



Markus
Kammermann

Markus
a Campo



CompTIA Security+

Vorbereitung auf die Prüfung SY0-301

Wo liegt denn das Problem?

Wenn Sie sich an den Text aus der Einleitung des ersten Kapitels erinnern, so scheint Laras Welt ähnlich der Welt vieler Anwender wie auch Informatikspezialisten ohne große Anstrengung in Ordnung zu sein. Wozu also der ganze Aufwand zum Thema Sicherheit?

Lesen Sie daher an dieser Stelle bitte den Text in Kapitel 1 noch einmal in Ruhe durch. Notieren Sie sich dabei auf einem Blatt Papier alle Ereignisse im Bericht von Lara, an denen Informationen in Form von Daten, Dokumenten oder Gesprächen weitergegeben werden. Blättern Sie jetzt also zurück und lesen Sie...

Hinweis

Nehmen Sie sich Ihre Zeit für Notizen.

Haben Sie den Text noch einmal gelesen? Und sich dabei Notizen gemacht?

Fragen Sie sich jetzt nach dem Lesen anhand Ihrer Notizen, wer an diesen Informationen Interesse haben könnte, und notieren Sie sich, ob diese Interessenten berechtigter- oder unberechtigterweise daran interessiert sind.

Und jetzt machen wir den letzten Schritt mit dieser Situation: Was passiert, wenn diese Informationen in falsche Hände gelangen? Und wie groß sind die Risiken, wenn Sie die einzelnen Tatbestände Revue passieren lassen?

Damit haben wir miteinander die Ausgangslage geschaffen, warum die Thematik »Sicherheit« von Bedeutung sein kann und vielerorts auch sein muss.

Stellen Sie sich an diesem Punkt doch einmal folgende Fragen zu Ihrem eigenen Umfeld, in dem Sie arbeiten:

- Wie wird bei Ihnen im Unternehmen der Internetzugang der Mitarbeiter geregelt? Gibt es dafür Richtlinien oder Beschränkungen?
- Verfügen Sie über drahtlose Netzwerke und wie sind diese eingerichtet?
- Verfügen Ihre Mitarbeiter über Installationsrechte auf den eigenen Systemen, an denen sie arbeiten?
- Werden in Ihrem Unternehmen Notebooks eingesetzt? Und wie werden diese aktualisiert sowie auf mögliche Gefährdungen überprüft?
- Wissen Sie, welche Ports wozu auf Ihren Firmen-Firewalls offen sind?

- Wie häufig müssen Ihre Mitarbeiter Passwörter für den Systemzugang wechseln? Und wie viele Passwörter müssen die Mitarbeiter kennen?
- Wer darf in Ihrem Unternehmen Auskünfte an externe Personen erteilen?
- Wie ist der Umgang mit E-Mails geregelt? Wer darf was lesen, anhängen, versenden, öffnen, weiterleiten oder speichern?

Nehmen Sie sich auch hier die Zeit, um Ihre persönlichen Antworten zu diesen Fragen zu notieren. Dann lesen Sie weiter, und wir sprechen über die Risiken im Umgang mit Informationen und Informationstechnik.

Hinweis

Nehmen Sie sich Ihre Zeit für Notizen.

3.1 Die Risikolage

Informationen sind wichtige Werte für ein Unternehmen und müssen daher entsprechend gesichert und geschützt werden. Denken Sie nur an Konstruktionspläne, Offerten, Rechnungen, Patentanmeldungen oder andere Informationen, welche für die Wertschöpfung eines Unternehmens von Bedeutung sind.

Zahlreiche dieser Informationen werden heute mithilfe der Informatik erstellt, bearbeitet, gespeichert und transportiert. Ebenso zahlreich ist die Anzahl von Geschäftsprozessen, welche ohne eine zuverlässige Informatik gar nicht mehr denkbar sind. Aus dieser Verknüpfung von Information und Informatik ergibt sich unser Fokus für die Informationssicherheit.

