das Risiko zu akzeptieren (accept) und keine weiteren Maßnahmen zu ergreifen. Falls man das Risiko nicht allein tragen möchte, kann durch Abschluss einer Versicherung das Risiko transferiert (transfer) werden. Wenn eine Gegenmaßnahme implementiert wird, reduziert sich das Risiko (reduce) auf das Restrisiko. Wenn das Management das Risiko verdrängt oder nicht wahrhaben will, erfolgt eine Zurückweisung – eine verantwortungslose Haltung, die bei Eintreten des Ereignisses zu Haftungsfällen führen kann.

1.5.3 Auswahl der Gegenmaßnahmen

Wenn sich ein Unternehmen für die Reduzierung des Gesamtrisikos durch Gegenmaßnahmen entscheidet, müssen diese einige Anforderungen erfüllen, wie im Folgenden dargestellt wird. Gegenmaßnahmen müssen:

- eine kosteneffiziente Sicherheitslösung für ein bekanntes Problem bieten

- es vermeiden, sich auf die Wirksamkeit der Mechanismen nur durch Geheimhaltung zu verlassen
- prüffähig sein, sodass das behauptete Schutzniveau nachvollziehbar ist
- einheitlichen Schutz für alle Vermögensgegenstände und Anwender bieten
- von anderen Absicherungen isoliert sein und nur geringe Abhängigkeiten zu diesen aufweisen
- minimale menschliche Intervention erfordern und vor Manipulation geschützt sein
- vor Außerkraftsetzung geschützt sein und bei Ausfall in einen sicheren Zustand übergehen
- bei Rücksetzen oder Wiederanlauf dennoch die Schutzwirkung aufrechterhalten
- differenzierte Zugriffsrechte vorsehen: administrative Rechte für die Konfiguration und Anwenderrechte, die keine Konfiguration oder Abschaltung der Absicherung erlauben

Lokaler Dialekt

Ein Übergang in einen sicheren Zustand bei Ausfall (fail-safe default) bedeutet, dass der Mechanismus bei Störung oder Ausfall kein Risiko für den zu schützenden Vermögensgegenstand sein darf. Beispielsweise sollte eine Firewall bei Versagen keinen Datenverkehr mehr zulassen, anstatt »aufzumachen« und jeglichen Datenverkehr zur inneren Netzwerkumgebung durchzulassen.

Ziel 1.06

1.6 Sicherheitspolitik und unterstützende Dokumente

Bis zu diesem Punkt hat das Sicherheitsteam im Rahmen der Risikoanalyse alle Vermögensgegenstände identifiziert, ihnen einen finanziellen Wert zugewiesen, Bedrohungen und zugehörige Gegenmaßnahmen ermittelt. Das Management ist über die Situation informiert worden und hat über den Umgang mit den Risiken entschieden. Die notwendigen Gegenmaßnahmen sind abgestimmt. All diese Schritte sollten abgeschlossen sein, *bevor* ein Sicherheitsmanagement entwickelt wird, weil dadurch gut informierte Entscheidungen und solide Grundlagen für ein solches Programm ermöglicht werden.

Sicherheitsmanagement ist die Gesamtheit der Politik, der Verfahren, Dokumente, Normen und Kontrollen der Einhaltung dieser Verpflichtungen, der Hardware, Software, Schulung und des Personals. All diese Faktoren müssen zusammenwirken, um das Unternehmen und seine Vermögensgegenstände zu schützen. Der Rest dieses Kapitels beschäftigt sich tiefergehend mit einigen der Dinge, die ein Sicherheitsmanagement ausmachen.

1.6.1 Sicherheitspolitik

Der nächste Schritt des Managements ist die Entwicklung einer *Sicherheitspolitik* (*security policy*). Es handelt sich um ein Dokument, das generelle Anweisungen der Führung zur Rolle der Sicherheit im Unternehmen enthält. Die Sicherheitspolitik etabliert einen Rahmen für die Einrichtung eines Sicherheitsprozesses, die übergeordneten Ziele, die Verantwortlichkeiten, die strategische und taktische Bedeutung der Sicherheit, und legt dar, wie dies durchgesetzt werden soll. Die Politik muss Gesetzgebung, Vorschriften und Haftungsfragen für das Unternehmen behandeln und zeigen, wie diese Anforderungen zu erfüllen sind. Die Sicherheitspolitik gibt die Richtung für alle sicherheitsbezogenen Aktivitäten an, die zukünftig im Unternehmen stattfinden werden.

Nachdem die Sicherheitspolitik erstellt worden ist, können Normen (*standards*), Leitlinien (*guidelines*), Mindestanforderungen (*baselines*) und Verfahren (*procedures*) entwickelt werden. Jedes dieser Dokumente unterstützt die allgemeine Sicherheitspolitik und hilft bei ihrer Durchsetzung; damit bekommt die Sicherheitspolitik eine Struktur und einen Inhalt.

1.6.2 Normen

Normen (*standards*) sind Regeln für Mitarbeiter, die klar aussagen, was beispielsweise am Arbeitsplatz zu tun und zu unterlassen ist, wofür Geräte benutzt werden und welche Softwarekonfiguration für bestimmte Produkte zulässig ist. Sie haben Vorschriftencharakter und ihre Befolgung ist zwingend. Das Ziel solcher Normen ist Konsistenz in der Nutzung der unternehmenseigenen Vermögensgegenstände, dem Anwenderverhalten und der Haltung gegenüber der Sicherheit. Normen werden häufig eingeführt, um beispielsweise das Verbot des Downloads pornographischer Materials, unangemessene E-Mail-Nutzung, spezielle Anweisungen für die Installation von Servern, die Ausweispflicht im Gebäude oder die Protokollierung und Überwachung von Anwenderaktivitäten zu regeln. Die Normen werden direkt von der allgemeinen Sicherheitspolitik abgeleitet.

