1 Einleitung

Der englische Begriff Security fasst üblicherweise die Themen Datenschutz und Datensicherheit zusammen. Damit wird eine Zugriffsbeschränkung der Daten im Rahmen der Autorisierung und ein Verhindern von Hackerangriffen definiert. Des Weiteren werden Anforderungen abgeleitet, die eine Zerstörung der Daten verhindern sollen, sei es durch unvorhergesehene Ereignisse oder durch bewusste Sabotage, wiederum durch Hacker. Dies schließt auch eine Betrachtung der Applikationen, Systemarchitektur und Rechenzentrumsinfrastruktur mit ein.

Dieses Buch will all diesen Aspekten Rechnung tragen und behandelt Security aus drei Sichten:

- Behandlung von Bedrohungen durch kriminelle Aktivitäten
- Ordnungsmäßigkeit des Betriebs, insbesondere Strukturierung von Berechtigungen und Autorisierungsprozessen
- Sicherstellung des Betriebs

Das Buch orientiert sich sowohl an einer klassischen BI-Architektur – mit oder ohne zentralem Data Warehouse (DWH) – als auch an einer explorativen Architektur für Data-Science-Aufgaben mit einem Data Lake. Soweit notwendig und möglich werden spezifische Exkurse in Spezialthemen, wie Cloud BI oder Big Data Analytics, in Unterabschnitten berücksichtigt und vertieft.

Die meisten Fachbücher werden nicht von vorne bis hinten durchgelesen wie ein Roman. Vielmehr sind sie praktische Arbeitshilfsmittel. Nur einzelne Abschnitte werden vollständig gelesen. Andere Teile werden nur benötigt, um schnell etwas nachzuschlagen, beispielsweise Checklisten, Begriffs- oder Methodenerklärungen. Und natürlich gibt es auch Teile, die gar nicht gelesen werden.

Ähnlich wird es sich auch beim Gebrauch dieses Buches verhalten, wobei ich als Autor natürlich hoffe, dass die ungelesenen Teile recht gering sind.

1.1 Aufbau des Buches

Um eine schnelle Nutzung des Buches zu ermöglichen, will ich zuerst die Hauptteile des Buches erklären, die nach der allgemeinen Einführung in das Buch in diesem und in Kapitel 2 folgen:

Teil I – Behandlung von externen Bedrohungen

In diesem Teil des Buches liegt der Fokus in der Abwehr von Hackerangriffen auf die eigenen Systeme, Daten und Infrastruktur. Es werden alle Aspekte zur Entdeckung und Abwehr von kriminellen Aktivitäten behandelt. Das einleitend beschriebene Referenzmodell führt Schritt für Schritt durch die verschiedenen Aktivitäten, beginnend mit der Bedrohungsmodellierung bis hin zur Risikobeurteilung und Behandlung. In Kapitel 3 wird das Modell erklärt und die einzelnen Schritte werden in den nachfolgenden Kapiteln jeweils vertieft.

Teil II – Berechtigungsstrukturen, Prozesse und Systeme

Im zweiten Hauptteil werden ab Kapitel 7 alle Aspekte der Autorisierung betrachtet. Zuerst werden die Anforderungen an Berechtigungsmodelle und unterschiedliche Implementierungsarten behandelt. Anschließend werden alle Prozesse zur Erteilung, Überprüfung und zum Entziehen von Rechten erklärt. Abschließend erfolgt noch eine Beschreibung der organisatorischen Verantwortlichkeiten und Herausforderungen bei komplexen Berechtigungsanforderungen.

Teil III – Sicherstellen des operativen Betriebs

Es nützt wenig, wenn wir zweckmäßige Berechtigungssysteme implementieren und unsere Systeme perfekt gegen jede Art von kriminellen Bedrohungen schützen, wenn der Server »abraucht«. Das bedeutet, dass wir uns auch Gedanken zur betrieblichen Sicherheit machen müssen, wozu auch Backup- und Restore- oder Disaster-Recovery-Konzepte gehören (siehe Kap. 10). Dazu muss zuerst die betriebliche Kritikalität des Systems bekannt sein. Das heißt, wir müssen wissen, welcher Schaden, abhängig von der Systemausfalldauer, entstehen kann.