Nach dieser Einleitung, dem Lesen des Textes und Ihren eigenen Notizen und Gedankengängen ist Ihnen wahrscheinlich bewusst, dass zu vielen Gelegenheiten und in verschiedenster Umgebung Informationen und Daten weitergereicht werden, und dass es ebenso viele Risiken gibt, denen diese Daten und die dazu gehörigen Systeme ausgesetzt sind.

Mögliche Risiken können ganz unterschiedlicher Herkunft sein:

- Irrtümer oder Fehler der eigenen Mitarbeiter im Umgang mit Systemen und Anwendungen
- Hard- oder Softwaremängel
- Defekte an Systemen und Netzwerkkomponenten
- Mangelnde Dokumentationen
- Höhere Gewalt wie Feuer oder Wasser
- Malware wie Viren, Würmer und Trojaner
- Informationsdiebstahl und Spionage
- Hacking, d. h. bewusstes Eindringen in Systeme und Netzwerke
- Sabotage und technische Angriffe

Bedeutung und Auftreten dieser Risiken verändern sich immer wieder von Jahr zu Jahr, doch insgesamt lässt sich bis heute zuverlässig aussagen: Die häufigsten Risikoquellen sind bis heute die menschlichen Irrtümer und Fehler, gefolgt von Malware aller Art.

Etwas anders sieht die Schadenstatistik aus. Hier sind die Schäden, welche durch Malware verursacht werden, erstens größer und zweitens häufig teurer als diejenigen, welche durch Mitarbeiter entstehen.

3.2 Kategorien der Informationssicherheit

Die Informationssicherheit, auch IT-Sicherheit oder Datensicherheit genannt, bedient sich zur Beschreibung des Schutzes vor Schaden dreier Kategorien, auch die drei Grundsäulen der Informationssicherheit genannt:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Niemand anderes darf an die Daten gelangen, weder technisch noch organisatorisch.

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf »Daten« angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf »Informationen« angewendet. Der Begriff »Information« wird dabei für »Daten« verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Die *Verfügbarkeit* von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. Die Verfügbarkeit hat dabei zwei Aspekte: Sie muss gewährleistet sein, aber in ihrer Zugänglichkeit auch auf die Berechtigten gemäß Vertraulichkeit und Integrität beschränkt werden.

Weitere Kategorien, welche ergänzend genannt werden können, sind die Verbindlichkeit sowie die Authentizität von Informationen. Die drei oben genannten sind aber die zentralen drei Säulen der Sicherheit.

Der Schutz von Informatiksystemen und -daten wird wiederum in drei Kategorien unterteilt:

- Physische Sicherheit
- Technische Sicherheit
- Organisatorische Sicherheit

Die *physische Sicherheit* kümmert sich um Bedrohungen und Maßnahmen, welche baulich oder gebäudebezogen sind wie etwa der Hochwasserschutz für einen Serverraum oder die Stromversorgung von IT-Systemen.

Die *technische Sicherheit* kümmert sich um alle Risiken und Maßnahmen im Zusammenhang mit den eigentlichen Systemen. Viren und deren Bekämpfung, die Implementierung von Verschlüsselungstechnologien oder der Schutz von Netzwerken sind Themen dieser Kategorie.

Die *organisatorische Sicherheit* kümmert sich letztlich um alle Fragen der Organisation, etwa wer für die Datensicherung zuständig ist, wie häufig ein Passwort gewechselt werden muss oder wer die Meldeliste für Notfälle führt.

Aus operationaler Sicht ergeben sich damit für Techniker und Administratoren unterschiedliche Felder, die es in allen drei obigen Bereichen zu berücksichtigen gilt:

- Computer und Netzwerke
- Sicherheitsmanagement und Richtlinien
- Authentifikation und Zugriffsrechte
- Datensicherung und -sicherstellung
- Gesetzliche Aspekte wie die Sicherstellung des Datenschutzes und dessen unmittelbare Folgen für die Informationssicherheit

Gerade das Sicherheitsmanagement und die dazugehörigen Richtlinien sind aber nicht einzig das Gebiet der technischen Verantwortlichen, da es für die Implementierung dieser Themen zwingend die Unterstützung der Betriebsleitung braucht. Sicherheitsverantwortliche können und müssen die notwendigen Vorschläge einbringen. Doch nur, wenn die Sicherheitspolitik durch das Management getragen und gefördert wird, kann sie im Unternehmen auch wirklich umgesetzt werden. Und damit kommen wir zum nächsten Thema: den Lösungsansätzen für die Sicherheitsproblematik.

