Inventarisierung

2

Zusammenfassung

Unter dem Stichwort *Inventarisierung* versteht man die Erfassung aller für die Sicherheit der Informationsverarbeitung grundlegenden Elemente und Informationen. Darunter fallen die sensiblen Daten, die verwendeten IT-Systeme und Netze, die darauf aufbauenden IT-Anwendungen, die begleitenden Organisationsstrukturen und Rollen. Eng verbunden damit ist der Prozess des Änderungsmanagements (Change Management). In diesem Kapitel wollen wir den Aufbau einer Inventarisierung und den Pflegeprozess behandeln.

2.1 „Inventar" der Begriffe

In den internen Besprechungen zum Thema Sicherheit operiert man häufig mit unklaren Begriffen: So versteht jeder Beteiligte etwas anderes und es gibt langwierige, ineffektive Diskussionen; das führt oft zu „unscharfen" Analysen in Leitlinien und Konzepten; Ergebnisse werden unterschiedlich interpretiert und sind wenig belastbar, in alle Richtungen auslegbar und damit nichtssagend – letztlich also überflüssig.

Die dringende Empfehlung lautet, ein einheitliches Begriffsverständnis zwischen allen Beteiligten herzustellen und dieses schriftlich festzuhalten – etwa in Form eines Glossars, auf welches alle anderen Dokumente verweisen oder das allen anderen Dokumenten vorangestellt wird. Es sollte stets Basis aller Diskussionen sein. In diesem und den folgenden Kapiteln werden wir deshalb wichtige Grundbegriffe vorstellen und im Zusammenhang erläutern. Hieraus lässt sich ein Glossar aufbauen – eine erste Liste könnte auch aus den Begriffen im Anhang (Fachbegriffe deutsch/englisch) zusammengestellt werden.

Ausgehend von diesem Glossar kann man daran gehen, wichtige Arbeitsschritte zu präzisieren und zu dokumentieren. Ein typisches Beispiel hierfür ist der Ablauf der