Das Vorgehensmodell aus Teil I dieses Buches eignet sich zwar auch zur Erhebung und Implementierung der Verfügbarkeitsanforderungen, ähnlich wie verschiedene Normen und Standards im Sicherheitsbereich. Allerdings geht das Vorgehensmodell eher auf die Behandlung und das Verhindern von kriminellen Aktivitäten ein und weniger auf die Behandlung von operativen Risiken der eigenen Systemlandschaft, beispielsweise ISO 27000 ff. oder BSI[1]. Deshalb habe ich mich entschlossen, einen weiteren Hauptteil einzufügen, rein aus der Sicht von IT-Operations und deren Anforderungen.

---

1. BSI – Deutsches Bundesamt für Sicherheit in der Informationstechnik.

Teil IV – Standards, Methoden und Normen

Viele Unternehmen orientieren sich bereits ganz oder teilweise an der einen oder anderen Norm oder sind sogar danach zertifiziert. Weitere Firmen nutzen zumindest Teile von bestehenden Sicherheitsstandards, -methoden und -normen sowie Modelle für Business Intelligence und Data Warehousing. Bei der Beschreibung der verschiedenen Schritte des Vorgehensmodells aus Teil I wird regelmäßig auf die entsprechenden Normen referenziert. Dadurch bietet dieser Teil mit Kapitel 11 eine Orientierung über die bestehenden Normen in Form einer Kurzbeschreibung, wie sich diese für Data-Warehouse- oder Business-Intelligence-Systeme eignen.

Es ist nicht Ziel des Buches, komplett neue Konzepte zu erfinden und zu beschreiben, sondern die vorhandenen Konzepte möglichst zweckmäßig für analytische Systeme zu adaptieren und nur, wenn notwendig, durch neue Elemente zu ergänzen. Daher werden die wichtigsten Frameworks kurz beschrieben, sodass deren Grundkonzept ganzheitlich verstanden wird.

Teil V – Hilfsmittel und Checklisten

Dieser Teil enthält in Kapitel 12 eine Sammlung von Checklisten, Kurzbeschreibungen oder Arbeitsanweisungen. Er bietet somit einen Werkzeugkasten, aus dem Sie sich bedienen können.

Zusätzlich enthält dieser Teil auch Abschnitte zu Aspekten der Security, die in kein vorheriges Kapitel gepasst haben und mir trotzdem wichtig sind.

Durch die wachsenden und sich schnell verändernden Bedrohungssituationen ist es schwierig, abzuschätzen, wie sich das Thema Security verändern wird. Einige Trends sind in Kapitel 14 aufgeführt.

Anhang

Der Anhang dieses Buches enthält eine Beschreibung der wichtigsten Werkzeugkategorien und jeweils eine Auflistung verschiedener Tools sowie einen Exkurs in die verwandten Themen Privacy und Lizenzmanagement. Den Abschluss bilden ein Glossar, ein Literaturverzeichnis und eine Linkliste sowie ein Stichwortverzeichnis.

1.2 Grundkonzept

Zweck eines Security-Konzepts ist es, alle fachlichen, technischen und organisatorischen Anforderungen aufzuzeigen und einzuordnen, Lösungsmöglichkeiten zu erklären und vorzuschlagen sowie geeignete Maßnahmen umzusetzen. Nicht Teil des hier vorgestellten Konzepts sind Konfigurationseinstellungen in einzelnen Technologien, wie beispielsweise Active Directory, oder Tools für Reporting und Analyse. Ziel dieses Buches ist es, Security-Aspekte aufzuzeigen, die während des

Anforderungsmanagements, der Projektumsetzung und des IT-Betriebs relevant sind.