3.3 Lösungsansätze im Überblick

Nachdem wir bisher die Problematik der Informatiksicherheit angesprochen haben, wird es Zeit, dass wir uns an dieser Stelle mit Lösungen für diese Probleme auseinandersetzen.

Natürlich geht dies nicht in einem einzigen Kapitel, sonst bräuchte es kaum eine eigene Zertifizierung für diese Thematik. Vielmehr möchte das vorliegende Kapitel in verschiedene Lösungsansätze einführen, welche anschließend in den folgenden Kapiteln detailliert vorgestellt werden.

Halten wir uns das noch einmal vor Augen. Die drei Grundsäulen der Informatik-sicherheit lauten:

- **Integrität:** Es darf auf keine Weise und niemandem möglich sein, zufällig oder unberechtigt Daten zu verändern.
- **Vertraulichkeit:** Nur wer berechtigt ist, darf Zugriff auf für ihn bestimmte Daten und Bearbeitungsmöglichkeiten erhalten.
- **Verfügbarkeit:** Die Daten müssen jederzeit verlustfrei zur Verfügung stehen.

Auf Englisch bestehen dafür auch die Begriffe *Confidentiality* (Vertraulichkeit), *Integrity* (Integrität) und *Availability* (Verfügbarkeit) und daraus abgeleitet die Abkürzung CIA, die Sie in diesem Zusammenhang antreffen, auch in den Bezeichnungen von CompTIA.

Um diese drei Grundsäulen umzusetzen, benötigt ein Unternehmen eine Sicherheitsrichtlinie, welche von oben her durch die Geschäftsstrategie getragen und in konkrete technische und organisatorische Maßnahmen und Richtlinien umgesetzt wird. Im operativen Bereich werden diese Maßnahmen und Richtlinien dann konkret manifestiert, implementiert, durchgesetzt und regelmäßig aktualisiert.

3.4 TCSEC, ITSEC und Common Criteria

Um die Umsetzung von sicherheitstechnischen Maßnahmen zu überprüfen, wurden verschiedene Normen eingeführt, welche diese Prüfung ermöglichen. Da sind zum einen die amerikanische Normen TCSEC (Trusted Computer System Evaluation Criteria). Sie werden umgangssprachlich auch als *Orange Book* bezeichnet. Hierbei handelt es sich um einen von der US-Regierung herausgegebenen Standard für die Bewertung und Zertifizierung der Sicherheit von Computersystemen. Die Norm stammt im Wesentlichen aus den Jahren 1983 bis 1985 und wurde 2005 durch die internationalen »Common Criteria«-Standards ersetzt.

In Europa existieren demgegenüber die Standards nach ITSEC, welche seit 1991 von der europäischen Union formuliert worden sind. Auch ITSEC ist mittlerweile in den Common Criteria aufgegangen.

TCSEC kategorisiert die Sicherheit von Computersystemen in ein hierarchisches System mit vier Hauptstufen: A, B, C und D, wobei »A« ein sehr sicheres System ist und »D« ein unsicheres System. Die meisten Unix- und Windows-Systeme erfüllen von sich aus »C1«, lassen sich aber ohne großen Aufwand auch so konfigurieren, dass sie »C2« erfüllen.

Bei ITSEC lauten die entsprechenden, etwas detaillierter formulierten fünf Klassen dann F-C1 bis F-B3, wobei es dann noch zusätzliche Klassen für die Funktionalität von Systemen gibt. Da das ganze System an dieser Stelle aber zu weit führt, sei es lediglich erwähnt und auf die Seiten des BSI (Bundesamt für Sicherheit in der Informationstechnik) verwiesen (www.bsi.de).