Prüfungstipp

Wenn eine Person fortdauernd gegen die Vorschriften und die Sicherheitspolitik verstößt, sollte dieses Verhalten den Vorgesetzten gemeldet und nicht in einer direkten Konfrontation angesprochen werden.

Im englischsprachigen Raum gibt es viele Sicherheitsmaßnahmen, die für deutschsprachige Länder so nicht zulässig sind. Beispielsweise ist die Überwachung des Mitarbeiters am Arbeitsplatz üblich, ebenso wie die interne Klärung zweifelhafter Verhaltensweisen ohne Einschaltung der Polizei. In der Prüfung werden amerikanische Gesetze und Vorschriften vorausgesetzt; manche Fragen sind dadurch anders zu bewerten, als Sie dies in Deutschland, Österreich oder der Schweiz tun würden.

1.6.3 Mindestanforderungen

Eine *Mindestanforderung (baseline)* beschreibt das Minimum an Sicherheit, das im Unternehmen gefordert ist. Mindestanforderungen können direkt auf die Rechner hin formuliert werden, für die sie notwendig sind. Beispielsweise könnte gefordert sein, dass alle Computer in der Buchhaltung mindestens eine C2-Klassifizierung (nach den Common Criteria) haben müssen. Das ist wohlgermerkt nur das Minimum, und stärkere Sicherheitsmechanismen können jederzeit hinzugefügt werden. Alle betroffenen Systeme müssen jedoch die Mindestanforderungen erfüllen. Eine Mindestanforderung wird bisweilen als Abstraktion einer Norm bezeichnet – die Mindestanforderung ist das Ziel, und die Norm beschreibt, wie das Ziel erreicht werden soll. Wir folgen also den Normen (standards), um ein bestimmtes Sicherheitsniveau (baseline) zu erreichen.

1.6.4 Verfahren

Verfahren (procedures) sind detaillierte, schrittweise Anleitungen zur Erfüllung einer spezifischen Aufgabe. Beispielsweise kann ein Verfahren bestehen, um Schritt für Schritt ein Anwender-Account aufzusetzen, diesem Rechte zuzuweisen und ein neues Postfach zu konfigurieren. Es kann Verfahren geben, nach denen neue Server installiert werden, welche Konfiguration zu wählen ist und welche Service Packs zu benutzen sind. Verfahren stellen sicher, dass unabhängig von den handelnden Personen unternehmensweit standardisierte Abläufe vorliegen, die kontrolliert wiederholbar sind.

1.6.5 Leitlinien

Vielfach sind sich Firmen nicht sicher, wo die Entwicklung eines Sicherheitsmanagements anfängt und aufhört, welche Dinge angesprochen werden müssen und welche Bestandteile das Sicherheitsmanagement bilden oder wie spezielle Fragestellungen gehandhabt werden sollten. *Leitlinien (guidelines)* sind Empfehlungen und operative Hinweise für Unternehmen und werden oft als »best practices« bezeichnet.

Es gibt genormte Leitlinien, die Hinweise für Firmen, Sicherheitsexperten und Dateneigentümer geben, beispielsweise ISO 17799. Firmen können auch ihre eigenen internen Leitlinien haben, um die Behandlung bestimmter Fragestellungen zu regeln. In einer IPsec-Implementierung zum Beispiel könnte ein Unternehmen die Leitlinie haben, die einen stärkeren Verschlüsselungsalgorithmus verlangt, so immer dies möglich ist, etwa 3DES statt DES.

Lokaler Dialekt

ISO 17799 sind international genormte Leitlinien, die unter anderem die Entwicklung einer Sicherheitspolitik, die Klassifikation der Vermögensgegenstände, Zugriffskontrollen und die Einhaltung der Verpflichtungen regeln.

Mittlerweile sind deutschsprachige Versionen des Leitfadens ISO 17799 beim Österreichischen Normungsinstitut als ÖNORM 17799 und ÖNORM 7799 erhältlich. Die Normen regeln die Gestaltung des Informationssicherheits-Management-systems (ISMS) und beziehen sich daher auf Managementfragen, im Gegensatz zu den »Common Criteria« (ISO 15408), die sich auf Produkte beziehen.

Normen, Leitlinien und Mindestanforderungen sind allesamt von der allgemeinen Sicherheitspolitik abgeleitet und unterstützen diese beziehungsweise helfen bei der Implementierung. Wenn die Politik ganz allgemein und etwas vage gehalten ist, sind die anderen Dokumente meistens sehr spezifisch und granular.

Ziel 1.07

1.7 Rollen und Verantwortlichkeiten

Jeder hat im Leben eine Rolle, die gewisse Verantwortlichkeiten mit sich bringt. Das gilt auch für das Sicherheitsmanagement im Unternehmen. Klare Rollen und Verantwortlichkeiten stellen sicher, dass jeder weiß, was von ihm erwartet wird. Sie verhindern die typische Haltung, die sich im Satz »Das gehört nicht zu meinem Aufgabengebiet« äußert, und – allen anderen Dingen voran – stattet uns mit einem Schuldigen aus, den wir scheinbar immer als notwendig erachten.