H. Kersten, G. Klett, *Der IT Security Manager,* Edition <kes>,
DOI 10.1007/978-3-658-09974-9_2

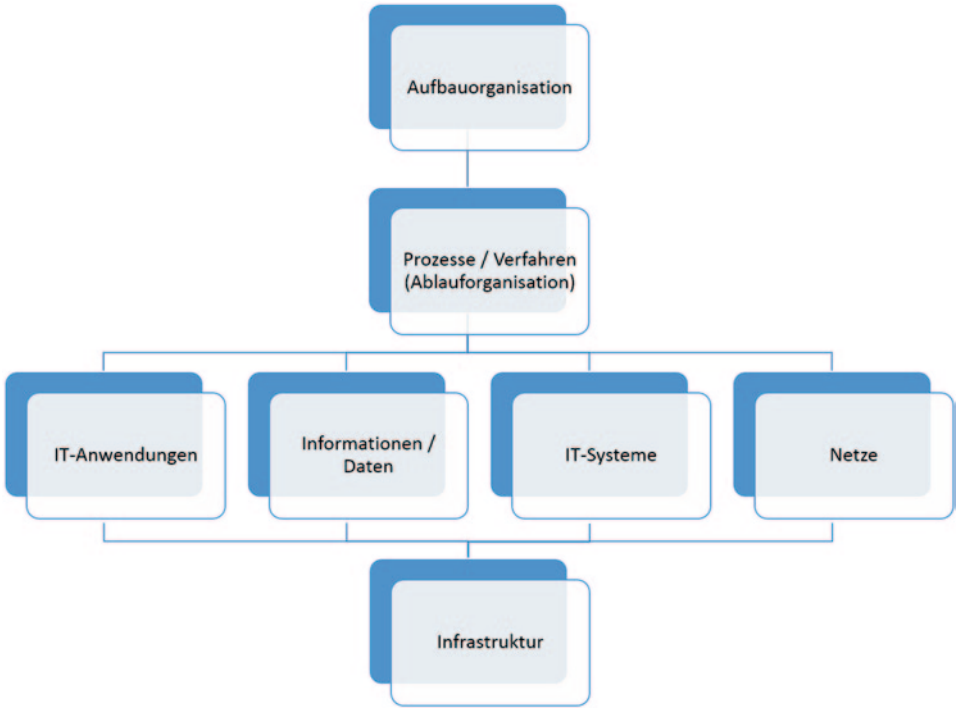

Abb. 2.1 Inventarisierungs-Objekte und -Ebenen

Risikoanalyse und -bewertung. Ohne ein klares, nachlesbares Schema hierfür wird man schnell Schiffbruch erleiden. Solche Beschreibungen kann man in einem z. B. Verfahrenshandbuch ablegen – beim Beispiel der Risikoanalyse und -bewertung könnte man einen entsprechenden Text als einführendes Kapitel einem Sicherheitskonzept voranstellen.

Im Folgenden starten wir mit der Erfassung der organisatorischen und personellen Gegebenheiten und wenden uns dann klassischen Elementen wie IT-Anwendungen, Daten, IT-Systemen, Netzen und der Infrastruktur zu (Abb. 2.1).

Eine wichtige Anmerkung vorweg: In den folgenden Abschnitten beschreiben wir eine sehr umfassende Form der Inventarisierung, die auch einen gewissen Aufwand bedingt. In der Praxis kann man dieses Modell natürlich an die eigenen Wünsche anpassen, verkürzen oder ausbauen. Lesen Sie dazu auch die Zusammenfassung am Ende dieses Kapitels.

2.2 Organisation und Rollen

2.2.1 Grundsätzliches

Als *Organisation* bezeichnen wir im Folgenden Unternehmen, Behörden, Verbände und andere Institutionen, deren Sicherheit analysiert und konzipiert werden soll.

Die innere Gliederung einer Organisation in Organisationseinheiten (Bereiche, Abteilungen, Referate etc.) nennen wir die *Aufbauorganisation*. Sie ist meist in einem entsprechenden Organisationsplan oder Organigramm dargestellt.

Dies gilt sinngemäß auch für größere Verbünde von Organisationen, etwa bei Konzernen, bei denen die Aufbauorganisation des Unternehmensverbunds in einzelne Gesellschaften in entsprechenden Plänen und Übersichten skizziert ist.

Als *Rolle* bezeichnen wir eine Funktion, der bestimmte Aufgaben und damit verbundene Rechte und Pflichten zugewiesen sind. Eine solche Rolle kann im Organisationsplan auftauchen – was aber nicht zwangsläufig ist.

Jede Rolle kann durch eine Person, durch mehrere Personen bzw. eine Gruppe oder durch eine Organisationseinheit als Ganzes besetzt sein. Bei der Besetzung durch eine Person – z. B. als Sicherheitsbeauftragte(r) oder Datenschutzbeauftragte(r) – ist stets eine Vertretung erforderlich, um die Kontinuität der Aufgabenwahrnehmung beispielsweise im Urlaubs- oder Krankheitsfall gewährleisten zu können. Daraus schließen wir, dass eine Rolle mit mindestens zwei Personen zu besetzen ist. Ein klassisches Beispiel die Rollenbesetzung durch eine größere Gruppe stellt die Rolle *System-Administration* dar, in der alle IT-Administratoren einer Organisation zusammengefasst sein können.