Die bereits erwähnten Common Criteria liegen mittlerweile in Version 3.x vor und wurden zum internationalen Standard ISO/IEC 15408 erklärt.

Mit der ISO-Norm 27001 besteht überdies eine Normenreihe für Informationssicherheitsmanagementsysteme (ISMS), und mit ISO 27002 bis 27005 besteht ein Leitfaden für das Informationssicherheitsmanagement (vormals ISO/IEC 17799:2005, Technical Corrigendum 1 vom 01/07/2007). Diese Norm wurde aus dem britischen Standard BS7799 heraus entwickelt und erstmals 2005 vorgelegt.

Die Norm ISO/IEC 27001 nennt sich »Information technology – Security techniques – Information Security Management Systems – Requirements«. Sie spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profit-Organisationen) berücksichtigt. Die Norm wurde im Jahr 2008 zudem als DIN-Norm veröffentlicht.

3.5 Die IT-Grundschutzkataloge des BSI

Nun sind wir also hier nicht die ersten, welche sich mit der Sicherheit befassen. Für Deutschland, Österreich und die Schweiz ist das BSI dabei die maßgebliche Stelle, welche sich seit vielen Jahren mit dieser Problematik auseinandersetzt und die Ergebnisse seit Jahren auch publiziert, damit Behörden (ihr eigentliches und erstes Zielpublikum) und Unternehmen sich daran orientieren und ihre Informatiksicherheit optimieren können.

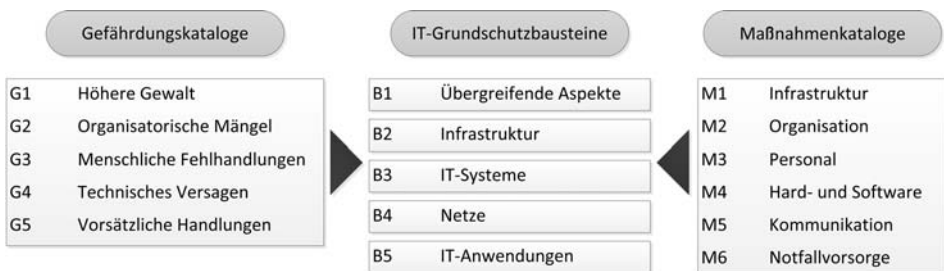


Abb. 3.1: Der Aufbau der IT-Grundschutzkataloge mit den Bausteinen im Schichtenmodell

Die Grundschutzkataloge des BSI sind dreiteilig aufgebaut:

- IT-Grundschutz-Bausteine
- Gefährdungskataloge
- Maßnahmenkataloge

Die einzelnen Bausteine werden dabei als Schichtenmodell dargestellt und behandelt. Diese werden vom BSI selbst wie folgt beschrieben:

- Schicht 1 umfasst sämtliche übergreifenden Aspekte der Informationssicherheit. Beispiele sind die Bausteine Personal, Datensicherungskonzept und Outsourcing.
- Schicht 2 befasst sich mit den baulich-technischen Gegebenheiten. Beispiele sind die Bausteine Gebäude, Serverraum und häuslicher Arbeitsplatz.
- Schicht 3 betrifft die einzelnen IT-Systeme. Beispiele sind die Bausteine Allgemeiner Client, Allgemeiner Server, TK-Anlage, Laptop und Mobiltelefon.
- Schicht 4 betrachtet die Vernetzungsaspekte der IT-Systeme. Beispiele sind die Bausteine Heterogene Netze, WLAN, VoIP sowie Netz- und Systemmanagement.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen Anwendungen. Beispiele sind die Bausteine E-Mail, Webserver und Datenbanken.