1.7.1 Dateneigentümer

Jede Person im Unternehmen hat eine unterschiedliche Verantwortung in Bezug auf die Sicherheit. Der letzte *Dateneigentümer (data owner)* ist ein Mitglied der Geschäftsführung und verantwortlich für den Schutz der firmeneigenen Vermögensgegenstände, also auch der Daten. Diese Person ist zur kaufmännischen Sorgfalt verpflichtet und haftet bei Kompromittierung der Daten. Der Dateneigentümer bestimmt das Klassifizierungsniveau der Daten, die Art des Schutzes für Vermögensgegenstände und den Zugriff darauf. Er delegiert die Aufgaben des Tagesgeschäfts an andere, die diese Anweisungen ausführen und die Regeln durchsetzen müssen.

1.7.2 Datenmanager

Der *Datenmanager (data custodian)* – der »Hüter der Daten« – übernimmt im Wege der Delegation die Verantwortung für die Wartung und den Schutz der unternehmenseigenen Vermögensgegenstände und Daten. Diese Person oder Abteilung installiert und konfiguriert Hardware und Software, führt Datensicherungen durch, prüft die Vertraulichkeit, Integrität und Verfügbarkeit der Ressourcen und führt die täglichen Aufgaben aus, welche die Funktion des Systems und den Schutz der Daten gewährleisten. Diese Rolle wird gewöhnlich der IT-Abteilung übertragen.

1.7.3 Anwender

Der *Anwender (user)* ist jeder, der regelmäßig Firmeneigentum und -daten verwendet, um ihre bzw. seine Rolle und Verantwortlichkeiten innerhalb des Unternehmens wahrzunehmen. Der Anwender muss den notwendigen Zugriff auf die Daten haben, um die operativen Aufgaben erledigen zu können, und muss operative Sicherheitsverfahren und Normen einhalten, um die Vertraulichkeit, Integrität und Verfügbarkeit der Ressourcen sicherzustellen. Anwender sollten begrenzte Zugriffsrechte haben, was die Konfiguration der Ressourcen und die Handhabung von Daten angeht.

1.7.4 Sicherheitsprüfer

Die *Revision in der Sicherheit (security auditor)* ist eine Person oder Gruppe, die periodisch Prüfungen der Sicherheitsverfahren und der zugehörigen Mechanismen im Unternehmen vornimmt, um die Einhaltung vorgegebener Schutzziele zu gewährleisten. Diese Art von Prüfung wird normalerweise in bestimmten Branchen verlangt, beispielsweise im Finanzsektor, Teilen der Regierung und im Gesundheitswesen. Der Dateneigentümer oder ein bevollmächtigter Vertreter muss seine Zustimmung erteilen, bevor eine Prüfung durchgeführt wird. Diese Zustimmung sollte in nachvollziehbarer Weise dokumentiert werden.

Prüfungstipp

Wenn ein Prüfer Zugriff auf Daten benötigt, die durch logische Zugriffskontrollen geschützt sind, sollte eine schriftliche Zustimmung vorliegen, bevor der Prüfer irgendeinen Zugriff vornimmt.

Im deutschsprachigen Raum wird die Sicherheitsüberprüfung im Regelfall durch den Wirtschaftsprüfer durchgeführt und ist durch dessen strenge gesetzliche Auflagen bestimmt. Der Prüfer darf grundsätzlich alles sehen und hat eine Verschwiegenheitspflicht, die gesetzlich geregelt ist. In den angelsächsischen Ländern hingegen ist die Zustimmung (approval) ein wichtiger Bestandteil, der bisweilen durch eigene Vertraulichkeitsvereinbarungen (non-disclosure agreements) zusätzlich abgesichert wird. Die Frage, wann eine Sicherheitsüberprüfung wirklich genehmigt ist, stellt sich in den USA immer wieder.

Entscheidungen über Sicherheitsziele sollten nicht den Datenmanagern überlassen werden, sondern direkt bei der erweiterten Geschäftsführung (senior management) liegen. Diese hat ein umfassenderes Verständnis des Unternehmens und ist letzten Endes verantwortlich, wenn etwas schief geht. Die nächste Schicht unterhalb der erweiterten Geschäftsführung ist das funktionale Management (functional management), das ein detaillierteres Verständnis der Abläufe und der Art, wie diese durch die Sicherheit beeinflusst werden. Noch weiter unterhalb finden sich Gruppenleiter (operational managers) und Personal (staff), die näher am

Betrieb des Unternehmens sind und die technischen Details der vorhandenen Sicherheitsmechanismen verstehen. Jede Schicht hat also ihre eigenen Einsichten in die Sicherheit als Ganzes; es ist wichtig, dass alle den gleichen Weg gehen und die gleichen Ziele verfolgen.

Ziel 1.08

1.8 Klassifikation der Informationen

Es wurde schon erwähnt, dass alle Vermögensgegenstände identifiziert und bewertet werden sollten. Das umfasst auch die Informationen. Informationen sind sehr wichtig – manchmal kritisch – für Unternehmen. Die Zuweisung eines finanziellen Werts zu einem Vermögensgegenstand zeigt, wie wichtig er für die Firma ist, welcher Schutzbedarf anzunehmen ist und wie viel Geld im Sicherheitsbudget für die Aufrechterhaltung dieses Schutzes vorgesehen werden sollte. Aus demselben Grund werden Daten klassifiziert. Die Einordnung in eine Klasse zeigt die Wichtigkeit für die Firma, die Sensibilität der Daten, wer darauf zugreifen darf und welche Sicherheitsmaßnahmen zu implementieren sind, um den jeweiligen Datenbestand zu schützen.

Die Klassifikation der Daten stellt sicher, dass die Informationen geschützt werden, indem das erforderliche Niveau der Vertraulichkeit, der Integrität und der Verfügbarkeit festgelegt wird. Jedes Klassifikationsniveau sollte unterschiedliche Prozeduren der Handhabung, Zugriffsverfahren, Normen zur Verwendung der Daten und Verfahren für die Zerstörung nicht mehr benötigter Daten haben. Kriterien für die Einstufung neuer Daten sollten festgelegt werden, anstatt hier oder da in willkürlicher Weise eine Einstufung vorzunehmen.