Wir wollen einige weitere typische Rollen in einer Organisation aufzählen:

- Ein *Asset Manager* hat die Aufgabe, die Werte (Assets[1]) einer Organisation zu erfassen und zu verwalten – darunter auch die *Information Assets*.
- Ein *Sicherheitskoordinator* arbeitet stellvertretend für eine Organisationseinheit beim Sicherheitsmanagement bzw. in entsprechenden Gremien mit.
- Der *Datenschutzbeauftragte* ist zuständig für die Einhaltung der Datenschutzvorschriften (im Rahmen der Datenerfassung, -verarbeitung und -weitergabe).
- Der *IT-Sicherheitsbeauftragte* bzw. das *IT-Sicherheitsmanagement* ist in einer Organisation für das IT-Sicherheitsthema verantwortlich; die genaue Aufgabenbeschreibung und Abgrenzung unterscheidet sich aber von Organisation zu Organisation (siehe Abschn. 2.2.5).
- Einige weitere Rollen als Stichwörter: Leitung (der Organisation), IT-Leiter bzw. RZ-Leiter, Beauftragter für die Infrastruktur, Werkschutz, Personalvertretung, Backup Manager, IT-Notfallbeauftragter.

Die aufgeführten Beispiele sind *nicht* so zu verstehen, dass alle genannten Rollen bei jeder Organisation vorhanden und besetzt sein müssen:

- Wenn z. B. keine besonderen Anforderungen an die Ausfallsicherheit von IT-Anwendungen bestehen, kann man ggf. auf die Rolle des IT-Notfallbeauftragten verzichten.

[1] Neben den *Information* Assets, die sich auf Informationen und die Informationsverarbeitung beziehen, gibt es andere Typen von Assets – etwa Grundstücke, Gebäude, Anlagen, Maschinen, Personal, Organisationsmittel, Know-how, finanzielle Ressourcen, Kreditwürdigkeit, Image.

- Wenn Rollen nicht explizit vorhanden sind, aber die Aufgaben dennoch wahrzunehmen sind, müssen sie von anderen Rollen übernommen werden. Typisches Beispiel: Die Verwaltung der *Information Assets* (Daten, Systeme, Netze, Anwendungen) gehört zum Asset Management; ist dies jedoch nicht eingerichtet worden, muss z. B. das IT-Sicherheitsmanagement diese Aufgaben übernehmen.

Es kann Rollen geben, die miteinander unverträglich sind, d. h. sie sollten bzw. dürfen nicht von der gleichen Person besetzt sein. Zwei Beispiele dazu:

- RZ-Leiter und IT-Sicherheitsbeauftragter: Hier können sich Interessenkonflikte ergeben, wenn der RZ-Leiter vorrangig den ununterbrochenen „Normalbetrieb" des Rechenzentrums im Auge hat, der Sicherheitsbeauftragte aber aufgrund einer bestimmten Risikolage oder eines Sicherheitsvorfalls bestimmte Anwendungen unterbrechen will.
- IT-Sicherheitsbeauftragter und Datenschutzbeauftragter: Die Beurteilung möglicher Rollenkonflikte ist hier sehr unterschiedlich; z. B. finden sich in [1] in der abschließenden Tabelle Kommentierungen von „empfehlenswert" bis zu „i.d. R unzulässig".

Sind solche Konstellationen von Rollenkonflikten möglich, ist ein *Rollenausschluss* vorzusehen und für Konfliktfälle festzulegen, wer das „Sagen" hat.

Es kommt vor, dass Personen z. B. aufgrund von Personalengpässen mehrere Rollen übernehmen müssen. Solange dies keine Rollenausschlüsse tangiert, ist alles in Ordnung – bleibt noch die Frage, ob diese Situation vom Arbeitsumfang her leistbar ist.

Bei besonderen Situationen – Urlaubs- und Krankheitsfälle, Notfalleintritt – kommt es gelegentlich zu einer temporären *Rollenhäufung*, weil unter dem gegebenen Zeitdruck bestimmte Funktionen oder Aufgaben von dazu eigentlich nicht vorgesehenen Rollen übernommen werden müssen. In der Praxis stellt man dann oft später fest, dass temporär eingerichtete Berechtigungen nicht mehr zurückgenommen worden sind; dann wird aus der *temporären* eine sich schleichend *stabilisierende* Rollenhäufung. Dass diese sogar festgelegten Rollenausschlüssen widersprechen kann, findet dann oft keine Beachtung mehr.