(Quelle: BSI-Grundschutzkataloge, www.bsi.de)

Um nun die Sicherheit im Unternehmen nach diesen Grundschutzkatalogen zu optimieren, empfiehlt das BSI folgendes Verfahren:

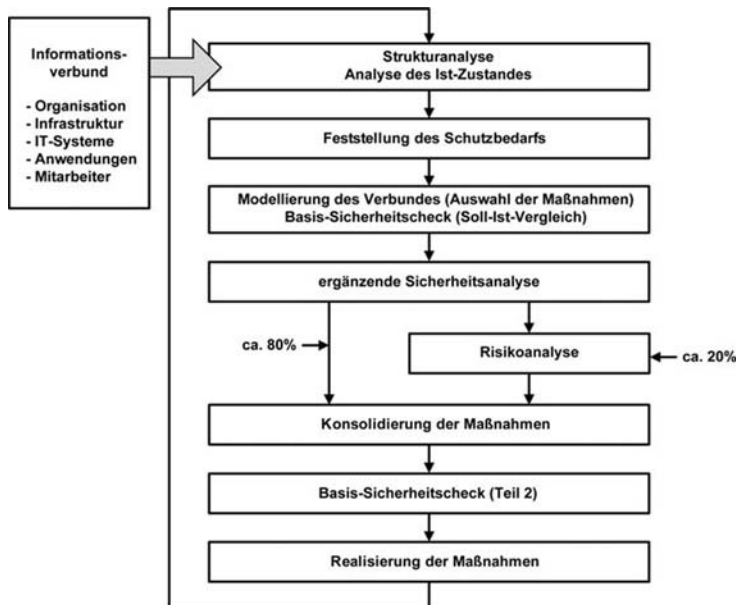


Abb. 3.2: Vorgehensmodell nach BSI (Standard 100-2, Grafik aus diesem Standard entnommen)

Ziel einer Schutzbedarfsfeststellung ist es zu festzustellen, welcher Schutz für die Informationen und die damit eingesetzte Informationstechnik ausreichend und angemessen ist. Dazu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, welche bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist dabei auch eine realistische Einschätzung der möglichen Folgeschäden. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien »niedrig bis mittel«, »hoch« und »sehr hoch«.

Das BSI hat diese Schlüsselfaktoren einer messbaren IT-Sicherheit in den Grundschutzkatalogen klar definiert.

Um die erfolgreiche Umsetzung von IT-Grundschutz nach außen transparent machen zu können, hat das BSI basierend auf der Norm ISO/IEC 27001 ein Zertifizierungsschema entwickelt. Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz oder auch ein Auditor-Testat bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um Informationssicherheit transparent zu machen.

Grundlage für die Vergabe eines entsprechenden ISO 27001-Zertifikats auf der Basis des IT-Grundschutzes ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entscheidet. Kriterienwerke des Verfahrens sind neben der Norm ISO 27001 die in diesem Dokument beschriebene IT-Grundschutz-Vorgehensweise und die IT-Grundschutzkataloge des BSI.

3.6 Lösungsansätze für die Praxis

Die IT-Grundschutzkataloge bieten eine hervorragende Grundlage für die praktische Umsetzung des IT-Grundschutzes. Für das Unternehmen geht es also darum, die in den IT-Grundschutzbausteinen beschriebenen Elemente gemäß Vorgehensmodell (BSI-Standard 100-2) zu analysieren, den Schutzbedarf zu bestimmen und entsprechend zu handeln.

Die Informationssicherheit in ihrer Umsetzung verfolgt drei unterschiedliche praktische Ziele:

- **Vorsorge:** Schutz gegen mögliche Gefahren
- **Entdeckung:** Auffinden von eingetretenen Risiken und Schäden
- **Behandlung:** Reaktion auf Ereignisse mit geeigneten Maßnahmen

Die Vorsorge kümmert sich darum, dass durch die bereits erwähnten, technischen, organisatorischen und physischen Maßnahmen möglichst viele Risiken soweit abgedeckt werden können, dass kein Schadensereignis eintritt. Die Maß-

nahmen zur Entdeckung liegen vor allem im Bereich der Überwachung und ver- helfen dazu, ein dennoch eingetretenes Problem möglichst rasch zu erkennen, um die Auswirkungen zu minimieren. Die Behandlung obliegt dann der vorgängi- gen guten Planung, damit effektiv auf den Schaden reagiert und das operative Geschäft möglichst rasch vollumfänglich wieder hergestellt werden kann.