Orientierungshilfe

Ein typisches Problem in Zusammenhang mit der Klassifikation ist die Deklassifikation (declassification). Sehr oft haben Firmen keine Schritte vorgesehen, um die Einstufung der Daten in eine bestimmte Klasse aufzuheben. Das verschwendet Ressourcen und schwächt die Bemühungen, insgesamt nur kritische und relevante Informationen zu schützen. Deklassifikation sollte in einer Anweisung geregelt werden, und die Schritte zur Aufhebung einer Einstufung sollten in einem Verfahren definiert werden.

Die Klassifikation hilft überdies dabei, den vorhandenen Schutz kosteneffizient zu gestalten, weil Geld nur für den Schutz sensibler Daten ausgegeben wird. Wenn im Gegensatz dazu versucht wird, einfach alles zu schützen, endet das im Normalfall damit, das nichts richtig geschützt wird.

Prüfungstipp

Die Klassifikation und das Einstufen von Daten in eine Klasse liegen in der Verantwortung des Dateneigentümers.

1.8.1 Militärische und kommerzielle Klassifikationen

Das Militär und die Regierungsbehörden beschäftigen sich – im Vergleich zur Privatwirtschaft – wesentlich mehr damit, ihre Informationen geheim zu halten. Aufgrund der unterschiedlichen Ziele dieser Organisationen implementieren sie andere Klassifikationsschemata, um damit andere Zwecke zu verfolgen. Die Klassenstruktur ist gewöhnlich anders, und die Kontrollen zur Durchsetzung der Klassifikationshinweise sind sehr weitreichend.

Die Privatwirtschaft verwendet normalerweise die folgenden Klassifikationsstufen bzw. Klassen (von oben nach unten):

- vertraulich (confidential)
- privat (private)
- sensibel (sensitive)
- offen (public)

Militär und Behörden verwenden hingegen die folgenden Klassen (von oben nach unten):

- streng geheim (top secret)
- geheim (secret)
- verschluss-sache nur für den Dienstgebrauch, VS-NfD (confidential)
- sensibel, aber nicht VS (sensitive but unclassified)
- offen (unclassified)

Während die militärischen bzw. staatlichen Datenklassen international einheitlich verwendet werden, sind in der Privatwirtschaft starke Schwankungen zu beobachten. Im deutschsprachigen Raum sind Klassifikationsstufen meistens nur dort vorhanden, wo ein Unternehmen aufgrund des Geschäftsgegenstands einer Betreuung durch einschlägige Behörden unterliegt. Dagegen wird in den USA und anderen englischsprachigen Ländern von der Einteilung der Daten in die oben erwähnten Stufen ziemlich häufig Gebrauch gemacht. Wichtig ist in diesem Zusammenhang, dass eine hohe Einstufung eines Datenbestands stets Kosten und Aufwand verursacht, die Menge der beispielsweise als »geheim« eingestuft Daten immer möglichst gering sein sollte.

Nachdem das Klassifikationsschema vereinbart worden ist, müssen Kriterien entwickelt werden, nach denen die Information in eine Klasse eingeordnet werden kann. Die folgenden Punkte sind Beispiele für charakteristische Kriterien, die zu prüfen sind, um das notwendige Klassifikationsniveau zu bestimmen:

- Nutzen der Daten
- Wert der Daten
- Alter der Daten
- Schaden, der durch Offenlegung der Daten entstehen könnte
- Schaden, der durch Änderung oder Unbrauchbarmachung der Daten entstehen könnte
- Gesetze, Vorschriften oder Haftung im Zusammenhang mit dem Schutz der Daten
- Auswirkung der Daten auf die nationale Sicherheit
- Wer sollte Zugriff haben?
- Wer sollte den Datenbestand pflegen?
- Wo sollten die Daten aufbewahrt werden?
- Wer sollte in der Lage sein, diese Daten zu reproduzieren?
- Welche Daten erfordern spezielle Kennzeichnungen?

Von diesem Punkt an müssen die Kontrollen und Gegenmaßnahmen zum Schutz der einzelnen Klassifikationsniveaus in Kraft gesetzt werden, die ursprünglich in der Risikoanalyse ermittelt und vom Management genehmigt wurden. Datenmanager (data custodians) sind zu identifizieren, und ihnen wird die Verantwortung für die Implementierung der Kontrollmechanismen und Verfahren auferlegt, um das festgelegte Sicherheitsniveau jederzeit aufrechtzuerhalten.

Die Verfahren zur ordnungsmäßigen Klassifikation der Informationen:

1. Beschreiben Sie Klassifikationsstufen/Klassen (classification levels) und ihre genaue Bedeutung.
2. Weisen Sie auf Sicherheitskontrollen und -mechanismen (security controls) hin, die für jede Klassifikationsstufe erforderlich sind.
3. Entwickeln Sie Kriterien (criteria), die verwendet werden, um die Einstufung neuer Daten zu bestimmen.
4. Der Dateneigentümer (data owner) bestimmt die Einstufung der Daten, für die er/sie verantwortlich ist.
5. Identifizieren Sie den Datenmanager (data custodian), der für die Aufrechterhaltung der definierten Sicherheitsniveaus verantwortlich ist.

6. Dokumentieren Sie jegliche Ausnahmen von den vorher beschriebenen Klassifikationsschritten.
7. Entwickeln Sie Freigabe- und Deklassifikationsverfahren.
8. Integrieren Sie alle Angelegenheiten im Zusammenhang mit der Klassifikation der Informationen im Rahmen eines Programms zur Bewusstseinsbildung (security awareness) in der Sicherheit.