2.2.2 Inventarisierung

Nach dieser langen Vorrede kommen wir zu einem sehr praktischen Punkt, nämlich der *Inventarisierung* aller für die Informationssicherheit relevanten Informationen aus den Bereichen der Aufbau- und Ablauforganisation. Was gehört alles dazu?

1. Es sind Übersichten über den Organisationsaufbau bzw. Organigramme zu inventarisieren.
2. Es sind alle vorhandenen, für die Sicherheit relevanten Rollen zu erfassen – etwa unter Berücksichtigung unserer Beispiele oben.

Tab. 2.1 Rollen-Inventarisierung

Rollen-bezeichnung	Rollen-beschreibung	Arbeits-anweisung	Checklisten	Rollen-ausschlüsse	Rolleninhaber

Beim Arbeitsschritt 1 kann man meist auf Vorhandenes zurückgreifen. Den Arbeitsschritt 2 erledigt man am einfachsten mit einer Tabelle, die natürlich auch Teil einer umfassenden, elektronisch geführten Inventar-Datenbank sein kann. Wie könnte eine solche Tabelle aussehen? Die folgende Tab. 2.1 gibt dazu einen Vorschlag, deren Spalten wir anschließend erläutern.

Eine Rolle erschließt sich nicht immer allein durch ihre Bezeichnung (Spalte 1): Es ist deshalb wünschenswert, für jede Rolle in unserer Tabelle eine *Rollenbeschreibung* zur Verfügung zu haben. Darin sollten folgende Informationen enthalten sein:

- eine Übersicht über die der Rolle zugewiesenen Aufgaben und Verantwortlichkeiten
- damit verbundene Rechte und Pflichten
- Verweise auf Arbeitsanweisungen und Checklisten für die jeweilige Rolle (sofern notwendig und vorhanden)

Zumindest bei Rollen, die *sicherheitsrelevante* Aufgaben haben, sollte zusätzlich in der Rollenbeschreibung oder an anderer Stelle festgelegt werden,

- welche Anforderung an Rolleninhaber betreffend Ausbildung, Berufserfahrung und Spezialkenntnisse gestellt werden (*Anforderungsprofil*),
- wie diese Qualifikationen aufrechterhalten bzw. weiterentwickelt werden sollen (*Schulung und Training*).

Solche Informationen sind insbesondere für die *Besetzung* von Rollen, aber auch für Vertretungs-, Ressourcen- und Schulungspläne wichtig.

Unsere Rollentabelle bauen wir dementsprechend aus und fügen jeweils einen Link auf die entsprechende Rollenbeschreibung ein (Spalte 2).

Für jede sicherheitsrelevante Tätigkeit sollte eine entsprechende *Arbeitsanweisung* vorliegen, in der die Aufgaben Schritt für Schritt zumindest soweit präzisiert sind, dass eine korrekte und nachvollziehbare Abwicklung der Tätigkeiten gewährleistet ist. Jede Arbeitsanweisung wird ggf. weitere Rollen aufführen, die bei den Tätigkeiten zu beteiligen sind, und die entsprechenden Schnittstellen erläutern.

Bei besonders sicherheits*kritischen* Tätigkeiten sieht man ergänzend eine *Checkliste* vor, die bei jeder Durchführung dieser Tätigkeiten ausgefüllt und unterschrieben wird.

Solche Nachweise sind z. B. bei der Installation und Konfiguration von IT-Systemen und anderen Administrationsarbeiten, Update-Prozessen, dem Backup und Recovery notwendig; besonders prädestiniert für Checklisten sind auch Tätigkeiten an sensiblen Systemen wie z. B. Konfigurationsarbeiten an Firewalls.

Die Existenz einer Arbeitsanweisung und ggf. von Checklisten vermerken wir in unserer Rollentabelle (Spalte 2 und Spalte 3) wieder mit einem entsprechenden Link auf das jeweilige Dokument.