Für alle diese Ziele und Schritte ist es sehr wichtig, dass das Management und die Mitarbeiter entsprechend ihrer Verantwortung mit einbezogen werden.

Man kann sagen, alles beginnt damit, dass im Unternehmen und bei den einzel- nen Mitarbeitern ein Sicherheitsbewusstsein geschaffen wird, neudeutsch »Secu- rity Awareness« genannt.

Hierbei geht es zum einen um generelle IT-Sicherheitsmaßnahmen, etwa Sicher- heitsvorschriften für allgemeine Arbeiten im Unternehmen, aber auch um Not- fallmaßnahmen oder das Meldewesen.

Es geht im Weiteren um den Umgang mit vertraulichen Daten, was damit beginnt, dass sich das Unternehmen überhaupt bewusst wird, welche Daten wie zu klassifizieren sind, wobei nicht zur vergessen ist, dass der Datenbegriff elektro- nische und auch auf Papier oder Tonband enthaltene Informationen umfasst. Auch die Datensicherung wird an dieser Stelle zum Thema (wer sichert wann was wo und wie).

Ein weiterer Bereich der Security Awareness umfasst den Bereich der persönli- chen Sicherheit am Arbeitsplatz. Wie werden private Arbeiten am Arbeitsplatz gehandhabt, was ist der Umgang mit fremder Software und wie sind Passwort- richtlinien umgesetzt? Auch der Umgang mit dem Internet sowie E-Mail sind hier anzusiedeln.

Nicht zuletzt gehört in die Security Awareness die Ausbildung der Mitarbeiter im konkreten Umgang mit Bedrohungen, angefangen bei Viren und dem Einsatz von Antivirensoftware über den Umgang mit Daten und Dokumenten bis hin zu Umgangsregeln mit Fremden (Stichwort: Social Engineering).

3.7 Sicherheitsmanagement und Richtlinien

Für das Unternehmen ist über das Bewusstsein im Umgang mit der Sicherheit hinaus ein geordneter Umgang mit Informationen entscheidend, welcher durch ein Sicherheitsmanagement gemäß BSI oder ISO 27001 geleistet wird. Dieses mündet in einer übergreifenden Sicherheitsrichtlinie, welche mehrere einzelne Richtlinien enthalten wird, wie etwa:

- Informationsrichtlinien
- Systemsicherheitsrichtlinien
- Administrative Richtlinien

- Disaster-Recovery-Pläne
- Richtlinien zur Benutzerverwaltung
- Richtlinien zur Internet- und Mail-Nutzung
- Softwaredesign-Richtlinien

Die Informationsrichtlinien legen fest, wie Informationen klassifiziert werden und wer welche Informationen zu welchen Bedingungen an wen weitergeben darf. Es wird unterschieden in öffentliche, interne, private und vertrauliche Informationen und festgelegt, wer sich zu welchen Klassen Zugang verschaffen darf.

Systemsicherheitsrichtlinien definieren die Konfigurationen von Netzwerken und Systemen, was die Hardware, die Softwareinstallationen und die Netzwerkverbindungen anbelangt. Auch der Einsatz von Sicherheitssoftware, Passwortregelungen und entsprechende Anforderungen an die Verschlüsselung werden hier definiert.

Administrative Richtlinien legen Regeln für den Unterhalt, die Aktualisierung und die Überwachung von Systemen und Netzwerken fest. Dazu gehören auch Angaben über die Datensicherung oder die Auswertung von Protokollen, welche in der Überwachung erstellt werden.