Die Praxis der Klassifikation der Informationen nach diesen Schritten erscheint auf den ersten Blick altmodisch, da neuere Berechtigungskonzepte für Software und Betriebssysteme wesentlich mehr Möglichkeiten bieten. Bedenken Sie aber, dass »Klassifikation« auch alte Daten und Informationen in Papierform umfasst. Bei solchen Dokumenten, beispielsweise Gehaltszetteln, Vereinbarungen über einen Firmenkauf oder Personalakten, ist die Notwendigkeit einer personenunabhängigen Einstufung durchaus einleuchtend.

Ziel 1.09

1.9 Personalmanagement

Der Mensch ist fast immer das schwächste Glied in der langen Kette der Sicherheitsmaßnahmen. Die meisten Sicherheitsvorfälle im Unternehmen gehen von Mitarbeitern aus, nicht von externen Hackern. Personalführung und -management sind der entscheidende Bestandteil eines Sicherheitsmanagements und können eine lange Liste von Risiken minimieren. Die folgenden Themen werden als administrative Kontrollen (administrative controls) für das Personalmanagement angesehen.

Zukünftige Mitarbeiter sollten eine Vertraulichkeitsvereinbarung (non-disclosure agreement) unterzeichnen, und die folgenden Punkte sind gegebenenfalls vollständig zu recherchieren:

- Prüfung des Werdegangs, einschließlich Ausbildung und Zeugnisse bzw. Referenzen
- Drogentest
- Sicherheitsstufe (security clearance)
- Finanz- und Bonitätsprüfung (credit check)

Bei Beendigung eines Arbeitsverhältnisses sollten die folgenden Schritte unternommen werden:

- Mitarbeiter verlässt unverzüglich unter Aufsicht das Gebäude.
- Mitarbeiter gibt Ausweise, Schlüssel und Firmeneigentum ab.
- Ein Abschlussgespräch (exit interview) ist durchzuführen.
- Anwenderberechtigungen (user accounts) sind zu entziehen.
- Kennwörter sind unverzüglich zu ändern.

Hinsichtlich des Umgangs mit dem Personal gelten in Europa und den USA sehr unterschiedliche Regeln. Die Ausforschung der persönlichen Lebensumstände (credit check, background check, employee screening) ist beispielsweise nicht ohne Einschränkungen zulässig, und bei Kündigung oder Aufhebung eines Arbeitsvertrags ist nur sehr selten von einer fristlosen Kündigung (termination, dismissal) die Rede. Das beaufsichtigte Leerräumen des Schreibtischs ist ebenso unüblich wie die unmittelbare Verweisung vom Firmengelände in Begleitung eines (Noch-) Angestellten (leaving facility under supervision). Abschlussgespräche (exit interviews) sind zwar an der Tagesordnung, haben aber in deutschsprachigen Ländern einen eher freundlichen Charakter, während in den USA das Ziel einzig und allein ist, etwaige feindliche Absichten des verärgerten (disgruntled) Mitarbeiters herauszufinden. Für die Prüfung sollten Sie versuchen, sich in die Lage eines amerikanischen Unternehmers oder Managers zu versetzen und die rasche Trennung von Mitarbeitern – mit all ihren Problemen – als alltägliches Ereignis voraussetzen.

Obwohl all diese Punkte für sämtliche Trennungen von Mitarbeitern durchgeführt werden, ist bei Mitarbeitern, die in irgendeiner Weise verärgert sind, die sofortige Abschaltung der Anwenderkonten und die Änderung aller Kennwörter unverzichtbar.

1.9.1 Administrative Kontrollen im Betrieb

Die *Funktionstrennung* (*separation of duties*) muss durchgesetzt werden. Das bedeutet, dass eine Person oder Abteilung kritische Aufgaben nicht unbeaufsichtigt durchführen darf. Wenn getrennte Personen oder Abteilungen unabhängig an einem Arbeitsschritt mitwirken, müsste ein potenzieller Täter unter der Hand mit anderen *zusammenarbeiten* (*collusion*), um irgendwelche Zerstörungen oder betrügerische Handlungen zu begehen. Die Funktionstrennung reduziert daher die Wahrscheinlichkeit eines Betrugsfalls drastisch.

Orientierungshilfe

Der Sicherheitsbeauftragte (security officer) sollte strikt getrennt vom Management und von der IT-Abteilung sein, um sicherzustellen, dass alle Entscheidungen ausschließlich unter dem Gesichtspunkt der Sicherheit getroffen werden. Die Feststellungen und Empfehlungen des Sicherheitsbeauftragten sollten an eine Gruppe berichtet werden, deren Zusammensetzung nicht allgemein bekannt ist.

Eine weitere administrative Kontrolle ist die *Arbeitsplatzrotation* (*job rotation*). Mitarbeiter werden in verschiedenen Funktionen ausgebildet und eingesetzt. Diese Praxis stellt sicher, dass Wissen breit gestreut ist, vermeidet das Problem der Schlüsselpersonen und hilft dabei, betrügerische Aktivitäten festzustellen.

Prüfungstipp

Die Arbeitsplatzrotation kann als Gegenmaßnahme eingesetzt werden, um konspirative Zusammenarbeit (collusion) zu kriminellen Zwecken zu verhindern.