Mögliche Rollenausschlüsse lassen sich in einer weiteren Spalte unserer Tabelle eintragen. Man kann hier aber auch einen Verweis auf eine separate Tabelle eintragen, bei der in der ersten Spalte und in der ersten Zeile alle festgelegten Rollen aufgeführt sind; dann markiert man in den Kreuzungspunkten die Rollenausschlüsse (X) oder trägt bestimmte Bedingungen für die Rollenverträglichkeit (z. B. temporär zulässig, falls…) ein.

Man kann in der Tab. 2.1 in weiteren Spalten die Namen der aktuellen Rolleninhaber und Vertreter eintragen sowie entsprechende Kontaktdaten hinzuzufügen. Die Alternative wäre hier wieder, eine separate Besetzungsliste zu erstellen.

Auf diese Weise haben wir eine umfassende Datenbasis über alle für die Sicherheit relevanten Funktionen in unserer Organisation angelegt und können uns über die jeweiligen Aspekte einer Rolle schnell informieren.

2.2.3 Change Management

Nun kommen wir zum Änderungs- und Pflegeprozess: Organisationsdiagramme, die Tabelle der Rollen und Rollenausschlüsse, die verlinkten Rollenbeschreibungen, Arbeitsanweisungen und Checklisten sowie die Besetzungsliste sind nur dann hilfreich, wenn sie stets *aktuelle* Informationen beinhalten.

Änderungen kommen aber in der Praxis sehr häufig vor, weil neue Rollen erforderlich oder vorhandene obsolet werden, Rollenbesetzungen geändert werden, der Aufgabenzuschnitt einer Rolle angepasst wird, eine Arbeitsanweisung wegen neuer technischer Gegebenheiten verändert werden muss u.v.m.

Diese Problematik bekommt man nur mit einem geordneten *Change Management* in den Griff: Eine Änderung an den genannten Daten darf nur auf Antrag und nach Genehmigung vorgenommen werden. Jede Änderung ist zu dokumentieren, die geänderte Dokumentation ist einem Freigabeverfahren zu unterziehen, allen betroffenen Personen zur Kenntnis zu geben und sodann in Kraft zu setzen.

Je nach Art der Änderung wird es unterschiedliche Zuständigkeiten geben: Das Anlegen neuer Rollen (auch deren Löschung) erfolgt ggf. erst nach Zustimmung durch die Leitung oder die Personalabteilung. IT-spezifische Arbeitsanweisungen werden vermutlich in der IT-Abteilung erstellt und vom IT-Leiter in Kraft gesetzt. Die Verteilung dieser Aufgaben wird in jeder Organisation unterschiedlich sein – wichtig ist, dass es klare Zuständigkeiten und einheitliche Verfahren gibt. Dies macht im Kern das Change Management aus.

Eine grundsätzliche Aufgabenverteilung könnte darin bestehen,

- die Rollentabelle zentral zu erstellen und zu pflegen, und zwar durch die für die Aufbauorganisation zuständige Stelle,
- Rollenbeschreibungen und Arbeitsanweisungen dezentral in derjenigen Abteilung zu bearbeiten, in der die betreffende Rolle angesiedelt ist.

Haben Rollenbeschreibungen auch die arbeitsrechtliche Bedeutung einer *Tätigkeitsdarstellung*, so wird man bei Änderungen die Personalabteilung beteiligen müssen.

2.2.4 Organisation der IT-Sicherheit

Immer wieder wird die Frage gestellt, wie die IT-Sicherheit selbst zu organisieren ist: Soll es eine eigene Sicherheitsabteilung geben? Vielleicht ein Querschnittsgremium oder ein Sicherheitsforum? Oder ist die Sicherheitsthematik nur einer bestimmten Person zuzuweisen?

Zunächst ist festzuhalten, dass die Informationssicherheit eine *Vorsorgeaufgabe* und damit grundsätzlich bei der Leitung der Organisation angesiedelt ist. Diese wird die Verantwortung vor allem nach außen wahrnehmen, intern aber die Zuständigkeit delegieren, d. h. eine Rolle für dieses Thema festlegen – das *IT-Sicherheitsmanagement* – und ihr diese Aufgabe (formell) übertragen.