Das Buch enthält konkrete Lösungsvorschläge, Handlungsempfehlungen und Checklisten. Dadurch wird eine einfache und schnelle Umsetzung ermöglicht, ohne sich zuerst über Wochen oder Monate zum Security-Experten ausbilden lassen zu müssen. Trotz aller Tipps sollte frühzeitig mit der Berücksichtigung von Security-Aspekten in den Projekten begonnen werden, da besonders organisatorische Regelungen manchmal recht zeitraubende Abstimmungsprozesse nach sich ziehen. Idealerweise werden bereits alle Anforderungen auf Auswirkungen bezüglich Sicherheit geprüft oder entsprechend erweitert, bevor eine Umsetzung erfolgt.

1.3 Ganzheitliche Betrachtung von Security

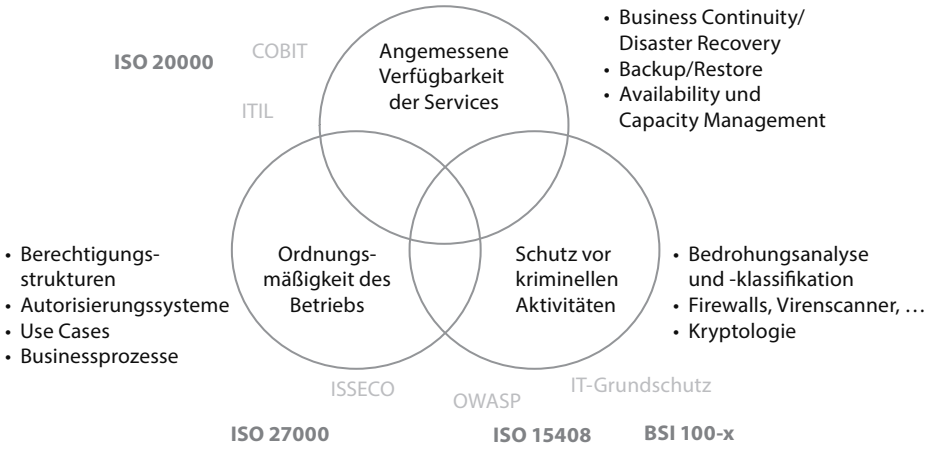

Abb. 1–1 *Die drei Security-Aspekte: Ordnungsmäßigkeit, Schutz und Verfügbarkeit*

Unter IT-Sicherheit wird häufig nur das Vermeiden von bösartigen Zugriffen von externer Seite verstanden und die Vorstellung, dass Passwörter davor schützen können. Dies wird so leider nicht funktionieren. Um dies zu verstehen, ist es notwendig, zuerst alle drei Aspekte von Security zu erklären:

- Ordnungsmäßigkeit des Betriebs
- Schutz vor kriminellen Aktivitäten
- Angemessene Verfügbarkeit der Services

Alle drei Aspekte sind nicht vollständig voneinander abgegrenzt und es ist wichtig, die Gemeinsamkeiten aus Sicht von Datenschutz und Datensicherheit zu verstehen.

1.3.1 Ordnungsmäßigkeit des Betriebs

Im Rahmen eines ordnungsmäßigen Betriebs wird sichergestellt, dass Mitarbeiter nur Aktivitäten ihres Aufgabenbereichs ausführen können, für die sie autorisiert sind und die notwendigen Qualifikationen haben. Das heißt, es wird eine Berechtigungsstruktur benötigt. Diese Berechtigungen werden abgeleitet von der organisatorischen Zugehörigkeit, den Aufgaben in den Geschäftsprozessen oder von einzelnen Anwendungsfällen (engl. Use Cases).

Die Verwaltung der Benutzerrechte erfolgt idealerweise über ein zentrales, rollenbasiertes Autorisierungssystem. Die Identifikation eines Anwenders in einer Applikation geschieht zumindest über User und Passwort, Single Sign-on oder über technische Hilfsmittel wie Token. Bei kritischen Anwendungen ist eine Kombination mehrerer Hilfsmittel oder eine Zwei-Wege-Authentifizierung sinnvoll. Alle Aktivitäten werden zudem protokolliert.