Die letzte Kontrolle, die wir uns ansehen werden, ist das *Sicherheitsbewusstsein* (*security awareness*). Für eine effektive Sicherheit im Unternehmen ist es wichtig, dass von der Geschäftsführung abwärts alle wissen, wie wichtig Sicherheit ist und was von ihnen erwartet wird. Die Schulungen sollten erläutern, *was wann wie* und *warum* in der Sicherheit für Computer, Personal und die physische Umgebung zu tun ist. Dies dient auch dazu, die Haltung der Mitarbeiter zu ändern, damit sie das Anliegen der Sicherheit aktiv unterstützen, statt ständig zu versuchen, Sicherheitsmaßnahmen zu umgehen oder auszuhebeln.

Wenn Mitarbeitern nicht gesagt wird, was man von ihnen erwartet und was das Management als Verstoß betrachtet, wird es für das Unternehmen wesentlich schwieriger sein, Regeln der Sicherheit durchzusetzen. Zudem kann es zu Haftungsfällen kommen, da die Kommunikation der Sicherheit und die Schaffung eines entsprechenden Bewusstseins unter die kaufmännische Sorgfaltspflicht fallen.

1.10 Zwischenstation

Ziel 1.01: Verantwortlichkeiten des Managements Die Geschäftsführung ist letzten Endes verantwortlich für alles, was sich im Unternehmen abspielt. Kaufmännische Sorgfalt muss in der Entwicklung, Pflege und Unterstützung eines Sicherheitsmanagements und aller seiner Elemente beachtet werden. Sicherheit im Unternehmen sollte von oben nach unten und nicht umgekehrt implementiert werden.

Ziel 1.02: Risikomanagement Risikomanagement bedeutet, mit Schwachstellen und Bedrohungen in der Weise umzugehen, die das Unternehmen am besten schützt. Die Firma sollte das akzeptable Risikoniveau festlegen; das Risikomanagement stellt sicher, dass diese Schwelle nie überschritten wird. Die Risikoanalyse als Werkzeug des Risikomanagements ist der Prozess, in welchem alle Vermögensgegenstände identifiziert werden, diesen finanzielle Werte zugewiesen werden, alle denkbaren Bedrohungen ermittelt werden, mögliche Eintrittsrisiken dieser Bedrohungen berechnet werden und Gegenmaßnahmen überlegt werden.

Ziel 1.03: Bedrohungspotenzial Ein Unternehmen sieht sich verschiedenen Arten von Bedrohungen gegenüber. Es ist wichtig, diese zu erkennen und die zugehörigen Gegenmaßnahmen zu identifizieren, die zum Schutz implementiert werden sollten. Eine Schwachstelle ist zugleich eine Schwäche; eine Bedrohung macht sich diese Schwäche zunutze; Gegenmaßnahmen reduzieren das Risiko und bieten Schutz.

Ziel 1.04: Arten von Kontrollmechanismen in der Sicherheit Es gibt verschiedene Kontrollen, die zum Schutz des Unternehmens und seiner Vermögensgegenstände eingesetzt werden können. Sie fallen in eine von drei Kategorien: administrativ, technisch oder physisch. Diese Kontrollmechanismen werden implementiert, um die Vertraulichkeit, Integrität und Verfügbarkeit der Vermögensgegenstände zu schützen.

Ziel 1.05: Risikoberechnung Die Risikoanalyse kann einen quantitativen oder qualitativen Ansatz wählen. Quantitative Methoden weisen den untersuchten Gegenständen numerische oder finanzielle Werte zu. Qualitative Methoden verwenden Punktwertsysteme und Ratings, das »Bauchgefühl« verschiedener Experten und Szenarien. Firmen können sich dafür entscheiden, das durch Analyse ermittelte Risiko zu akzeptieren, zu transferieren, zu reduzieren oder zu ignorieren.

Ziel 1.06: Sicherheitspolitik und unterstützende Dokumente Die allgemeine Sicherheitspolitik enthält die Sichtweise der Geschäftsführung und übergeordnete Vorgaben zur Sicherheit. Normen sind Regeln, die befolgt werden müssen. Verfahren sind schrittweise Anleitungen; Mindestanforderungen beschreiben das minimal erforderliche Maß an Sicherheit; Leitlinien haben empfehlenden Charakter. Diese Dokumente werden von der allgemeinen Sicherheitspolitik abgeleitet und unterstützen diese.

Ziel 1.07: Rollen und Verantwortlichkeiten Jede Person im Unternehmen hat eine Rolle und individuelle Verantwortlichkeiten im Rahmen der Sicherheit. Die Geschäftsführung muss diese Rollen beschreiben, die damit verbundenen Verantwortlichkeiten vorgeben und sie Personen zuweisen. Die hauptsächlichen Rollen in diesem Zusammenhang sind Dateneigentümer, Datenmanager, Sicherheitsprüfer und Anwender.

Ziel 1.08: Klassifikation der Informationen Information ist so zu schützen wie andere Vermögensgegenstände auch. Dies geschieht durch Identifikation, Zuweisung eines Werts, Hinweise auf notwendige Schutzmaßnahmen und Erläuterungen zum Zugriff, zur Pflege und zur Vernichtung der Daten. Der Dateneigentümer ist verantwortlich für die Zuweisung einer Klassifikationsstufe zu den betroffenen Daten. Die unterschiedlichen Klassen beschreiben das Niveau der Datensensibilität. Jede Klasse schreibt andere Handhabungs- und Sicherheitsanforderungen vor.

Ziel 1.09: Personalmanagement Die Belegschaft ist ein bedeutender Faktor im Unternehmen und gewöhnlich der schlimmste Feind der Sicherheit. Mitarbeiter sollten einem ordnungsmäßigen Einstellungs- und Kündigungsprozess folgen und klar darüber informiert werden, was von ihnen erwartet wird. Das Bewusstsein für Sicherheit entsteht durch Schulungen, die mindestens einmal jährlich stattfinden sollten. Funktionstrennung und Arbeitsplatzrotation sollten durchgesetzt werden, um betrügerischen Aktivitäten vorzubeugen.