Disaster Recovery ist für viele Sicherheitsverantwortliche ein Reizwort. Es gilt, die Balance zwischen möglichen Vorkehrungen und realen Risiken zu finden. Braucht das Unternehmen wirklich eine Hot Site oder reichen Ersatzgeräte aus? Wie müssen die Wiederanlaufsznarien definiert werden, damit der operative Betrieb im Katastrophenfall möglichst nicht unterbrochen wird? Eine umfassende und konkret auf das Unternehmen bezogene Risikoanalyse ist hier die Mutter aller sinnvollen Pläne.

Die Richtlinien zur Benutzerverwaltung regeln, wie und durch wen neue Benutzer erfasst werden, wie die Rechte erteilt und bei Bedarf auch angepasst werden (Stichwort: Abteilungs- oder Aufgabenwechsel). Dazu gehört auch, dass man weiß, wer ausgeschiedenen Mitarbeitern den Account wieder sperrt oder nicht mehr benötigte Rechte rechtzeitig wieder entzieht, damit kein Chaos entstehen kann. Ein besonderes Augenmerk gilt hier übrigens gerade den IT-Administratoren selber: Es muss sichergestellt sein, dass bei Personalwechsel auch hier keine Möglichkeit mehr besteht, mit bestehenden Zugriffsberechtigungen auf Systeme zuzugreifen, z. B. weil man vergisst, externe Zugänge wie VPN oder RDP für nicht mehr angestellte Admins zu deaktivieren.

Die Internet- und Mailnutzung wird in einer Richtlinie definiert, die den Mitarbeitern Klarheit darüber verschafft, welche Nutzungen erlaubt und welche untersagt sind. Die Verwendung von Sicherheitsmaßnahmen und auch die (soweit gesetzlich erlaubte) Überwachung von Internet und Mail werden hier festgelegt.

Richtlinien zum Softwaredesign definieren, welche Sicherheitsanforderungen ein System aufweisen muss. Hier wird auch beschrieben, welche Kapazitäten die Anwendung aufweisen muss, damit sie danach sicher betrieben werden kann. Für Eigenentwicklungen sind die Testabläufe hier im Grundsatz festgeschrieben, damit für alle Anwendungen gleichermaßen geregelt ist, wie und in welchem Umfang sie vor der Freigabe für den produktiven Betrieb getestet werden.

Auf alle diese Richtlinien werden wir im Rahmen der weiteren Kapitel zu sprechen kommen, damit Sie in der Lage sind zu erkennen, welche Themen in einer solchen Richtlinie jeweils behandelt werden müssen.

3.8 Fragen zu diesem Kapitel

1. Wofür steht die Abkürzung CIA im Zusammenhang mit Sicherheit in der Informatik?
 - A Confidentiality, Integrity, Availability
 - B Confidentiality, Intrusion, Aversion
 - C Computer Integrity Approved
 - D Computing Industries Award for Security
2. Welche Organisation kümmert sich in Deutschland um die Belange der Informatiksicherheit?
 - A ISO
 - B ANSI
 - C BSI
 - D IEEE
3. Wie nennen sich die drei grundlegenden Elemente, welche in den Grundschutzkatalogen erläutert sind?
 - A Risikoplan, Maßnahmenplan, Grundschutzbausteine
 - B Gefährdungskataloge, Maßnahmenkataloge, Audit-Kataloge
 - C Risikokataloge, IT-Grundschutzbausteine, Maßnahmenkataloge
 - D Gefährdungskataloge, IT-Grundschutzbausteine, Maßnahmenkataloge
4. Welche Sicherheitsmaßnahmen kümmern sich hauptsächlich darum, dass ein Server nicht gestohlen werden kann?
 - A Physische Sicherheit
 - B Organisatorische Sicherheit
 - C Technische Sicherheit
 - D Operative Sicherheit

5. Welche Sicherheitsmaßnahmen kümmern sich hauptsächlich darum, dass Daten auf einem Server nicht gestohlen werden können?
 - A Physische Sicherheit
 - B Organisatorische Sicherheit
 - C Technische Sicherheit
 - D Operative Sicherheit