1.3.2 Schutz vor kriminellen Aktivitäten

Passwörter bieten leider nur einen geringen Schutz gegenüber Hackerangriffen. Üblicherweise erfolgt der Einstieg in Systeme über technische Lücken, wie bekannte oder unbekannte Fehler in der Software oder in einer unvollständig konfigurierten Systemlandschaft.

Ein Hacker muss nur eine einzige Lücke finden, um zum Ziel zu gelangen. Währenddessen müssen Security-Verantwortliche alle Lücken finden und diese schnellstmöglich schließen. Diese Diskrepanz führt zum ein oder anderen Frustrationserlebnis bei Security-Verantwortlichen. In diesem Bereich findet daher ein laufendes Wettrüsten statt zwischen besseren Sicherheitsmechanismen und raffinierteren Tools und Tricks für einen Angriff.

1.3.3 Angemessene Verfügbarkeit der Services

Es nützt wenig, wenn die Systeme gegen Hackerangriffe geschützt sind und über ein zweckmäßiges Berechtigungssystem verfügen, wenn sich die Infrastruktur verabschiedet, beispielsweise durch einen Brand im Rechenzentrum. Um eine angemessene Verfügbarkeit sicherzustellen, müssen verschiedene Aufgaben gelöst werden. Diese lassen sich in einfache und komplexe Maßnahmen gliedern. Zu den einfacheren Aufgaben gehören Datensicherungen (Backup und Restore). Komplexer ist die Erstellung eines Disaster-Recovery-Konzepts, das die Wiederherstellung eines Service oder der gesamten Infrastruktur sicherstellt. Dabei werden Szenarios wie der Ausfall eines kompletten Rechenzentrums, Konkurs eines Cloud-Anbieters oder Softwarelieferanten oder auch Elementarereignisse (Feuer, Wasser, Erdbeben, Blackouts, …) berücksichtigt.

1.3.4 Standards, Methoden und Zertifikate

Verschiedene Organisationen haben eigene Verfahren und Methoden zur Erreichung einer genügenden Sicherheit entwickelt und diese publiziert. Dazu gehören Unternehmen wie Microsoft mit der STRIDE-Methode[2], staatliche Organisationen, wie das deutsche Bundesamt für Sicherheit (BSI), oder Vereinigungen und Non-Profit-Organisationen wie die OWASP[3].

Viele dieser Modelle und Methoden eignen sich ebenfalls sehr gut für Data Warehouses und Business-Intelligence-Systeme.

Darüber hinaus wurden mehrere Standards entwickelt, nach denen sich ein Unternehmen oder ein Unternehmensbereich zertifizieren lassen kann, beispielsweise nach ISO 27000. Eine Zertifizierung hat den Vorteil, dass die Minimalanforderungen mit einem allgemein gültigen Maßstab überprüft werden. Die zertifizierte IT hat dadurch einen offiziellen Nachweis für die Ordnungsmäßigkeit gegenüber ihrer Geschäftsleitung, was vonseiten des IT-Managements als entlastend empfunden wird. Als Nachteil wird jedoch der Aufwand für die Erreichung des Zertifikats angesehen. Meistens muss dazu eine umfangreiche Dokumentation erstellt und laufend aktualisiert werden.

1.4 Klassen von potenziellen Schäden

Alle Störungen und Schadensereignisse können nach ihren Auswirkungen in drei Hauptklassen gruppiert werden:

- Verlust der Verfügbarkeit
- Verlust der Vertraulichkeit
- Verlust der Integrität

Die einzelnen Hauptklassen sind nachfolgend kurz beschrieben.

2. STRIDE-Methode: Akronym aus den Anfangsbuchstaben der sechs typischen Bedrohungs- bzw. Schadensarten: Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
3. OWASP – Open Web Application Security Project. Non-Profit-Organisation mit dem Ziel der Entwicklung sicherer Software jeglicher Art. Der Name stammt noch aus der Gründung, als der Schwerpunkt einzig bei Webapplikationen lag.