1.11 Musterfragen

1. Which of the following make up the CIA triad?

- A. Confidentiality, Integrity, Assurance
- B. Confidentiality, Integrity, Availability
- C. Confidentiality, Integration, Assurance
- D. Confidentiality, Integration, Availability

Welche der folgenden Kombinationen bezeichnet die drei Hauptkontrollziele der Sicherheit?

- A. Vertraulichkeit, Integrität, Gewährleistung
- B. Vertraulichkeit, Integrität, Verfügbarkeit
- C. Vertraulichkeit, Integration, Gewährleistung
- D. Vertraulichkeit, Integration, Verfügbarkeit

2. How is the annualized loss expectancy (ALE) calculated?

- A. $SLE \times ARO$
- B. $ARO \times EF$
- C. $SLE \times EF \times ARO$
- D. $ARO \times SLE - EF$

Wie wird der Erwartungswert des jährlichen Gesamtverlusts (ALE) berechnet?

3. Of the following, who has the responsibility of determining the classification levels for information?

- A. User
- B. Data Owner
- C. Auditor
- D. Security Manager

Welche der nachfolgend bezeichneten Personen bestimmt die Klassifikation der Informationen?

- A. Anwender
- B. Dateneigentümer
- C. Sicherheitsprüfer
- D. Sicherheitsmanager

4. Which of the following best describes organizational security policies?

- A. General guidelines defining access control requirements
- B. Suggestions on how to achieve compliance with standards

- C. High-level statements that indicate management's intentions
- D. High-level statements indicating specific technical controls to be used

Welcher der folgenden Begriffe beschreibt am besten die organisatorische Sicherheitspolitik?

- A. Allgemeine Leitlinien zur Definition der Zugriffsschutzanforderungen
 - B. Vorschläge, wie die Konformität mit den Normen erreicht werden kann
 - C. Übergeordnete Aussagen, die Hinweise auf die Haltung der Geschäftsführung geben
 - D. Übergeordnete Aussagen, die Hinweise auf zu verwendende spezifische technische Kontrollmechanismen geben
5. For a company to properly protect its intellectual property and other assets, which of the following would be the best approach when terminating an employee?
- A. Perform an exit interview, have employee review nondisclosure agreement, disable accounts, and change passwords
 - B. Perform an exit interview, disable accounts, and change passwords
 - C. Have employee agree to a transborder agreement
 - D. Outline all employee duties relating to due care before being dismissed

Welche der folgenden Vorgehensweisen ist bei Kündigung eines Mitarbeiters die beste, um den Schutz des geistigen Eigentums und anderer Vermögensgegenstände im Unternehmen sicherzustellen?

- A. Abschlussgespräch durchführen, den Mitarbeiter die Vertraulichkeitserklärung durchlesen lassen, Anwenderaccounts sperren, Kennwörter ändern
 - B. Abschlussgespräch durchführen, Anwenderaccounts sperren, Kennwörter ändern.
 - C. Mitarbeiter zu einer grenzüberschreitenden Vereinbarung verpflichten
 - D. Alle Mitarbeiterpflichten in Bezug auf kaufmännische Sorgfalt darlegen, bevor die Entlassung erfolgt
6. Which of the following best describes the difference between quantitative and qualitative approaches to risk analysis?
- A. A qualitative approach assigns monetary values to assets and percentages to risk probabilities.
 - B. A quantitative approach gets experts' advice.
 - C. A quantitative approach supplies a rating to each risk and countermeasure.
 - D. A qualitative approach uses risk scenarios.

Welche der folgenden Aussagen beschreibt am besten den Unterschied zwischen quantitativen und qualitativen Ansätzen der Risikoanalyse?

- A. Der qualitative Ansatz weist Vermögensgegenständen einen finanziellen Wert zu und weist Eintrittswahrscheinlichkeiten eine Prozentzahl zu.
 - B. Der quantitative Ansatz holt Expertenmeinungen ein.
 - C. Der quantitative Ansatz weist jedem Risiko und jeder Gegenmaßnahme einen Punktwert zu.
 - D. Der qualitative Ansatz benutzt Risikoszenarien.
7. Which of the following is a compulsory rule pertaining to computer or information security?
- A. Standard
 - B. Security policy
 - C. Guideline
 - D. Procedure

Welcher der nachstehenden Begriffe bezeichnet eine zwingende Regel in Bezug auf Computer- oder Informationssicherheit?

- A. Norm
 - B. Sicherheitspolitik
 - C. Leitlinie
 - D. Verfahren
8. Which best describes the purpose of a risk analysis?
- A. Identify liability issues and regulations in place to protect assets
 - B. Identify assets and what technical controls should be put into place to protect them
 - C. Identify assets, vulnerabilities and calculate potential risks
 - D. Identify threats that have a direct relationship to liability

Wodurch wird der Zweck einer Risikoanalyse am besten beschrieben?

- A. Identifikation der Haftungsfragen und der Vorschriften zum Schutz der Vermögensgegenstände.
- B. Identifikation der Vermögensgegenstände und der technischen Kontrollen, die zu ihrem Schutz implementiert werden sollten.
- C. Identifikation der Vermögensgegenstände und Schwachstellen, Berechnung potenzieller Risiken.
- D. Identifikation der Bedrohungen, die eine direkte Beziehung zur Haftung haben.