Es ist deshalb anerkannte Praxis und auch in Standards niedergelegt, dass das IT-Sicherheitsmanagement direkt der Leitung der Organisation unterstellt sein soll, zumindest aber einen direkten Berichtsweg zur Leitungsebene haben sollte.

Grundsätzlich sollte das IT-Sicherheitsmanagement nicht Weisungen anderer Fachabteilungen unterstellt sein – natürlich aber den Weisungen der Leitung der Organisation. Bei Letzterem muss dennoch geklärt sein, dass das IT-Sicherheitsmanagement seine fachlichen Ansichten unabhängig präsentieren kann; die Entscheidung über seine Vorschläge liegt aber letztlich bei der Leitung.

Wie bei allen Rollen kann auch das Sicherheitsmanagement entweder durch eine Person (plus Vertreter) – mit der Bezeichnung *(IT-)Sicherheitsbeauftragter* oder *IT Security Manager* – oder durch eine größere Gruppe repräsentiert werden.

Bei den Gruppen ist zunächst die klassische Sicherheitsabteilung zu nennen, die allerdings meist nur in größeren Unternehmen vorhanden ist. In dieser Abteilung könnte der IT-Sicherheitsbeauftragte angesiedelt sein.

Moderner ist die Form einer *Arbeitsgruppe* für IT-Sicherheit oder des *Information Security Forums* (ISF): Falls es einen IT-Sicherheitsbeauftragten gibt, könnte er dieses Forum moderieren oder leiten. Alternativ könnte die Gruppe gemeinschaftlich Verantwortung tragen.

Wer ist sinnvollerweise sonst noch an einer solchen Gruppe zu beteiligen? Im Grunde Vertreter (IT-Koordinatoren) aus solchen Organisationseinheiten, die von dem Thema IT-Sicherheit betroffen sind und damit auch Beiträge zur Sicherheit leisten können. Dazu

dürften in aller Regel gehören: die einzelnen Abteilungen der Organisation, ggf. Verantwortliche für wichtige Geschäftsprozesse, der Datenschutzbeauftragte, der Notfallbeauftragte, die Personalvertretung (Betriebs- oder Personalrat).

Vor allem im deutschen Sprachraum ist es üblich, das IT-Sicherheitsmanagement zunächst in Form eines *IT-Sicherheitsbeauftragten* als Rolle festzulegen. Selbst in diesem Fall sollten die Arbeiten in einer der genannten (Arbeits-)Gruppen durchgeführt, zumindest aber koordiniert werden.

Man findet vor allem in Behörden einen übergeordneten *IT-Koordinierungsausschuss*, dessen Aufgabe die IT als Ganzes ist und der damit geeignet wäre, sich ebenfalls der Sicherheitsthematik anzunehmen. Der IT-Sicherheitsbeauftragte müsste dann Mitglied dieses Ausschusses sein.

Wie ist nun die Tätigkeit des IT-Sicherheitsmanagements einzuordnen und abzugrenzen? Besteht die Aufgabe darin, die Leitungsebene in Sachen Informationssicherheit zu *beraten*? Oder ist das IT-Sicherheitsmanagement intern *verantwortlich* für die Informationssicherheit der Organisation?

Die Praxis zeigt, dass alle Formen vorkommen – von einer reinen Beratungsfunktion (vielfach z. B. bei Behörden) bis hin zur vollen Übernahme der Verantwortung (häufig in straff organisierten Unternehmen). Die Übernahme der Verantwortung kann dabei so weit gehen, dass die Informationssicherheit in Zielvereinbarungen der Beteiligten auftaucht und Auswirkungen auf das individuelle Gehalt hat. Konsequenzen bei „schlechtem“ Sicherheitsmanagement – was das auch immer heißen mag und wie es gemessen wird – sind dann ähnlich wie bei Umsatzverantwortlichen mit einem zu geringen Jahresumsatz.