Verlust der Verfügbarkeit

Auswirkung	Beispiele
Wichtige Informationen sind nicht mehr verfügbar. Die Ausführung von Arbeiten ist nur eingeschränkt oder nicht mehr möglich.	■ Brand des Rechenzentrums ■ Das Data Warehouse steht nicht rechtzeitig mit den aktuellen Daten bereit infolge nicht zweckmäßiger Ladeprozesse ■ Blackout ■ Konkurs des Outsourcing-Partners ■ Untauglicher Backup/Recovery-Prozess ■ Das Netzwerkkabel zum Rechenzentrum wurde durch Baggerarbeiten zerstört

Tab. 1–1 *Verlust der Verfügbarkeit*

Verlust der Vertraulichkeit

Auswirkung	Beispiele
Der Schutz von personenbezogenen Daten gemäß DSG oder von Geschäftsgeheimnissen (Patente, Verfahren, strategische Dokumente, …) ist nicht mehr gewährleistet.	■ Lücken in Security-Systemen ■ Datendiebstahl durch Mitarbeiter oder Hacker ■ Spionage ■ Fehlerhafte automatisierte Reportverteilung (z. B. falscher Mailverteiler) ■ Diebstahl von Endgeräten mit lokal gespeicherten Reports (Notebooks, Tablets, …)

Tab. 1–2 *Verlust der Vertraulichkeit*

Verlust der Integrität

Auswirkung	Beispiele
Die Korrektheit und Vollständigkeit von Informationen ist nicht mehr sichergestellt. Die Glaubwürdigkeit ist teilweise oder vollständig infrage gestellt. Die Auskunftsbereitschaft ist mit den vorhandenen Daten nicht mehr möglich.	■ Fehlbuchungen ■ Fälschung ■ Technische Fehler bei der Datenübertragung ■ Ungenügende Datenpflege (Datenqualität) ■ Fehlende Schlüssel ■ Fehlende Einträge in Dimensionstabellen (Ladeprozesse ohne referenzielle Integrität nach Kimball)

Tab. 1–3 *Verlust der Integrität*

Die Aspekte Datensicherheit und Datenschutz sowie die drei Aspekte des Security-Modells dieses Buches können den abstrakten Schadensgruppen gegenübergestellt werden, wie in der nachfolgenden Matrix dargestellt. Daraus sind Gemeinsamkeiten ersichtlich.

	Datensicherheit	Datenschutz	Ordnungsmäßigkeit des Betriebs	Schutz vor kriminellen Aktivitäten	Angemessene Verfügbarkeit des Service
Verlust der Verfügbarkeit	X				X
Verlust der Vertraulichkeit		X	X		
Verlust der Integrität	X	X	X	X	

Tab. 1–4 *Matrix mit Security-Aspekten und abstrakten Schadensgruppen (Gemeinsamkeiten)*

1.5 Unterschiede zu transaktionalen Systemen

Irgendwann stellt sich die Frage, was denn die Unterschiede von Data Warehouses und Business-Intelligence-Systemen zu operativen Systemen sind. Gibt es überhaupt Unterschiede zu transaktionalen und operativen Systemen? Wenn ja, was sind dann diese?

Es gibt ein paar Punkte, die auf den ersten Blick recht banal wirken, jedoch aus Sicht der Security einige wesentliche Unterschiede ausmachen.

Fehlende Use Cases oder nur Use Cases mit untergeordneter Bedeutung

In einem operativen System kann jede der verschiedenen Transaktionen einem Use Case zugeordnet werden. Außerdem kann jeder Use Case bei der Anforderungsanalyse einer operativen Aufgabe, meistens einem Prozessschritt, zugeordnet und entsprechende Sicherheitsanforderungen und notwendige Berechtigungen definiert werden.

Diese Use Cases fehlen in BI-Systemen üblicherweise. Auch die Zuordnung von dispositiven Systemen[4] zu einem Geschäftsprozess oder einer Aufgabe ist selten möglich. Im Vordergrund stehen dafür Abfragen und Daten, die einen nur unscharf definierten Informationsbedarf decken sollen. Das bedeutet, dass daraus nicht so einfach notwendige Zugriffsrechte aufgrund einer Aufgabe abgeleitet werden können. Außerdem kommt den Datenrechten eine höhere Bedeutung zu.