9. Which of the following most clearly indicates whether specific countermeasures should be put into place?
- A. ALE results
 - B. Countermeasures cost/benefit analysis
 - C. Threat and risk analysis
 - D. Risk evaluation

Welche der folgenden Aussagen weist am deutlichsten darauf hin, ob spezifische Gegenmaßnahmen implementiert werden sollten?

- A. ALE-Werte
 - B. Kosten-Nutzen-Analyse der Gegenmaßnahmen
 - C. Bedrohungs- und Risikoanalyse
 - D. Risikobewertung
10. When is it acceptable for a manager overseeing the execution of a risk analysis not to take action on an identified risk?
- A. When the cost of the necessary countermeasure outweighs the potential cost of the realized risk.
 - B. When the risk reduction measures improve the productivity of the business.
 - C. When the conditions that cause the risk to arise is outside the control of the department.
 - D. It is never acceptable.

Wann ist es für einen mit der Durchführung einer Risikoanalyse beauftragten Manager akzeptabel, hinsichtlich eines identifizierten Risikos keine Maßnahmen zu ergreifen?

- A. Wenn die Kosten der notwendigen Gegenmaßnahme höher als die potenziellen Kosten des eintretenden Risikos sind.
 - B. Wenn die Risikoreduzierungsmaßnahmen die Produktivität des Geschäfts erhöhen.
 - C. Wenn die Bedingungen, die zur Entstehung des Risikos führen, außerhalb der Kontrolle der Abteilung liegen.
 - D. Es ist niemals akzeptabel.
11. A browsing attack is referred to when which of the following takes places?
- A. Attacker is shoulder surfing to identify confidential information.
 - B. Attacker is looking for sensitive data without knowing its format.
 - C. Attacker is collecting electrical radiation and recompiling to uncover sensitive information.
 - D. Attacker is performing dumpster diving.

Es wird als Browsing-Angriff bezeichnet, wenn

- A. der Angreifer über die Schulter schaut, um vertrauliche Informationen zu erlangen,
- B. der Angreifer nach sensiblen Daten sucht, ohne deren Format zu kennen,
- C. der Angreifer elektromagnetische Strahlung auffängt und neu zusammensetzt, um sensible Informationen aufzudecken,
- D. der Angreifer Mülltonnen durchsucht.

1.12 Musterantworten

1. B Die »CIA-Triade« enthält die Hauptprinzipien der Sicherheit, nämlich Vertraulichkeit, Integrität und Verfügbarkeit. Jede Sicherheitskontrolle bedient eines oder mehrere Prinzipien.
2. A Der Erwartungswert des mittleren jährlichen Verlusts (ALE) entspricht dem potenziellen Gesamtschaden (SLE) multipliziert mit der mittleren jährlichen Häufigkeit (ARO). Das Ergebnis gibt dem Management einen Hinweis darauf, wie viel ausgegeben werden kann, um den Vermögensgegenstand vor einer spezifischen Bedrohung zu schützen.
3. B Der letztendliche Dateneigentümer ist die Geschäftsführung, da diese haftet. Sie muss verstehen, dass Daten wichtig sind und wie sie geschützt werden sollten; das ist auch der Grund für eine Klassifikation der Informationen. Die Geschäftsführung kann die Verantwortung für das Dateneigentum delegieren.
4. C Die Politik besteht aus generellen, übergeordneten Aussagen, welche die Absichten der Geschäftsführung und ihre Haltung in Bezug auf Computer, Informationen, Personal und physische Sicherheit im Unternehmen darlegen.
5. A Im Unternehmen sollte für jeden entlassenen Mitarbeiter ein Abschlussgespräch geführt werden; jede gekündigte Person sollte zur Durchsicht der Vertraulichkeitsvereinbarung verpflichtet werden; Anwender-Accounts sind zu sperren, Kennwörter zu ändern, und der Mitarbeiter sollte unter Aufsicht das Gebäude verlassen.
6. D Ein qualitativer Ansatz verwendet Risikoszenarien, um Expertenrat einzuholen und danach die Risiken und Gegenmaßnahmen zu bewerten. Ein quantitativer Ansatz weist Vermögensgegenständen und Risiken finanzielle Werte zu und schätzt die Eintrittswahrscheinlichkeit des Risikos ab.
7. A Eine Norm ist eine Regel, die beschreibt, welche Reaktionen und welches Verhalten das Management vom Einzelnen erwartet. Normen können außerdem beschreiben, wie Geräte zu benutzen sind und wie spezielle Computer zu konfigurieren sind.

8. C Der Grund für die Durchführung einer solchen Art der Analyse ist die Ermittlung dessen, was das Unternehmen besitzt (Vermögensgegenstände), des Werts dieser Gegenstände und der potenziellen Risiken. Sie befasst sich mit mehr als nur den technischen Kontrollen (Antwort B) und ist ein Werkzeug zur Berechnung des Risikos.
9. B Die Gegenmaßnahme muss anhand ihrer eigenen Wertigkeit und nach Kosten-Nutzen-Erwägungen bewertet werden. Der ALE-Wert berechnet den potenziellen Verlust, aber nicht die Kosten einer Gegenmaßnahme, betrachtet also nur einen Teil der Geschichte.
10. A Wenn eine Gegenmaßnahme mehr kostet als der potenzielle Schaden und der Spätfolgeschaden zusammen, ist es eine gute geschäftliche Entscheidung, die Gegenmaßnahme nicht zu implementieren.
11. B Ein Browsing-Angriff geschieht, wenn der Eindringling die persönlichen Dateien, Festplatten oder andere persönliche Gegenstände durchstöbert. Der Eindringling sucht Informationen, weiß aber nicht genau, ob sie in einer Datenbank, Excel-Tabelle oder in einem Dokument gespeichert sind; daher ist das Datenformat unbekannt.