Grundsätzlich sollte die Funktion natürlich so angelegt sein, dass mehr Verantwortung auch mehr Entscheidungsfreiheit bedeutet.

Bereits erwähnt wurde die dringende Empfehlung, für alle sicherheitsrelevanten Rollen entsprechende *Rollenbeschreibungen* zu erstellen. Dies gilt zuvorderst natürlich für das Sicherheitsmanagement bzw. den IT-Sicherheitsbeauftragten selbst. Neben den grundsätzlichen Anforderungen an Rollenbeschreibungen sollte hier schriftlich festgehalten werden,

- wie das Sicherheitsmanagement aufgestellt ist (Person, Gruppe, Forum etc.),
- wie die Aufgabe verstanden wird (Beratung bzw. Grad der Verantwortung),
- wie weit die Zuständigkeit inhaltlich reicht: z. B. zuständig nur für einen Teil der IT oder für einige benannte Geschäftsprozesse oder Standorte – oder für die gesamte IT,
- welche zeitlichen und inhaltlichen Ziele gesetzt sind.

2.2.5 Aufgaben des Sicherheitsmanagements im Überblick

Wir wollen hier einen ersten Überblick über die Aufgaben des IT-Sicherheitsmanagements geben.

Fall 1: Wir betrachten dazu zunächst eine in sich geschlossene Organisation mit einzelnen Abteilungen und einem IT-Sicherheitsbeauftragten:

- In Abstimmung mit und nach Vorgaben der Leitung ist ggf. die IT-Sicherheitsleitlinie der Organisation zu erstellen, die anschließend von der Leitung in Kraft zu setzen ist (vgl. Kap. 6).
- Aus der Sicherheitsleitlinie sind das Sicherheitskonzept und alle dazu gehörenden Begleitdokumente zu entwickeln, in der Organisation abzustimmen und der Umsetzung zuzuführen (vgl. Kap. 8).
- Der Themenbereich *Sensibilisierung, Schulung, Training* ist zu planen und umzusetzen (vgl. Abschn. 3.2).
- Ein zentrales Sicherheits-Informationssystem ist einzurichten und aktuell zu halten (zumindest in größeren Unternehmen).
- Dokumentation und Aufzeichnungen sind zu lenken (vgl. Abschn. 3.3 und Abschn. 3.4).
- Die korrekte Einhaltung des Sicherheitskonzeptes ist kontinuierlich zu prüfen (vgl. Abschn. 16.1).
- Sicherheitsvorfälle müssen geeignet behandelt werden (vgl. Abschn. 16.3).
- Es ist ein Berichtswesen aufzubauen und zu betreiben – unter Berücksichtigung der Verfahren zur Generierung von Nachweisen (vgl. Abschn. 16.4).
- Eine Wartung aller Sicherheitselemente – Dokumentation, Maßnahmen, Prozesse – ist regelmäßig zu planen und durchzuführen (vgl. Abschn. 3.1).

Fall 2: Etwas differenzierter sieht es bei größeren Organisationen, etwa Konzernen aus. Gehen wir zunächst von einer *zweistufigen* Hierarchie aus. In der obersten Konzernebene (Holding etc.) wird ein *zentraler IT-Sicherheitsbeauftragter* anzusiedeln sein, dessen Aufgaben insbesondere darin bestehen,

- die Sicherheitsleitlinie des Konzerns aktuell zu halten und für den gesamten Konzern verbindlich zu machen,
- gewisse Vorgaben zur Interoperabilität bei der Sicherheit zwischen den Konzerntöchtern herzustellen (z. B. Vorgaben über einheitlich anzuwendende Verschlüsselungsverfahren),
- ein zentrales Sicherheits-Informationssystem für den Konzern einzurichten und zu betreiben,
- ggf. das Thema *Sensibilisierung, Schulung, Training* übergreifend zu organisieren,
- sich von den IT-Sicherheitsbeauftragten der einzelnen Konzerntöchter die Einhaltung der Sicherheitsleitlinie regelmäßig nachweisen zu lassen.