4. Der Begriff dispositive Systeme wird üblicherweise für Data Warehouses und für Reporting-Systeme oder Dashboards verwendet. Diese Systeme können nicht einer operativen Aufgabe zugeordnet werden, sondern stellen den übergreifenden Informationsbedarf einer Unternehmung oder Organisation sicher.

Single Point of Truth (SPOT)

Data Warehouses bilden eine unternehmensweite Sicht oder mindestens Teilsicht ab und nutzen dazu verschiedene Datenquellen. Dadurch steckt in einem Data Warehouse ein großes Potenzial von Wissen, was natürlich auch das Interesse von Angreifern weckt.

Da lange Zeit Data Warehouses nur intern zur Verfügung standen, war es allerdings für externe Hacker nicht oder nur schwierig möglich, sich einen Zugang zu den Daten zu verschaffen. Durch die zunehmende Verbreitung von Mobile BI hat jedoch das Potenzial eines unbefugten externen Zugriffs deutlich zugenommen.

Ein großes Risiko geht auch von den internen Mitarbeitern aus. Nicht jeder ist hundertprozentig loyal zur Unternehmung. Das heißt, der Diebstahl von Daten und die finanzielle Verwertung sind möglich, sei es durch den Verkauf an externe Personen oder durch Erpressung des Arbeitgebers. Eine regelmäßige Sicherheitsüberprüfung der Mitarbeiter oder ihrer vorhandenen Rechte ist daher sinnvoll.

Allerdings erfolgt nicht jede Straftat von Mitarbeitern aus kriminellen Absichten. Möglicherweise ist ein Mitarbeiter selbst das Opfer eines Social-Engineering-Angriffs[5] geworden oder der Mitarbeiter wird selbst erpresst.

Erhöhtes Risiko der Entstehung von Persönlichkeitsprofilen

Sie haben vielleicht auch schon einmal erlebt, dass jemand eine Geschichte über eine nicht anwesende Person erzählt, ohne deren Namen zu nennen. Der Erzähler hat dabei so viele Eigenschaften über diese Person genannt, dass ein Zuhörer unterbricht und fragt: »Sprichst du von …?« Der Erzähler reagiert meist überrascht, weil er die Identität der Person schützen wollte, indem der Name nicht genannt wurde. Er war sich allerdings nicht bewusst, dass eine Identifikation über die von ihm preisgegebenen Informationen möglich war. Es ist ein Persönlichkeitsprofil entstanden.

Der Gesetzgeber behandelt Persönlichkeitsprofile wie nicht anonymisierte Personendaten. Das heißt, sie unterstehen ebenfalls dem Datenschutzgesetz. Durch das Zusammenführen von Informationen aus mehreren Datenquellen nimmt die Anzahl der Merkmale einer Person zu. Das bedeutet, dass eine feingranulare Unterscheidung möglich ist oder schnell und unbewusst Persönlichkeitsprofile entstehen können.

Bei der Speicherung und Verwendung von Personendaten ist daher ein besonderes Augenmerk auf die mögliche Entstehung von Persönlichkeitsprofilen zu richten und die Anforderungen der Datenschutzgesetze sind einzuhalten.

---

5. Siehe dazu Abschnitt 13.1.2.

Redundante Datenhaltung

Data Warehouses werden häufig als redundante Datenhaltung zu den operativen Quellsystemen eingesetzt. Sie beinhalten meist andere auf Abfragen und Analysen optimierte Datenmodelle. Inhaltlich sind die Daten identisch. Eine Grundanforderung ist, dass die Datenzugriffsrechte im Data Warehouse in etwa denen in den operativen Quellsystemen entsprechen. Als logische Konsequenz muss der Analyst sich mit den datenbezogenen Berechtigungen des Quellsystems beschäftigen und ein ähnliches Berechtigungsmodell spezifizieren.

Unterschiedliche Rechte je Detaillierungsgrad

Eine weitere Eigenart von BI-Systemen sind Anforderungen an unterschiedliche Berechtigungen je Detaillierungsgrad. Manchmal ist es sinnvoll, auf der tiefsten Ebene eine eingeschränkte Sichtweise zuzulassen. Beispielsweise wenn sich auf dieser Ebene Personeninformation befinden, die durch das Datenschutzgesetz geschützt sind. Durch eine Verdichtung auf einer höheren Ebene findet automatisch auch eine Anonymisierung statt. Dadurch kann die Breite der Information deutlich zunehmen.

Leider sind noch die wenigsten Systeme in der Lage, diesen Sachverhalt von unterschiedlichen Berechtigungen je Aggregation zuzulassen. Daher müssen beim Design eines Systems einige Kniffe in den Datenmodellen angewandt werden, die später in diesem Buch eingehend erklärt werden.

Komplexe, meist eigenentwickelte Architektur

Die meisten Data Warehouses mit den dazugehörenden Dashboards und Reports sind eigenentwickelt. Zwar wurden dabei Standardsoftwarelösungen eingesetzt und die Architektur orientiert sich an üblichen Referenzmodellen. Die Datenmodelle, die gewählte Architektur, die Ladeprozesse und Reports basieren aber auf einer Eigenentwicklung. Erschwerend kommt hinzu, dass die eingesetzten Technologien häufig von unterschiedlichen Herstellern stammen. Das heißt, dass an verschiedenen Orten funktionale Berechtigungen definiert und eingerichtet werden müssen. Leider gibt es selten ein durchgängiges Metadatenmanagement, das diese Arbeit erleichtert. Außerdem werden an verschiedenen Orten Administratorenrechte benötigt für die Datenspeicherung, die Ladeprozesse und Frontend-Lösungen. Vielfach sind diese unterschiedlichen Administratorenrechte noch auf verschiedene Technologiespezialisten verteilt.

Selten operative Auswirkungen eines Systemausfalls

Bei operativen Systemen kann üblicherweise recht leicht bestimmt werden, welche Auswirkungen ein Systemausfall auf die Geschäftstätigkeit hat. So lassen sich entgangene Gewinne für den Ausfall eines Buchungssystems schätzen sowie Folgekosten für Workarounds oder die Aufarbeitung ermitteln. Daraus kann abgeleitet werden, wie lange eine Systemunterbrechung verkraftbar ist.

Da Data Warehouses und BI-Systeme mehrheitlich eine dispositive Bedeutung haben, wirken sich Systemunterbrechungen nur indirekt aus. Das heißt, es ist deutlich schwieriger zu ermitteln, welche Auswirkung mögliche Fehlentscheidungen haben, weil Informationen nicht rechtzeitig zur Verfügung stehen, oder welche monetären Konsequenzen verspätete Entscheidungen zur Folge haben. Somit ist der Nutzen von BI-Systemen höchstens indirekt und in Folge nicht klar quantifizierbar. Dies wiederum bedeutet, dass die notwendige Verfügbarkeit nur schwer zu ermitteln ist. Die gewählte Systemarchitektur orientiert sich daher meist an den Betriebskosten und nicht an den möglichen Auswirkungen eines Systemausfalls. Das heißt, es werden eine möglichst einfache Systemlandschaft und ein tiefer Service Level gewählt – manchmal zu tief.

Zusammenfassung und Merkpunkte

Dieses einleitende Kapitel behandelt folgende Themen:

- Erklärung zum Aufbau des Buches als Orientierungshilfe
- Beschreibung des Security-Modells, das als Grundlage für die Strukturierung dieses Buches dient, mit den Hauptaspekten: Ordnungsmäßigkeit des Betriebs, Schutz vor kriminellen Aktivitäten und angemessene Verfügbarkeit sicherstellen. Das Modell wird mit den abstrakten Schadensklassen »Verlust der Verfügbarkeit«, »Verlust der Vertraulichkeit« und »Verlust der Integrität« verglichen und Gemeinsamkeiten werden aufgezeigt.
- Auflistung und Beschreibung von Unterschieden von analytischen Systemen zu transaktionalen Systemen