Darüber hinaus wird dieser IT-Sicherheitsbeauftragte ggf. für die Sicherheit der Holding selbst zuständig sein.

In den *einzelnen Konzerntöchtern* wird es eigene IT-Sicherheitsbeauftragte geben. Ihre Tätigkeit haben wir im „Fall 1“ oben schon umrissen. In Relation zur Holding werden sie

- die „von oben“ kommende Sicherheitsleitlinie ggf. um für ihre Gesellschaft spezifische Dinge ergänzen,

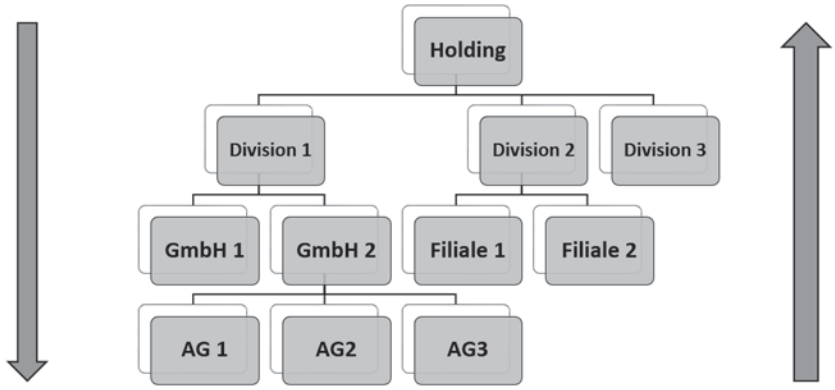

Abb. 2.2 Mehrstufiger Konzernverbund

- diese erweiterte Leitlinie in ihrer Gesellschaft in Kraft setzen (lassen) und
- sie durch ein Sicherheitskonzept für ihre Gesellschaft konkretisieren,
- das Sicherheitskonzept umsetzen und
- Nachweise generieren, die zeigen, dass insbesondere die Konzern-Sicherheitsleitlinie korrekt umgesetzt wurde.

Ergänzen bzw. *erweitern* meint, dass der von oben kommenden Leitlinie für die Gesellschaft spezifische Regelungen hinzugefügt werden können, Regelungen und Vorgaben der Konzernleitlinie aber weder explizit, noch implizit außer Kraft gesetzt werden dürfen.

Fall 3: Besitzt ein Konzern mehr als zwei Ebenen (siehe Abb. 2.2), so wird dies wie folgt zu organisieren sein:

- Die jeweils von der nächst höheren Ebene kommende Leitlinie wird ggf. mit spezifischen Ergänzungen in Kraft gesetzt, durch ein Sicherheitskonzept konkretisiert und umgesetzt.
- Es werden entsprechende Nachweise über die Einhaltung der Leitlinie erzeugt und „nach oben“ weitergeleitet.
- Die (ggf. ergänzte) Leitlinie wird „nach unten“ an die nächst tiefere Ebene durchgereicht (sofern eine solche existiert), dabei werden regelmäßige Nachweise die Einhaltung der Leitlinie betreffend gefordert.

2.3 Geschäfts- und Verwaltungsprozesse

2.3.1 Grundsätzliches

Man verwendet den Begriff der *Ablauforganisation*, um auszudrücken, wie die Abläufe in einer Organisation festgelegt sind. Statt von Abläufen ist auch von *Verfahren* oder *Prozessen* die Rede: bei Unternehmen von *Geschäftsprozessen*, bei Behörden eher von

http://www.springer.com/978-3-658-09973-2

Der IT Security Manager
Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden

Kersten, H.; Klett, G.

2015, XX, 297 S. 24 Abb., Softcover
ISBN: 978-3-658-09973-2